



GLOBAL  
NETWORK  
INITIATIVE



DERECHOS  
DIGITALES  
América Latina

# TECHNOLOGIES USED IN THE FIGHT AGAINST THE PANDEMIC

## PERSONAL DATA IN LATIN AMERICA

LAURA NATHALIE HERNÁNDEZ RIVERA, DERECHOS DIGITALES  
FOR THE GLOBAL NETWORK INITIATIVE | OCTOBER 2021

ESPAÑOL

ENGLISH

# TABLE OF CONTENTS

SUMMARY	3
ABOUT THE AUTHOR	4
ATTRIBUTION	4
ACKNOWLEDGEMENTS	4
<b>1. INTRODUCTION</b>	<b>5</b>
<b>2.1. DEPLOYMENT OF TECHNOLOGIES IN RESPONSE TO THE COVID-19 HEALTH CRISIS</b>	<b>8</b>
Argentina	7
Bolivia	10
Brazil	11
Colombia	14
Ecuador	15
El Salvador	17
<b>2.2. DATA PROTECTION LEGAL FRAMEWORK</b>	<b>20</b>
Table I. Data Protection Legal Framework	20
<b>2.3. GOVERNMENT REQUESTS TO ACCESS DATA HELD BY MOBILE OPERATORS</b>	<b>27</b>
Brazil	27
Colombia	29
Ecuador	30
<b>3. DISCUSSION</b>	<b>32</b>
<b>4. CONCLUSION AND RECOMMENDATIONS</b>	<b>37</b>
<b>ANNEX I. LIST OF THE MAIN APPS USED IN THE COVID-19 CONTEXT</b>	<b>40</b>



## SUMMARY

The health emergency brought about by the SARS-CoV-2 virus forced governments around the world to seek solutions to limit the spread of the virus. Technology played a key role in responding to this. Many apps were developed and big data was used to monitor crowds and people's movement through data regarding their cell phone connections to cell towers, geolocation and bluetooth. Latin America was part of this trend. With the purpose of learning about their implementation in the region, in particular regarding the use and protection of personal data, we conducted research on the development of technologies to fight the pandemic across six countries: Argentina, Bolivia, Brazil, Colombia, Ecuador, and El Salvador. Several official sources were consulted, including press reports, interviews with representatives of digital human rights protection organizations, and scholarly articles on this topic. Results show that while there has been a significant boost in the deployment of technologies and mechanisms to collect and process information, there is still much work to do to ensure that the design, development, and implementation of technologies for the protection of people's health strictly comply with human rights standards and are consistent with the protection of privacy and informational self-determination.



## ABOUT THE AUTHOR

Laura Nathalie Hernández Rivera is a Salvadoran lawyer that specializes in technology. She is also a public policy analyst for the civil society organization Derechos Digitales Latinoamérica where she monitors public policy and legislation-related events and initiatives related to human rights and technology in Latin America. She holds a PhD in Law from la Universidad Federal de Cear  in Brazil and has an LL. M. on the Right to High Technologies and Intellectual Property from the University of Santa Clara in the U.S.

## ATTRIBUTION

The content, analysis, and recommendations of this report belong solely to the author and do not necessarily reflect the opinions of the Global Network Initiative.

## ACKNOWLEDGEMENTS

I wish to express my gratitude to the following individuals for their contributions and availability to engage in interviews that allowed me to better understand the context in each one of the countries that formed part of this study:

- > Nathalie Fragoso (InternetLab- Brasil)
- > Daniel Ospina (Dejusticia- Colombia)
- > Luc a Camacho (Fundaci n Karisma- Colombia)
- > Enrique Chaparro (Fundaci n V a Libre- Argentina)
- > Eduardo Ferreyra (Asociaci n por los Derechos Civiles- Argentina)
- > Carlos Palomo (Transparencia-Contralor a Social-Datos Abiertos- El Salvador)
- > Wilson Sandoval (Centro de Asesor a Legal Anticorrupci n de El Salvador- El Salvador)
- > Paloma Villa Mateos (Telef nica, S.A.)

# 1. INTRODUCTION

On March 11, 2020, the World Health Organization (WHO) declared COVID-19 a global pandemic, caused by the novel SARS-CoV-2<sup>1</sup> coronavirus. As the disease spread across the Americas<sup>2</sup> and health systems began to collapse, governments declared states of emergency,<sup>3,4,5,6,7,8</sup> which restricted some rights and implemented several measures in an attempt to contain the spread of the virus. These measures ranged from shutting down airports and land borders, schools and leisure places, to confinements of entire populations. Some countries imposed those measures in a timely manner, while others implemented them later on.

Among the strategies adopted to fight the spread of this new virus and the disease brought about by it, most of the countries turned to technological resources, in an effort to minimize infections and keep an eye on the population during mobility restrictions. Thus, a great number of apps were developed to provide official information about the disease, conduct self-assessments, and track infections, among other things.<sup>9</sup>

One of the key discussion topics is the tension between the right to health and the right to privacy that occurs when governments use technologies to gather a great amount of personal and sensitive data used to strategize the containment of the disease, when they request private companies to deliver the data they collect, and when these technologies are deployed without considering the impact they can have



- 
- 1 <https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia>
  - 2 <https://www.bbc.com/mundo/noticias-america-latina-51802906>
  - 3 <https://es.euronews.com/2020/03/13/argentina-declara-emergencia-sanitaria-ante-nuevos-casos-de-coronavirus-en-el-pais>
  - 4 <https://www.elperiodico.com/es/internacional/20200326/bolivia-emergencia-sanitaria-medidas-covid-19-7905461>
  - 5 <https://www1.folha.uol.com.br/equilibrioesaude/2020/02/governo-decreta-estado-de-emergencia-por-cao-de-surto-do-coronavirus.shtml>
  - 6 <https://www.minsalud.gov.co/Paginas/Presidente-Duque-declara-Emergencia-Sanitaria-frente-a-COVID-19.aspx>
  - 7 <https://www.efe.com/efe/america/sociedad/el-presidente-de-ecuador-declara-la-emergencia-sanitaria-por-coronavirus/20000013-4193906>
  - 8 <https://www.france24.com/es/20200314-el-salvador-declara-estado-de-emergencia-en-prevenci%C3%B3n-de-coronavirus>
  - 9 <https://www.apc.org/sites/default/files/herejia-tecno-optimista.pdf>



on the population's human rights. In this context, this report analyzes the ways in which these six Latin American governments — Argentina, Bolivia, Brazil, Colombia, Ecuador, and El Salvador — used these technologies as part of their strategies to stop the spread of the virus, in order to find out how they were implemented and to analyze the risks to people's privacy. This report also provides an initial approach to the cases in which governments requested the data collected by mobile phone companies, with the purpose of understanding how this collaboration was conducted from the human rights perspective.

**The majority of the countries used technological resources in order to minimize spread of the disease and keep an eye on the population during mobility restrictions.**

This analysis is divided into four sections. The first one is an overview of the main technologies implemented by the governments under study, including a description of their features and some of their issues. The second section outlines the legal contexts of the countries at stake, in order to learn about the level of personal data protection provided by national legal frameworks. The third section sets out the countries where the government requested

mobile phone companies to hand over their user databases, in order to find out whether there were legal limits to this information exchange. Finally, the last section includes conclusions and some recommendations regarding the implementation of these solutions, keeping in mind the best practices and the observance of human rights.

## 2.1. DEPLOYMENT OF TECHNOLOGIES IN RESPONSE TO THE COVID-19 HEALTH CRISIS

This section provides a compilation of the technologies created and deployed in response to the COVID-19 health emergency, their functionalities, flaws, information security levels or security aspects that could compromise data, as well as some cases of data breaches or system vulnerabilities.<sup>10</sup>

### ARGENTINA

Argentina — as well as Brazil — was one of the countries that witnessed an unfettered development of apps. A study conducted by “Asociación por los Derechos Civiles” (Association for Civil Rights, or ADC)<sup>11,12</sup> reported there were 11 apps: one at the national level, eight at the provincial level, and two at the municipal level.

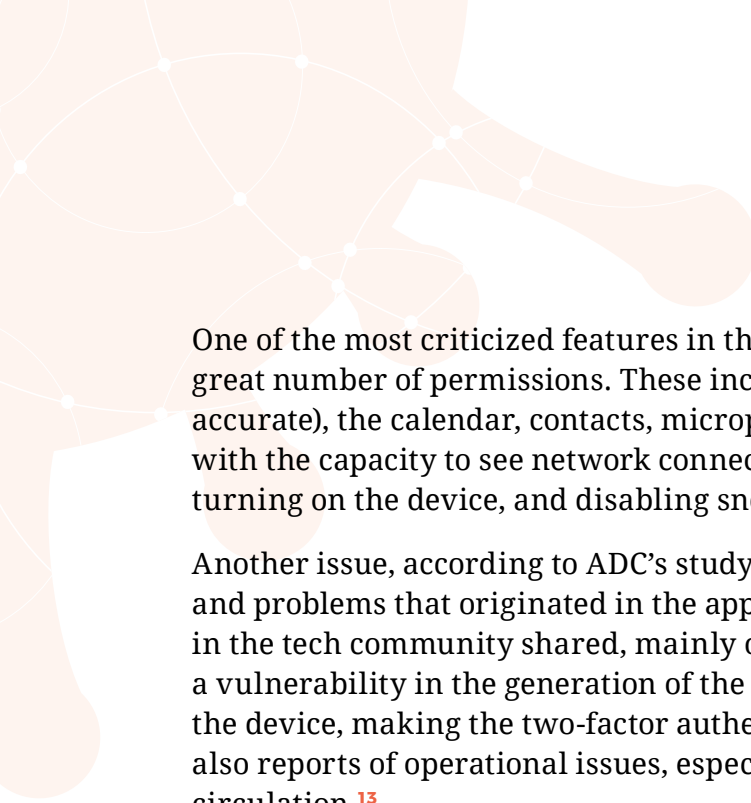
“Cuidar App” was an application launched by the national government. The app’s current version has two objectives: 1) to serve as a tool for self-assessment, and 2) to be an alternative storage for the Certificate for Circulation (a QR by default) to be shown to authorities when appropriate. When exhibiting symptoms of this disease, the information entered is sent to the Provincial Operational Committee of Emergency in the patient’s jurisdiction, so that they can be contacted and given the care needed. If the person gets a negative result in their self-assessment, they get a code allowing them to move through public spaces.



<sup>10</sup> A summary of this section is included in this document as an annex.

<sup>11</sup> <https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/>

<sup>12</sup> <https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/>



One of the most criticized features in the app's Android version is that it requested a great number of permissions. These included access to geolocation (approximate and accurate), the calendar, contacts, microphone, camera, complete access to the network with the capacity to see network connections, audio configuration, auto-start when turning on the device, and disabling snooze mode.

Another issue, according to ADC's study, was the detection of security vulnerabilities and problems that originated in the app's development. To cite ADC's report: "Experts in the tech community shared, mainly on social media, that the app reportedly contains a vulnerability in the generation of the single-use validation token associated with the device, making the two-factor authentication absolutely predictable." There were also reports of operational issues, especially in the generation of the QR code for circulation.<sup>13</sup>

The data collected by the app, as per Resolution 3/2020, was centralized in the "COVID-19 Ministerio de Salud" (COVID-19 Ministry of Health) platform. In this case, the information gathered was stored in the cloud provided by Amazon Web Services, Inc.

According to ADC's report, the Ministry of Innovation announced the publication of the app's source code with the intention of ensuring transparency, as it could be audited and reviewed. However, on top of the delay in publishing the code, it was published incomplete. The publication included only the client side of the code, and not the server side, which would have allowed one to "...analyze and effectively reveal the entire path of the collection and processing of personal data."

As for the other applications created at the different levels, ADC pointed out some of the problems they had:

1. an overlap of purposes they claim to pursue, which obstructs the identification of the actual need they intend to address;
2. terms and conditions failing to establish a deadline for the removal of the collected data, and very broad clauses about data transfers among institutions;
3. limited quality and accuracy of the data obtained through self-assessment apps; and
4. a strong tendency toward citizen persecution in apps that allow notifications about people who do not comply with quarantine.

---

<sup>13</sup> <https://www.cronista.com/economia-politica/Fallas-en-la-app-CuidAR-como-evitar-el-estres-de-no-tener-el-certificado-a-mano-20200703-0004.html>



---

## DATA BREACHES AND OTHER RISKS

During the pandemic, personal data was exposed through an app from the Province of San Juan, which was used to request circulation permissions during quarantine. As reported,<sup>14</sup> “The database containing information about over 115,000 Argentinians who requested circulation permission was uploaded to the network without a password or any other access authentication.” The leaked information included personal data, such as names, ID numbers, tax payer numbers (CUIL), photos, and in some cases, even phone numbers. On top of that, when using the data exposed to check the request status, the permission could be seen, which revealed more data, such as the place and company the person works for, the places the person can go during quarantine, whether the person is a health professional, etc.

The app developed in the Province of Salta was also made publicly available with serious security problems, with the potential to expose the personal and health data of the people who installed it on their phones.

This low level of information security was also evident in the ransomware attack against the National Migration Office’s database.<sup>15</sup> When the required ransom was not paid, the data was published on the Internet. Such data included the information of all the individuals who were repatriated in Argentina due to the pandemic.

One of the hottest topics was the introduction of a protocol named “*Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas*” (General Protocol for the Prevention of Crimes using Open Digital Sources). It aimed at “...establishing general principles, criteria and guidelines for the police force and law enforcement agents under the MINISTRY OF SECURITY to prevent cybercrimes” (Art. 1).

The protocol’s objective was to address “...the crimes associated to the commercialization, distribution and transport of apocryphal medication and critical medical supplies; the sale of medication commercialized allegedly to treat COVID-19 or its name derivations, without the approval or authorization of the relevant authority; and the cyberattacks against critical infrastructure — especially at hospitals and health centers...” (Art. 3).

---

14 <https://www.comparitech.com/es/blog/seguridad-de-informacion/en-argentina-el-ministerio-de-sanidad-hace-publica-la-informacion-personal/>

15 <https://www.pagina12.com.ar/290338-hackers-atacaron-la-direccion-nacional-de-migraciones>

Several organizations<sup>16,17</sup> criticized this rule as the activities regulated by the Protocol are still constitutive of cyber-patrolling and are not “preventive” practices, as they were called. Furthermore, the “*Agencia de Acceso a la Información Pública*” (Access to Public Information Agency, or AAIP) voiced its observations and recommended the discontinuation of the implementation of this Protocol until its alignment with the current personal data protection law was reviewed.<sup>18</sup>

## BOLIVIA

During the pandemic, Bolivia turned to technological tools, like most of the countries around the world, as a measure to stop the spread of the virus.

On the one hand, the platform “*Bolivia Segura*” was developed, with the objective to provide the population with reliable information, statistics about the evolution of the disease and the possibility to conduct a self-assessment to check whether the user is sick. This platform was originally run by the “*Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación*” (Electronic Government and Information and Communication Technology Agency, or AGETIC) but it was later administered by the Ministry of Communication. As reported, the epidemiological information shown on the platform was inconsistent and considerably outdated. There were even changes in the number of deaths.

After that, the “*Bolivia Segura*” app was launched, which contained a self-assessment section. The app requested information including the user’s name, ID number, age, and address. This information was then compared to the data held in the “*Servicio General de Identificación Personal*” (General Service of Personal Identification, or SEGIP) database for validation. The app also provided biometric fingerprint authentication. It also requested information about symptoms (in the self-assessment section) and geolocation to notify a person when they were at risk of infection according to their location at a certain moment. According to its terms and conditions, the information was stored in AGETIC servers, for which the Ministry of Communication was responsible.

These are some of the concerns about this app:

1. It allowed access to data by third parties with lawful purposes, without expressly stating who these third parties could be and what these “lawful purposes” were.
2. It lacked security measures for data protection.

---

16 <https://www.vialibre.org.ar/wp-content/uploads/2020/04/Respuesta.-Res.-Ministerial.-Ciberpatrullaje.pdf>

17 <https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia/>

18 <https://www.vialibre.org.ar/wp-content/uploads/2020/08/NO-2020-47326285-APN-AAIP-1.pdf>

3. It lacked a process to access the data the user enters.
4. It was interoperable with other institutions, like the SEGIP and the Ministry of Health, having no data protection law in place to ensure the appropriate use of data and security mechanisms.

There were other tools created at the regional level: the “*Salud Cochabamba*” app in the Department of Cochabamba and “Dr. Sammy Bot” chatbot for the Departments of La Paz and Santa Cruz.

---

## DATA BREACHES AND OTHER RISKS

Besides having no specific data protection law in place, Bolivia had at least one case of personal data breach. It occurred in an institutional government account, which stored data of people infected with COVID-19.<sup>19</sup>

This happened in April in the Twitter institutional account of the Ministry of Justice, where a list of people with COVID-19 kept by the government of Santa Cruz was disclosed. The list also contained information like age and address. While the local authorities issued a communication stating that the list was fake, it was proven that such a list was, in fact, stored in the government’s official web page, which means that there actually was an information security infringement.

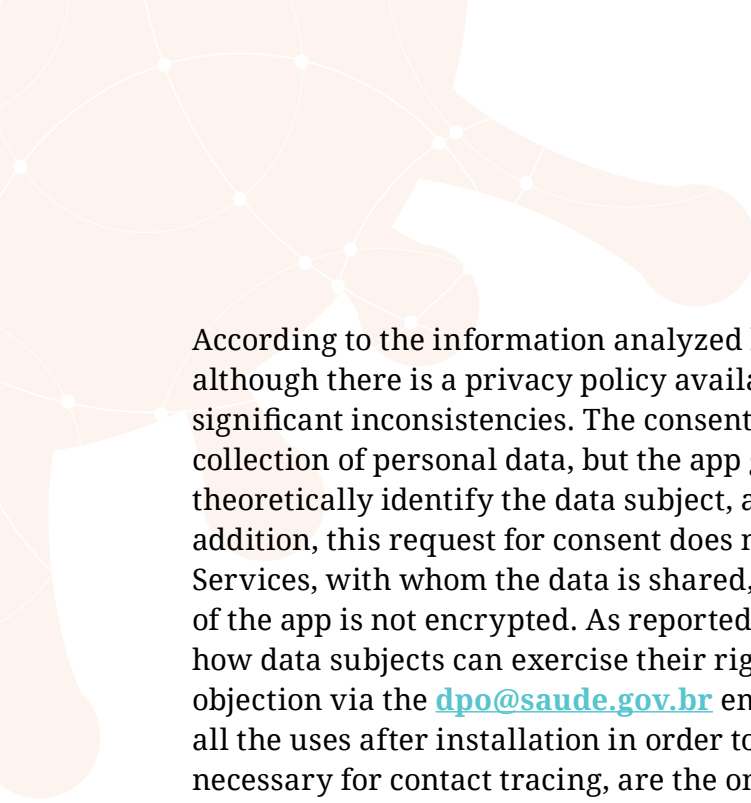
It should be noted that, despite having no proof that this information has been used maliciously by third parties, the fact that this infringement occurred is a sign of poor security management in personal data protection.

## BRAZIL

Brazil had one national app and some state initiatives. The national “Coronavirus-SUS” app was developed by the Health Informatics Department of the Unified Health System (DATASUS), in collaboration with the Federal Ministry of Health, according to official sources originally published on the Ministry’s website, which are currently not available. The app’s privacy policy claims that the specific goal of data processing is to allow the Ministry of Health to identify and notify users about potential contact with people infected with COVID-19.

---

19 [https://internetbolivia.org/wp-content/uploads/2020/11/fd\\_tecnopandemia\\_2021.pdf](https://internetbolivia.org/wp-content/uploads/2020/11/fd_tecnopandemia_2021.pdf)



According to the information analyzed by InternetLab, a civil society organization, although there is a privacy policy available in the current version of the app, it contains significant inconsistencies. The consent form in such a policy states that there is no collection of personal data, but the app gathers “the mobile phone key,” which can theoretically identify the data subject, as well as a positive COVID-19 test result. In addition, this request for consent does not explicitly state the role of Amazon Web Services, with whom the data is shared, or the fact that part of the data communication of the app is not encrypted. As reported by InternetLab, the privacy policy describes how data subjects can exercise their rights to access, rectification, termination, and objection via the [dpo@saude.gov.br](mailto:dpo@saude.gov.br) email address. However, the user must consent to all the uses after installation in order to use the app. Location and bluetooth, which are necessary for contact tracing, are the only opt-in functionalities the user can choose to consent to. The regulatory regime applicable to this app is the “*Lei Geral de Proteção de Dados*” (General Data Protection Law, or LGPD).

Similarly, other technology solutions were developed in other states and municipalities. For example, Rio de Janeiro and São Paulo developed solutions to monitor crowds and users’ movement by using aggregate and anonymized connection data from cell towers. These solutions were created through agreements executed with the companies Claro, Oi, TIM, and Vivo.

Some other solutions were developed by companies specialized in geolocation tools to monitor users’ movement using geolocation data in Recife and Santa Catarina. The system implemented in Recife also notified people who were having an amount of movement that was “higher than average,”<sup>20</sup> while the Santa Catarina system even sent notifications to people who lived near individuals infected with the virus.

Another app that used geolocation was the one implemented in the Amazon region, which monitored people infected with the virus and offered them telehealth services. The monitoring was conducted through the information about the disease evolution that patients were requested to provide.

In some cases, the main concerns about these solutions have to do with the lack of transparency regarding the agreements made between governments and users’ non-consent.<sup>21</sup>

---

20 According to the Executive Secretary of Urban Innovation in Recife, the first step is to analyze what is deemed as “normal” movement in an area; for example, a neighborhood with a hospital will see more movement than a neighborhood with a park. Interview available at: <https://www.uol.com.br/tilt/noticias/redacao/2020/03/28/recife-rastrea-o-celular-de-800-mil-pessoas-para-saber-quem-sai-de-casa.htm>

21 <https://br.boell.org/sites/default/files/2020-06/Tecnologias%20e%20Covid-19%20no%20Brasil%20vigil%C3%A2ncia%20e%20desigualdade%20social%20na%20periferia%20do%20capitalismo.pdf>

The above mentioned “*Sistema de Monitoramento Inteligente*” (Intelligent Monitoring System) deployed in São Paulo includes a Q&A section on the “*Instituto de Pesquisas Tecnológicas*” (Institute for Technological Research, or IPT) website, which includes aspects related to the system operation<sup>22</sup> and a fragment of the agreement executed with the telephone companies.<sup>23</sup>

## DATA BREACHES AND OTHER RISKS

During the pandemic, personal data leaks were reported on at least two occasions in the Ministry of Health. The first case<sup>24</sup> disclosed sensitive data belonging to 16 million Brazilians infected with COVID-19, while the second case<sup>25</sup> affected over 200 million Brazilians, including people affected by the pandemic and citizens registered in the Unified Health System or a health care plan. In total, this figure exceeds the total population of Brazil, since the leakage also included data from deceased people. The leaked data included full name, address, cell phone number, and “*Cadastro de Pessoas Físicas*” (Registry of Natural Persons, or CPF) number. The system, called e-SUS-Notifica, was developed by the technology company Zello. As a result of these leaks, the Ministry of Health could be sanctioned under the new Data Protection Law, since the obligation of providing the necessary data security falls on the data controller (Art. 41 and 42 of the LGPD).

In addition to the personal data leak, an alleged cyberattack against the Ministry of Health network was reported in November that affected the record keeping of COVID-19 data in some states.<sup>26</sup> According to relevant authorities, there was no evidence of compromise, seizure, or data leakage in the said attack.<sup>27</sup>

22 [https://www.ipt.br/noticia/1623-\\_perguntas\\_sobre\\_isolamento\\_social.htm](https://www.ipt.br/noticia/1623-_perguntas_sobre_isolamento_social.htm)

23 [https://www.ipt.br/download.php?filename=1920-Extrato\\_ACT\\_Prestadoras\\_de\\_Servicos\\_de\\_Telecomunicacoes.pdf](https://www.ipt.br/download.php?filename=1920-Extrato_ACT_Prestadoras_de_Servicos_de_Telecomunicacoes.pdf)

24 <https://www.privacytech.com.br/destaque/vazamento-no-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid.,381009.jhtml>

25 <https://www.privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml>

26 <https://g1.globo.com/ciencia-e-saude/noticia/2020/11/13/ministerio-da-saude-diz-que-ha-indicios-de-que-a-pasta-tenha-sido-alvo-de-ataques-ciberneticos.ghtml>

27 <https://g1.globo.com/ciencia-e-saude/noticia/2020/11/06/ministerio-enfrenta-incidente-em-sistemas-que-afeta-atualizacao-de-casos-e-mortes-da-covid-19.ghtml>



## COLOMBIA

Colombia, like many other countries in the world, has also used technological tools as part of its strategy to stop the pandemic. In this sense, the government launched an app called “CoronApp,” which was promoted by the Presidency, also responsible for the “*Instituto Nacional de Salud*” (National Institute of Health, or INS) and the *Agencia Nacional Digital* (National Digital Agency, or AND).

This app already existed in 2017. During that time, it was called “*Guardianes de la salud*” (Health Guardians) and was launched just before the Pope’s visit. Its objectives were to monitor health risks that could be posed by crowds and to receive notifications from users reporting they were sick. As of March 2020, using the 2017 app’s source code as a base, the app became “CoronApp,” now with informational and disease-tracking purposes. Its functionalities allowed the user to receive information and notifications about the disease, health status reports and conduct self-assessments. Later, the functionalities of location tracking and contact tracing by proximity were added.

The app requested the following data: first and last name, ID number, and cell phone number. It also requested health information, like risk factors (traveling, contacts), aggravating factors (chronic diseases, smoking, etc.), and a health status report (having a fever, coughing, having trouble breathing, etc.). It also requested these permissions: access to location (network and GPS), bluetooth, Wi-Fi networks, auto-start when turning on the device, disabling snooze mode, and calling other phone numbers directly. Then, the cell phone would send periodic reports about the device’s GPS location (location tracking), while bluetooth and Wi-Fi networks help identify different nearby devices (proximity tracing).

At first, the app used a contact tracing by proximity system from the U.S. company HypeLabs, which was identified as a centralized bluetooth protocol. Then, the “Blue Trace” protocol was introduced, which was developed for the Singaporean “Trace Together” app, through which “...every device stores in a local database a list of device identifiers with which it has come across.” According to Fundación Karisma, even though this protocol tackled the privacy problem, it was still a centralized protocol, as identifiers were generated by a database hosted in a central server. As Fundación Karisma points out, the risk to privacy is still high, as the server has the capacity to “deanonymize” the identifiers, making the user identifiable.<sup>28</sup>

---

28 <https://web.karisma.org.co/que-dice-que-hace-y-que-es-lo-que-realmente-hace-coronapp/>



A report<sup>29</sup> prepared by Fundación Karisma identified some flaws in the first versions of the app. For example, data was sent without security and encryption, through the HTTP protocol. A vulnerability related to an authentication flaw was also reported. It allowed an attacker to access the user's personal data in the server "from the client side" of the app. However, these flaws were later rectified.

Moreover, the report questions the protection of personal data, due to the lack of information on how privacy and data security are managed. It is not clear what will happen with the data once the emergency phase is over, and the terms of service contain very broad references in relation to the compliance with legal data protection obligations.

**A report prepared by Fundación Karisma questions the lack of information on how data privacy and security is managed by CoronApp Colombia is questioned.**

In this context, the "*Superintendencia de Industria y Comercio*" (Superintendency of Industry and Commerce, or SIC) recommended the INS, the AND, and the Presidential Council for Economic Affairs and Digital Transformation prepare a policy for special information processing, register the "CoronApp" database before the SIC, conduct an audit on the app's security levels, and make the information processing policy available to the public and easy to read.

Another issue was that it was compulsory to download the app. While the latest version of the information processing policy stated that downloading, using, and uninstalling the app was voluntary, the document also indicated that, in the current case of emergency, such freedoms did not apply to the "CoronApp."

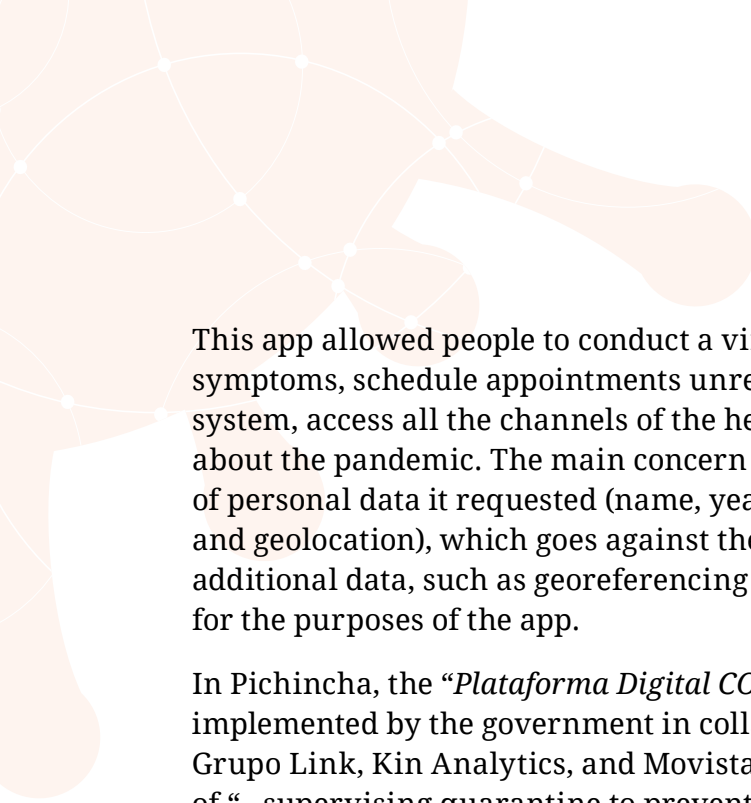
Like other South American countries, different apps were created that competed with the app launched by the federal government. In Colombia, those technologies were a web form called "*Medellín me cuida*," for the Municipality of Medellin, and an app for Cali and Valle del Cauca called "*CaliValle Corona*."

## ECUADOR

During the pandemic, Ecuador also turned to technological tools as part of its measures to mitigate the spread of the virus. The "*Salud EC*" (*Health EC*) app was created in the framework of Executive Decree N° 1017, which allows the use of georeferencing tools.

---

29 <https://web.karisma.org.co/wp-content/uploads/2020/04/Informe-p%C3%BAblico-t%C3%A9cnico-CoronApp-v170320-1-1.pdf>



This app allowed people to conduct a virtual medical triage to check for COVID-19 symptoms, schedule appointments unrelated to the pandemic in the Ecuadorian health system, access all the channels of the health system, and obtain official information about the pandemic. The main concern about this app had to do with the great amount of personal data it requested (name, year of birth, ID number, phone number, email, and geolocation), which goes against the data minimization principle, since it requested additional data, such as georeferencing of the user's address, which was not necessary for the purposes of the app.

In Pichincha, the “*Plataforma Digital COVID-19*”<sup>30</sup> (COVID-19 Digital Platform) was implemented by the government in collaboration with private companies: Claro, Grupo Link, Kin Analytics, and Movistar. The platform was created with the purpose of “...supervising quarantine to prevent people from breaking isolation rules, defining cordon sanitaires, conducting massive COVID-19 testing of users registered in 171 and “Salud EC,” monitoring crowds and the disinfection of areas, and applying penalties to those who break the curfew.”

This platform was designed to:

1. manage quarantine and cordon sanitaires by tracking people through apps, contact centers, and georeferencing tools;
2. manage massive testing through the information collected from calls made to the 171 phone line; and
3. monitor crowds and movement through the geolocation of gatherings of over 30 people, by using 911 cameras and big data from telecommunications companies.

The main red flag identified in this app is the huge amount of data collected through the integration of multiple databases. There should have been a robust process to ensure the security of the data stored, so that such data was not misused and did not represent a risk to people's privacy and informational self-determination.

Finally, the “*Ecuador Así*” app was developed by the company Link in collaboration with the Inter-American Development Bank (IDB) to notify about physical proximity of affected individuals by using Bluetooth. According to its privacy terms, both downloading the app and logging a confirmed or suspected COVID-19 infection were voluntary. To install or use the app, it was not necessary for users to enter their identity, address, email, or phone number. According to this document, the app did not access

---

30 <https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-pone-al-servicio-de-la-capital-de-la-republica-un-nuevo-instrumento-tecnologico-para-enfrenar-el-coronavirus-la-plataforma-digital-covid-19/>



An analysis of the app “Ecuador Así,” by the *Observatorio Ciberderechos & Tecnosociedad of the Universidad Andina Simón Bolívar*, presented informative, legal, and technical observations that should have been taken into account for the protection of the personal data of Ecuadorians.

the data stored in the cell phones where it was installed, nor did it track the user’s location.

Its terms of use do not contain any type of guidance for the data subjects to exercise their rights to access, rectification, termination, and objection, which is questionable. On the other hand, in an analysis conducted by the “*Observatorio Ciberderechos & Tecnosociedad*” (Cyber Rights and Technosociety Observatory) in the Universidad Andina Simón Bolívar<sup>31</sup>,

there were some informative, legal, and technical comments that should have been taken into account for the protection of Ecuadorians’ personal data, especially considering that:

1. at that moment, Ecuador was one of the few countries that did not have a specialized data protection law; and
2. there had been a massive data breach in September 2019.

The statements in the fourth informative remark highlight that: “In order to promote the app, SMS emergency messages (SNGRE) are sent without the user’s consent. It is worth mentioning that receiving such SMS messages directly from SNGRE is a poor security practice. Malicious attackers could use the same system to carry out social engineering attacks (phishing) against users as a means to propagate malware.”

## EL SALVADOR

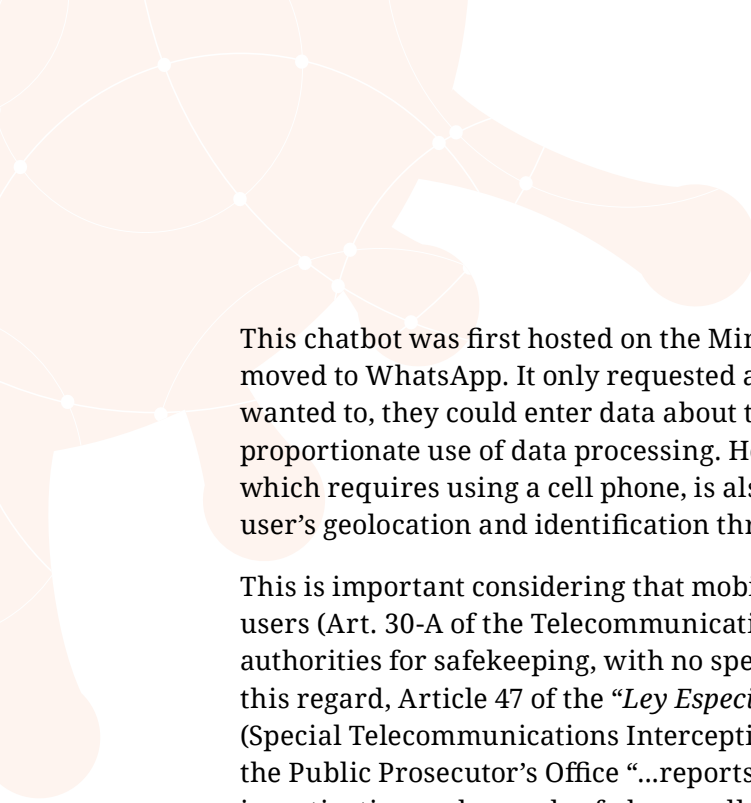
During the national emergency, some technological measures were implemented:

1. One was the “SIVI” chatbot,<sup>32</sup> developed jointly by the Ministry of Innovation, Facebook, and the company Infobip. The chatbot displayed a menu with six options. These allowed the user to conduct a self-assessment (by answering questions about symptoms), learn about the main symptoms and modes of transmission, learn about the home quarantine, get tips for the prevention of the disease, learn about myths and rumors about the virus, and submit reports (it is unknown what could be reported and what the reporting was like).

---

31 <https://www.uasb.edu.ec/web/ciberderechos/analisis-de-la-aplicacion-asi-ecuador>

32 <https://diario.elmundo.sv/sivi-respondera-dudas-sobre-covid-19-desde-messenger-de-facebook/>



This chatbot was first hosted on the Ministry of Health’s Facebook page, and then it was moved to WhatsApp. It only requested a name to begin the interaction and, then, if the user wanted to, they could enter data about their health (symptoms) — which could qualify as a proportionate use of data processing. However, we cannot overlook the fact that this tool, which requires using a cell phone, is also prone to generating other types of data, like the user’s geolocation and identification through their cell phone company’s databases.

This is important considering that mobile phone operators must keep a record of their users (Art. 30-A of the Telecommunications Law), which must be made available to the authorities for safekeeping, with no specifications on time limits for such retention. In this regard, Article 47 of the “*Ley Especial para la Intervención de las Telecomunicaciones*” (Special Telecommunications Interception Law) states that operators must submit before the Public Prosecutor’s Office “...reports about the data of registration of phone line(s) under investigation and records of phone calls, emails, and other means of telecommunications...” whenever it is required. Also, WhatsApp, owned by Facebook, has its own procedure for data processing, so we cannot rule out the risk of creating profiles for advertisement or any other activity for which the chatbot was not adopted.


Despite all this, we cannot confirm that there has been an improper processing of personal data, as there were no reports in the news or among the technology community on this during the three months in which it operated.

2. The other one was a web page created to learn about the economic benefits provided by the government during quarantine. To see their benefit, the user had to enter their unique ID number. If they were eligible to receive the benefit, they had to go to one of the banks in the bank system and withdraw the assigned amount (US\$ 300). The first website did not have a security certificate, which is an ongoing issue in government websites. After the website collapsed, it was moved to another server. There are no incidents reported in relation to the data of the beneficiaries, but it is not clear how the database feeding the website was processed (liquefied petroleum gas subsidy).

While there is no document reporting data breaches or system vulnerabilities, some weaknesses were identified in some of the technological tools deployed by the government as part of its response to the COVID-19 emergency. The most predominant one was the lack of security certificates in platforms and web pages. These websites included the platform that was deployed to check, by entering the person’s ID number, whether that person was a beneficiary of economic aid provided by the government during the first few days of quarantine. The site collapsed in a matter of minutes, since it did not have a SSL certificate.<sup>33</sup> A similar case was the implementation of an “immunity card” that included a database

---

33 <https://www.elsalvador.com/noticias/nacional/web-subsidio-coronavirus-colapsa/700662/2020/>



**In the case of El Salvador several weaknesses were identified regarding certain technological tools that the government implemented as part of the emergency response to COVID-19.**

about people who recovered from the disease, containing a QR code that led to a website without a security certificate.<sup>34</sup>

This becomes increasingly important when analyzed alongside other cases apart from the COVID-19 issue, underscoring the lack of basic security measures in the web pages of government institutions. Firstly, there was the publication of the confidential data of over five million Salvadorans on

the Ministry of Finance's website.<sup>35</sup> Secondly, students' grades were changed by hacking the web page of the Universidad de El Salvador.<sup>36</sup> In general, there is a lack of security certificates in the Salvadoran Ministries' web pages.

Finally, one of the most delicate cases about information security is associated with notifying individuals of their COVID-19 test results. According to a news article, COVID-19 test results are sent in Excel format, through WhatsApp, to the Ministry of Health and to Venezuelan advisors of the President, with the prohibition to include the results on the online platform of the "*Sistema de Vigilancia Epidemiológica*" (Epidemiological Surveillance System).<sup>37</sup>

---

34 <https://diario.elmundo.sv/gobierno-inicia-con-la-entrega-de-carnes-de-inmunidad-a-recuperados-de-covid-19/>

35 <https://gatoencerrado.news/2020/07/10/hacienda-publico-datos-privados-de-millones-de-salvadorenos/>

36 <https://www.elsalvador.com/noticias/nacional/hackean-sistema-web-universidad-el-salvador/732239/2020/>

37 <https://www.elsalvador.com/noticias/nacional/venezolanos-dirigen-mesa-toma-muestras-covid-19-el-salvador/722087/2020/>

## 2.2. DATA PROTECTION LEGAL FRAMEWORK

For the six countries in this study, this section compiles an analysis of the regulations, case law, guidelines or national agreements with regards to personal and health data processing, both before the pandemic and during the COVID-19 emergency. It includes the authorities in charge of data protection and their responsibilities regarding data protection.

To allow for easier interpretation, the information on such legislation is presented in a table followed by comments.

**TABLE I. DATA PROTECTION LEGAL FRAMEWORK**

Constitution	Data protection law	International treaties	Other secondary laws	Case law
<b>Argentina</b>				
Art. 43. It regulates Habeas Data. <sup>38</sup>	Data Protection Law (LDPD) N° 25.326. <sup>39</sup>	Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data <sup>40</sup> , introduced through Law N° 27.483.  The UN International Covenant on Civil and Political Rights (Art. 17); the Universal Declaration of Human Rights (Art. 12); and the American Convention on Human Rights (Art. 11).	Decree N° 1.558 of 2001 establishing the Data Protection Law N° 25.326.  “Guidelines on the processing of personal data in the use of geolocation tools,” <sup>41</sup> issued by the AAIP.  In the context of the pandemic, the AAIP published the “Guidelines on the processing of personal data during COVID-19.” <sup>42</sup>	Judgment by the National Supreme Court of Justice, October 15, 1998, known as the “Urteaga” case, which imposed on the State the obligation to make the information contained in their databases or files available to the public.

38 <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm>

39 <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto>

40 <https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf>

41 [https://www.argentina.gob.ar/sites/default/files/guia\\_geolocalizacion\\_0.pdf](https://www.argentina.gob.ar/sites/default/files/guia_geolocalizacion_0.pdf)

42 [https://www.argentina.gob.ar/sites/default/files/guia\\_coronavirus\\_0.pdf](https://www.argentina.gob.ar/sites/default/files/guia_coronavirus_0.pdf)

Constitution	Data protection law	International treaties	Other secondary laws	Case law
<b>Bolivia</b>				
<p>Art. 21. It establishes the right to privacy, intimacy, reputation, one's image and dignity.<sup>43</sup></p> <p>Art. 130. It regulates the so-called Privacy Protection Action, contained in Art. 58 of the Constitutional Procedure Code.</p>	None	<p>The UN International Covenant on Civil and Political Rights (Art. 17); the Universal Declaration of Human Rights (Art. 12); and the American Convention on Human Rights (Art. 11).</p>	<p>Art. 56 of the General Law of Telecommunications and Information and Communication Technologies. It amends Art. 79 of the Electoral Body Law, in reference to the interoperability between the Civic Registry Service (SERECI) and the SEGIP.</p> <p>Art. 12 of the Digital Citizen Law.</p> <p>Art. 19 of Supreme Decree N° 28.168 of May 18, 2005. It regulates Habeas Data.</p>	<p>The right to informational self-determination was recognized as a human right through Plurinational Constitutional Decision 0090/2014-S1.<sup>44</sup></p>
<b>Brasil</b>				
<p>Art. 5, subsection X of the Constitution, which regulates the inviolability of people's intimacy, private life, honor and image. Subsection XII, which regulates the inviolability of communications; and subsection LXXII, which regulates Habeas Data.<sup>45</sup></p>	<p>General Data Protection Law (LGPD) N° 13.709/18.<sup>46</sup></p>	<p>The UN International Covenant on Civil and Political Rights (Art. 17); the Universal Declaration of Human Rights (Art. 12); and the American Convention on Human Rights (Art. 11).</p>	<p>Civil Rights Framework for the Internet (Law N° 12.965 of 2014)<sup>47</sup></p> <p>Law N° 9.507 of 1997, which regulates Habeas Data.</p> <p>Consumer Protection Code (Law N° 8.078 of 1990).</p>	None

43 [https://www.oas.org/dil/esp/constitucion\\_bolivia.pdf](https://www.oas.org/dil/esp/constitucion_bolivia.pdf)

44 <https://jurisprudenciaconstitucional.com/resolucion/13467-sentencia-constitucional-plurinacional-0090-2014-s1>

45 [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)

46 [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)

47 [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)

Constitution	Data protection law	International treaties	Other secondary laws	Case law
<b>Colombia</b>				
Art. 15 of the Political Constitution <sup>48</sup> establishes people's right to "... know, update and rectify the information collected about them in databases and files held by private and public entities."	Law N° 1581 of 2012, which sets out the general provisions for data protection. <sup>49</sup>	The UN International Covenant on Civil and Political Rights (Art. 17); the Universal Declaration of Human Rights (Art. 12); and the American Convention on Human Rights (Art. 11).	Law N° 1266 of 2008, which regulates Habeas Data. Decree N° 1377 of 2013, which partially establishes Law N° 1581.	Judgment T-414 of 1992 <sup>50</sup> , which considers the right to Habeas Data as a guarantee of the right to privacy. This has evolved and, as of Judgment SU-082 of 1995, Habeas Data is deemed as an autonomous right. Such consideration is repeated in Judgment C-1011 of 2008 <sup>51</sup> by the Constitutional Court.
<b>Ecuador</b>				
Art. 66, paragraph 19 of the Constitution of the Republic <sup>52</sup> guarantees the right to the protection of personal data. It indicates that data processing needs to obtain the data subject's consent or be mandated by law. Art. 92 regulates Habeas Data.	Organic Law on Data Protection, Official Record N° 459, May 26, 2021. <sup>53</sup>	The UN International Covenant on Civil and Political Rights (Art. 17); the Universal Declaration of Human Rights (Art. 12); and the American Convention on Human Rights (Art. 11).	Art. 21 of the Statistics Law. Art. 2 of the Organic Law on Identity Management and Civil Data.	Judgment N° 001-14-PO-CC of July 3, 2014 <sup>54</sup> by the Constitutional Court, which establishes the reference criteria for personal data and information protection.

48 <https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf>

49 <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

50 <https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm>

51 <https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm>

52 [https://www.oas.org/juridico/pdfs/mesicic4\\_ecu\\_const.pdf](https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf)

53 <https://bit.ly/3c3wipJ>

54 <https://www.coronelyperez.com/wp-content/uploads/2019/10/5.-Habeas-Data-jurisprudencia-vinculante.pdf>

Constitution	Data protection law	International treaties	Other secondary laws	Case law
<b>El Salvador</b>				
Art. 2, which provides for the right of honor and dignity, from which derives informational self-determination. <sup>55</sup>	None	The UN International Covenant on Civil and Political Rights (Art. 17); the Universal Declaration of Human Rights (Art. 12); and the American Convention on Human Rights (Art. 11).	Title III of the Access to Public Information Law (LAIP) <sup>56</sup> and its Regulation (RE-LAIP).	Constitutional Case Law has recognized Habeas Data and the right to informational self-determination as a fundamental right on the grounds of Art. 2 of the Constitution, which indicates that the State must ensure the protection of Salvadorans' honor and dignity.

Source: author's compilation.

Table 1 shows that four of the six countries under scrutiny have a specific data protection law and the remaining two have relied on a legal framework made up of constitutional law, international covenants, secondary laws, and case law.

Argentina, Brazil, Colombia, and recently, Ecuador are the countries that have a data protection law. Bolivia and El Salvador do not have such a law yet. It should be mentioned that El Salvador had passed a data protection law, but it was later vetoed by the President,<sup>57</sup> so the country still lacks a specific law on data protection. In Bolivia, at least two bills on data protection were introduced, but there has been no progress on their passing by the Legislative Branch yet.

More specifically, it should be noted, first, the regulation established by the entity in charge of data protection, and, secondly, how health data is categorized in these countries.

55 [https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117\\_072857074\\_archivo\\_documento\\_legislativo.pdf](https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf)

56 [https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117\\_073009410\\_archivo\\_documento\\_legislativo.pdf](https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073009410_archivo_documento_legislativo.pdf)

57 <https://bit.ly/3fW0rZ8>



In Argentina, the authority in charge of overseeing the Data Protection Law is the AAIP, which, through Decree N° 899/2017, subsumed the functions of the National Directorate of Data Protection, which previously carried out the functions set out in Art. 29 of Law N° 25.326. The AAIP has jurisdiction over the data held by public and private entities (Art. 21, 22 and 24). In this sense, the Agency has the power to sanction violations of the LPD, under Art. 31 of this Law, among other things.

Bolivia, having no specific data protection law, has no authority in charge of the data protection, so the only possible means is through privacy protection actions, which are carried out before court.

In Brazil, data protection is a responsibility of the “*Autoridade Nacional de Proteção de Dados*” (National Data Protection Authority, or ANPD), under Art. 55-J, section I of the LGDP. This Authority, which is part of the Republic’s Presidency (Art. 55-A) and was recently set up, has the power to impose administrative sanctions (Art. 55-J, section IV), which are provided for in Art. 52 of the Law.

In Colombia, in line with Art. 19 of Law N° 1581, the authority in charge of data protection is the SIC, which has the power to impose the sanctions provided for in Art. 23 of the above mentioned Law.

In Ecuador, under Art. 75 of the Organic Law on Data Protection, the authority in charge is the Data Protection Authority, which has oversight powers and the authority to impose penalties, in accordance with subparagraphs “a” and “b” of Art. 75.

El Salvador does not have a specific law on this topic. The protection of personal data is under the responsibility of the “*Instituto de Acceso a la Información Pública*” (Institute for Access to Public Information, or IAIP), as established by Art. 51 of the “*Ley de Acceso a la Información Pública*” (Access to Public Information Law, or LAIP). More specifically, Art. 45 of the General Data Protection Guidelines for Public Institutions states that the responsibilities of the IAIP in relation to data protection include, among others: to order, at the request of the parties or upon court’s decision, the elimination, rectification, addition or restriction of the circulation of information held in their files and databases whenever the institutions disobey the rules on data protection. The IAIP’s power to sanction, granted by the same article, is governed by Title VIII of the LAIP, where both infringements and sanctions are set out (Art. 76 and 77, respectively).

In terms of how health data is treated, in Argentina, for instance, according to Law N° 25.326, health data is deemed as sensitive data under Art. 2. According to Art. 7 it grants this data a special protection, establishing that people are not compelled to provide sensitive data, and that the processing of such data can only occur when there is a general interest authorized by law or when there is a scientific and statistical purpose,



provided the person cannot be identified through it. Also, Art. 8 expressly states that the collection and processing of health data must comply with the principles of professional secrecy.

**Of the six countries in the study, four have a concrete law for the protection of personal data.**

Meanwhile, Bolivia includes the following health data references as part of its data protection legal framework:

a) Constitutional Judgement 0965/2004-R, which indicated that the scope of the protection of Habeas Data includes: “...e)


The right to exclude the so-called ‘sensitive information’ related to a person’s privacy...”; b) Law N° 3131 on Professional Medical Practice, which, even though there is no explicit mention of sensitive data, regulates the rights of patients: confidentiality, professional secrecy and respect for privacy.

In Brazil, health data is considered sensitive data under Law N° 13.709/18 (Art. 5, subsection II). Thus, sensitive data can be processed, as a general rule, only when the data subject or legal guardian expressly and specifically consents to the processing for specific purposes (Art. 11, subsection I). That is, consent alone is not enough. It must be specific, singled out and given for a certain purpose. The exceptions to the requirement of consent are established in subsection II of that article.

In Colombia, health data is categorized as sensitive data under Art. 5 of Law N1581, which, as a general rule, shall not be processed save for the exceptions set out in Art. 6.

Ecuador includes health data under the category of special personal data established in Art. 25 of the Organic Law on Data Protection. Thus, collecting and processing such data must comply with the provisions in Art. 30 and 31 of this Law. These articles regulate the authorization for the collection of such data, setting data confidentiality and security as the limit, as well as the exceptions to the requirement of consent to collect it. Additionally, they regulate the minimum parameters for the processing of this type of data, with the recommendation to anonymize or pseudonymize data so that it does not identify the data subject.

In El Salvador, health data is considered as sensitive data under Art. 6 of the LAIP, where there is a brief chapter on the topic. However, in 2018, the Institute for Access to Public Information issued the “Guidelines for the handling and protection of personal data in the medical records of the Salvadoran Health System.” Among other things, this document established directives so that relevant entities who process medical information adopt measures to protect personal data against alteration, loss, transmission, and unauthorized access. It also intends to ensure the confidentiality of sensitive data related to physical and mental health and the adoption of processes for



the submission of and response to requests to access, rectify and eliminate personal data. Meanwhile, in 2019, the Ministry of Health issued the “Technical Regulation for the Preparation, Safekeeping and Review of Medical Records,” which regulates the document management and data protection of medical records and other documents related to the care provided by health facilities. This regulation lays down a person’s right to access, rectify and eliminate information from a medical record, as well as rules for the physical and digital security of their records.

## 2.3. GOVERNMENT REQUESTS TO ACCESS DATA HELD BY MOBILE OPERATORS

This section analyzes the cases of Brazil, Colombia and Ecuador, where companies have been allowed to share users' data with government institutions. This section also includes the consequences of such requests. We were unable to get additional information on Argentina, Bolivia, and El Salvador.

### BRAZIL

During the pandemic, the government adopted Provisional Measure 954 mandating mobile phone carriers to share the name, phone number and address of users with the “*Instituto Brasileiro de Geografia e Estatística*” (Brazilian Institute of Geography and Statistics, or IBGE), given that the Institute was not able to conduct home interviews for the preparation of official statistics during the emergency. This was later suspended by the Federal Supreme Court, establishing that the measure did not clearly define how and to what end the data was going to be collected. It did not specify the types of technical mechanisms that would be implemented to avoid accidental data breaches or data misuse either.

However, some tools developed in States or Municipalities in Brazil did make use of data held by mobile phone carriers in order to operate. Such tools were developed under Law N° 13.979, which compelled federal, state, district and municipal public administration agencies to share, among one another, essential data to identify people with suspected or confirmed coronavirus infections.



In this context, the Prefecture of Rio de Janeiro and the company TIM executed an agreement by which the company would provide connection data from cell towers, in real time, allowing for the monitoring of crowds and population movement. This way, a heat map was generated based on crowds located at a certain place in a given moment. According to the company, this information would keep their clients' anonymity.<sup>58</sup>

Further, the State of São Paulo implemented the “*Sistema de Monitoramento Inteligente*” (Intelligent Monitoring System, or SIMI), developed in collaboration with the mobile phone companies Claro, Oi, TIM and Vivo. The system also used data from operator cell towers to identify crowds and send messages with advice to users. According to the State's authorities, there was no risk to users' privacy, as individual paths were not analyzed and data was anonymized and presented in an aggregated manner, complying with the provisions of the LGPD.<sup>59</sup>

In order to avoid the creation of new platforms with the same objective, the mobile phone operators Claro, Oi, TIM, and Vivo created a single service for state, municipal and federal governments to monitor crowds using heat maps generated by users' mobile data.<sup>60</sup> At the moment of the announcement, 15 states and two cities showed interest in the service. According to the President of the “*Sindicato Nacional das Empresas de Telefonia de Serviços Móvil Celular y Personal*” (National Union of Telephone Companies and Mobile and Personal Services), there would be no risk to privacy, as data was anonymized.

#### **THE NATIONAL GOVERNMENT INTENDED TO CONDUCT THIS TYPE OF MONITORING AT THE NATIONAL LEVEL, BUT IT LATER REFRAINED FROM DOING SO.<sup>61</sup>**

In this context, the “*Agência Nacional de Telecomunicações*” (National Telecommunications Agency, or ANATEL) voiced its opinions about these solutions, stating that “...the adoption of any such measures must derive from a sustained decision, have a legal basis and the sufficient transparency for oversight bodies and the society.”<sup>62</sup> In this regard, ANATEL considered that data collection must be in line with the current legislation and provisions in the Federal Constitution. The protection of health and privacy, even at times of crisis, must include the harmonization of both legal

---

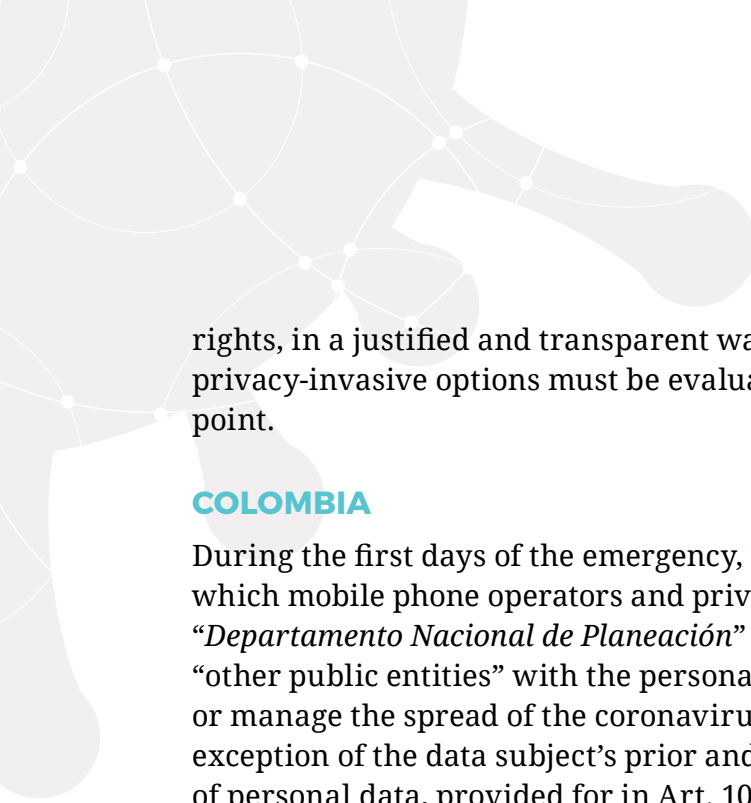
58 [https://www.tim.com.br/sp/sobre-a-tim/sala-de-imprensa/press-releases/institucional/prefeitura-do-rio-fecha-parceria-com-a-tim-para-montar-mapa-de-deslocamento-na-cidade-durante-a-pandemia\\_](https://www.tim.com.br/sp/sobre-a-tim/sala-de-imprensa/press-releases/institucional/prefeitura-do-rio-fecha-parceria-com-a-tim-para-montar-mapa-de-deslocamento-na-cidade-durante-a-pandemia_)

59 <https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contracoronavirus/>

60 <https://www.uol.com.br/tilt/noticias/redacao/2020/04/23/teles-criam-site-para-governos-monitorarem-isolamento-com-dados-de-celular.htm>

61 <https://www.uol.com.br/tilt/noticias/redacao/2020/04/13/bolsonaro-veta-uso-de-dados-de-celulares-para-monitorar-isolamento.htm>

62 <https://www.gov.br/anatel/pt-br/assuntos/noticias/posicionamento-da-anatel-a-respeito-da-utilizacao-de-rastreamento-de-usuarios-de-telecomunicacoes-no-ambito-de-medidas-no-combate-a-pandemia-de-covid-19>



rights, in a justified and transparent way. When considering proportionality, the least privacy-invasive options must be evaluated and consent must be addressed at some point.

## COLOMBIA

During the first days of the emergency, the SIC issued External Notice 001,<sup>63</sup> by which mobile phone operators and private entities were empowered to provide the “*Departamento Nacional de Planeación*” (National Planning Department, or DNP) and “other public entities” with the personal data necessary to deal with, avoid, address or manage the spread of the coronavirus. To justify this, the SIC made reference to the exception of the data subject’s prior and informed authorization for the processing of personal data, provided for in Art. 10, Section “C” of Law N° 1581 (cases of medical or health emergency). Moreover, it based its justification on Art. 13 of said Law, which states that data can be provided to “b) Public or administrative entities in the performance of their legal duties...”

The communication from the *Circular Externa 001* of the Superintendency of Industry and Commerce in Colombia represented a demonstration of authority that tried to go beyond the legal provisions to promote the delivery of personal information.

With regard to this notice, several national and international civil society organizations have warned about the dangers of the broad scope of the document,<sup>64</sup> which could facilitate the provision of personal information disproportionate to the need to control the pandemic. For example, they noticed that **the information about location, identification and communication of users held by these companies risks “... discrimination, undue surveillance, invasion of privacy and protection of journalistic sources.”** They also stated

that **the notice fails to describe in depth the requirements and legal conditions that must be fulfilled by private entities when handing over personal and sensitive data. Also, it does not establish a time limit for the delivery of information or the type of data that can be requested, considering that not all the data collected by the companies is needed to address the emergency.**<sup>65</sup> In short, this act of authority intended to go beyond the legal powers in order to push for the provision of people’s

---

63 <https://www.sic.gov.co/sites/default/files/normatividad/032020/Circular%20001.pdf.pdf>

64 <https://flip.org.co/index.php/es/informacion/pronunciamentos/item/2486-organizaciones-de-la-sociedad-civil-rechazan-circular-de-la-sic-sobre-uso-de-datos-personales-para-controlar-la-pandemia>

65 Idem.

information. We have no proof that such information has been delivered. However, the measure itself is an act that is not in line with the principles of legality, necessity or proportionality for the restriction of informational self-determination.

The “*Sistema de Inteligencia de Epidemiología del COVID-19*” (Epidemic Intelligence System for COVID-19, or SISCOVID) was a case of collaborative work by the government, academics and phone companies.<sup>66</sup> This project, funded by the Ministry of Science, Technology and Innovation, was conceived jointly by researchers from the “*Universidad de Los Andes*,” the “*Centro Nacional de Consultoría*” (National Consulting Center, or CNC) and the “*Universidad de Ibagué*,” together with companies like Movistar, LUCA Data Unit, and Facebook Geoinsights, who provided aggregate data on citizens’ movement taken from their cell phones.

The objective was “...to study the dynamics of the virus through models of mathematical and computer simulation supported by movement data (including MNO data) and surveys, with the purpose of providing evidence for the decisions made in five cities in the country: Barranquilla, Bogotá, Cali, Cartagena and Medellín.”<sup>67</sup> According to a Fundación Karisma report, “It is not clear how... the governments used the knowledge obtained from academic groups.”<sup>68</sup>

## ECUADOR

In the context of the pandemic, a state of exception was declared through Executive Decree N° 1017. This decree allowed “...satellite platforms and mobile phone platforms to monitor people’s location during mandatory quarantine and/or isolation [...]” (Art. 11). This means that through a mobile phone’s GPS, the government could monitor those with a confirmed case of the virus, those who were in contact with people infected or individuals entering the country from abroad, who had to self-isolate for 14 days.

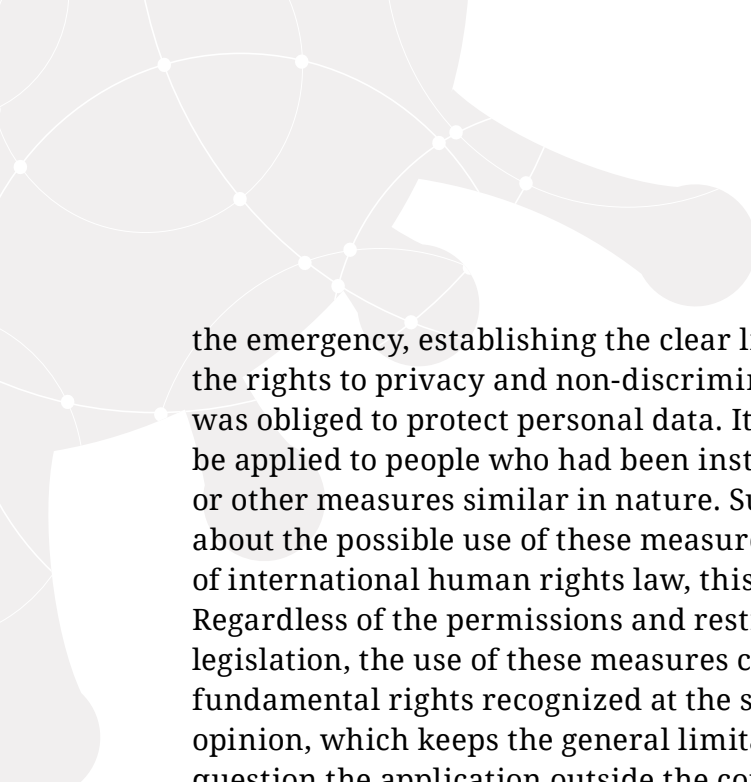
As it allowed for the access to the population’s sensitive information, this measure awakened some questions about its legality, necessity and proportionality, and also concerns about its impact on human rights, like the right to privacy. In this context, the Constitutional Court issued an opinion in favor of the measure, in general terms. However, the Court did comment on the scope of its application. In number 1, sections C) and D) of the opinion about the technological measures taken in Art. 11 of ED N° 1017, the Court pointed out that these measures should only be used in the framework of

---

66 [https://www.researchgate.net/publication/348950496\\_SISCOVID\\_modelos\\_de\\_sistemas\\_complejos\\_para\\_contribuir\\_a\\_disminuir\\_la\\_transmision\\_de\\_SARS-COV-2\\_en\\_contextos\\_urbanos\\_de\\_Colombia](https://www.researchgate.net/publication/348950496_SISCOVID_modelos_de_sistemas_complejos_para_contribuir_a_disminuir_la_transmision_de_SARS-COV-2_en_contextos_urbanos_de_Colombia)

67 <https://descubre.movistar.co/informe-de-gestion-responsable-2020/gestion-2020-4-2.html>

68 <https://web.karisma.org.co/wp-content/uploads/2021/05/Useless-and-Dangerous-A-Critical-Exploration-of-Covid-Applications-and-Their-Human-Rights-Impacts-in-Colombia.pdf>



the emergency, establishing the clear limit that they could not be used to undermine the rights to privacy and non-discrimination. It also underscored that the State was obliged to protect personal data. It also stated that these measures could only be applied to people who had been instructed to comply with voluntary isolation or other measures similar in nature. Such people had to be given information about the possible use of these measures and their scope.<sup>69</sup> From the perspective of international human rights law, this leads to a couple of relevant consequences. Regardless of the permissions and restrictions expressly provided for by the legislation, the use of these measures can eventually lead to the infringement of fundamental rights recognized at the supralegal level. Instead, this is a prospective opinion, which keeps the general limitations included in the Ecuadorian system to question the application outside the constitutional scope.

**The implementation of these measures can eventually represent infringements on fundamental rights.**

In this context, in early April 2020, the government introduced the [ecuador.analiticacovid.com](http://ecuador.analiticacovid.com) platform, which, through heat maps and other functionalities, shows the places where there are large crowds. These maps, according to specialists, are created with data from mobile phone companies,

through the connection of the devices to cell towers.<sup>70</sup> While this collection and representation of information about masses of people is not unprecedented, **the lack of explicit legal safeguards in Ecuador raises concerns about the processing of information from mobile phones, which can be personal or even sensitive information.**

---

69 [http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/0753708f-17ba-4a7b-a818-d93769a77b3a/Dictamen\\_1-20-EE-20\\_\(0001-20-EE\).pdf](http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/0753708f-17ba-4a7b-a818-d93769a77b3a/Dictamen_1-20-EE-20_(0001-20-EE).pdf)

70 <https://www.planv.com.ec/historias/sociedad/asi-funcionan-monitoreos-celulares-que-el-gobierno-usa-vigilar-la-epidemia>



### 3. DISCUSSION

The detailed analysis of the responses of the countries in this report will be based on the opinion of human rights experts at the United Nations (UN) of March 2020<sup>71</sup> regarding the States' responses to the health emergency, which stated "...we urgently remind States that any emergency responses to the coronavirus must be proportionate, necessary and non-discriminatory." The aim of the analysis is to identify these countries' level of compliance with such standards. From this viewpoint, following the UN's language closely, the recommendation points out measures that, by nature, restrict the enjoyment of fundamental rights in the interest of protecting public health.

**Not all countries approached the fight against the pandemic in a similar way through the use of technologies, nor did they clearly prioritize an analysis or evaluation of legality, necessity, proportionality, and non-discrimination.**

However, as can be noted, not all countries took the same approach in the fight against the pandemic using technologies, nor did they prioritize in a clear way an analysis or assessment of legality, necessity, proportionality and non-discrimination. Out of all these countries, El Salvador was the only one that did not develop any apps or request, as far as we know, data from mobile phone companies to map out a contact tracing strategy. Its only measure was a chatbot that provided the options of self-assessment and information about

the virus. And, although this measure may pose some risks due to the metadata in the phones using the chatbot and the sharing of sensitive data, the lack of response to freedom of information requests prevents us from finding more about this tool, whose updates stopped in August 2020.

It is also necessary to note that, in order to better analyze the Latin American States' responses, the social and economic conditions in the region must be taken into account too.

This is the case of measures that require a high level of public involvement, like tracking apps. On the one hand, in most of the countries in the region, a large part of the population does not have access to reliable digital structure, in spite of the governments' efforts to provide the service to the entire population. This gap was

---

71 <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E>



apparent with the implementation of virtual classes, which required students to have access to the Internet and computer devices to take school lessons.

Internet access in the countries studied in this report vary and, in some cases, it is still low. In Argentina, for instance, 82.9 percent of the population has Internet access, while in Bolivia, only 44.2 percent of the people have it. In Brazil, 79 percent of Brazilians have an Internet connection, while Colombia, Ecuador and El Salvador have percentages of 64.6, 59.2, and 59, respectively.<sup>72</sup>

However, in the context of this emergency, there were efforts made by mobile phone operators to help overcome the connectivity challenges through several actions, like an increase of Internet speed at no cost to users, and partnerships with the Ministries of Education in some countries for the deployment of educational platforms.<sup>73</sup> The effectiveness of those actions should be analyzed in the future.

On the other hand, while the penetration of mobile phones in these countries is high, not all of them necessarily have the latest operating system version to support the apps created. This can be paradoxical, since a person may have Internet connectivity on a mobile phone, but they might not be able to download and use the app without having the latest OS version.

An aspect that is often overlooked in the region is the lack of basic digital skills of a large portion of the population, which range from difficulty when using a phone to problems navigating the app's structure. This may lead to a lack of interest in the use of the app or to its misuse.

With regards to purpose, there is a dilemma that needs to be addressed immediately. It is true that the apps under scrutiny mention — some better than others — the purpose for which a person is required to provide their personal data. This would be fine if we were only to assess whether the app complies with the requirement and whether all apps requested the data that is strictly needed for such purpose. Nonetheless, the app alone does not solve the problem of the spread of the virus, but is merely a tool and, as such, it should be part of a much broader health strategy. In that sense, one of the main weak points of these apps is that the population does not get an explanation of how the app is part of a larger fighting strategy. This could limit the number of people who commit to the measure; the more information people have, the more confident they will be about the reasons for providing their data.

---

72 <https://covid.alsur.lat/es/>

73 <https://www.thedialogue.org/blogs/2020/07/desafios-de-conectividad/?lang=es>

Another aspect about purpose, related to the above, is the excessive proliferation of apps, which often have overlapping objectives, making it even more confusing to figure out what exactly these tools are meant to do. It cannot be established with absolute certainty that this disproportionate proliferation of apps is due to the lack of a specific data protection law. This study found that, out of all six countries, this phenomenon occurred in Argentina and Brazil, which do have regulation on data protection, and in Bolivia, where there is no regulation on this topic.

With regards to proportionality, apart from the reported issues of excessive data collection conducted by some apps in their initial stages, we should consider the scenarios in which mobile phone operators share user data with governments.


**When a government communicates its monitoring strategy of infected people to a private telephone company, it exposes the sensitive health data of those individuals.**

This is not just about the risks of this surveillance going beyond the epidemiological purposes. The additional issue is that, when a government engages a private phone company in the strategy of monitoring infected people, it shows sensitive health data about those people. Even when companies have their own privacy policy, and the data handed to the government is anonymized, we should remember that these companies know

their users' identities, so they absolutely can match sensitive data (virus infection) to the data previously collected.

This is an involuntary way of exposing data, so to speak, but this type of risk is precisely why States should be compelled to make prior assessments to determine whether the measure proposed is necessary and proportional; whether the objective being pursued can be accomplished through other, less intrusive means; and whether this measure maintains the balance between the right to health and the right to privacy.

Still in reference to the governments' request for personal data held by phone operators, we should thoroughly consider some other aspects. On the one hand, while anonymization is a successful process and the possibility to re-identify a person is very complicated, it is not enough to simply delete names or phone numbers — although many officials think it is. It is possible to use other data sources to triangulate an individual's personal information. This is why those in charge of cybersecurity in public and private institutions must be extra careful when carrying out this process.




On the other hand, these kinds of collaboration must be transparent. The agreements signed between States and companies must be available to the public. There is no reason under the international human rights law or restrictions on the right to access to information, according to the American Convention on Human Rights, that warrant the execution of such agreements while keeping the public in the dark.

In more complex surveillance systems, transparency must be one of the most important requirements from the perspective of the right to access to information. In these cases, the information necessary to understand the surveillance architecture must be made publicly available.

In this section, we should comment on some apps and computer systems created by States. In the first place, we should mention the risky move of countries like Bolivia and Ecuador, which do not have data protection laws but still created apps and systems to monitor the population's movement. Deploying such apps and systems calls for solid legal frameworks to guarantee privacy and the protection of personal and sensitive data, not only in their corrective aspect but also in their preventive one. In these cases, international human rights law gains more relevance, as it serves as a protective framework for fundamental rights in other countries. That is, concerns about personal information and people's dignity are directly associated with their recognition as fundamental rights in the intersection of constitutional protection and the international treaties ratified by the countries.

This does not mean that, in countries where there are specific data protection laws, the effective protection of informational self-determination is guaranteed, and all actors in the digital ecosystem comply with those regulations to the letter. We simply need to pay attention to the assessments by the different human rights advocacy organizations in the digital space — mainly in Argentina, Brazil, and Colombia — to confirm that the problem does not lie in the lack of legislation, but in the oversight powers and the capacity to impose sanctions vested upon data protection authorities, as well as in the general public's awareness regarding the importance of such protection.

Another reported issue in the design of these apps was their poor security, at least in their first versions. As stated in this report, the civil society organizations working for the protection of human rights in the digital space have reported vulnerabilities in the apps, risking personal data exposure that would affect a large portion of the population. To some extent, the urgency of the public health measures seemed to justify the rushed deployments of emergency mechanisms. However, the risk posed to personal information by the lack of reasonable security conditions is, at the same time, a departure from the principle of data protection security, leading to the possibility of sensitive information affecting the dignity and non-discrimination rights of people.



States should not allow the urgency of a situation to lead to rushed reactions. Each State must assess whether the implementation of certain technologies is necessary and adequate; whether it has the capacity to strike a balance between health and privacy; and, whether there is sufficient evidence on the effectiveness of the proposed tools for the intended purpose. In other words, the development and deployment of technologies must go through a prior assessment process, in tune with the potential impact that their proper or improper operation may have on people. This is an analysis of adequacy, as part of the compliance with the standards of necessity and proportionality, required

**The emergency seemed to justify rapid deployments of relief mechanisms. However, the lack of reasonable security conditions ignored the principle of security in the protection of personal data.**

during the pandemic by international bodies and, outside the pandemic by the human rights instruments in force.

There were also reports about problems around the consent requested for the collection of personal data. The cases of Argentina and Colombia — where announcements and provisions were opposing, on the one hand establishing the mandatory use of the app in certain situations, but stating that downloading it was voluntary — underscore the need to

abide by the protection of human rights from the very design of these tools, especially because consent for sensitive personal data processing is mandatory under most of the legislation on the topic.

Moreover, there is no certainty as to how long the apps under study will keep their databases; whether the data will be destroyed after the emergency; or whether the data will be used afterwards with purposes different from epidemiological monitoring. While the apps' terms of use make reference to the laws that protect people's personal data in each country, we must remember that, when dealing with a data category that needs special protection, the provisions on sensitive data processing should be as specific as possible regarding the respect for users' privacy before, during, and after the emergency.

## 4. CONCLUSION AND RECOMMENDATIONS

The coronavirus emergency has put the whole world's health systems to the test with consequences in every aspect of our lives. To face the pandemic, the governments in most of the countries around the world deployed technological tools in an attempt to slow down the spread of the virus. Latin America was no exception.

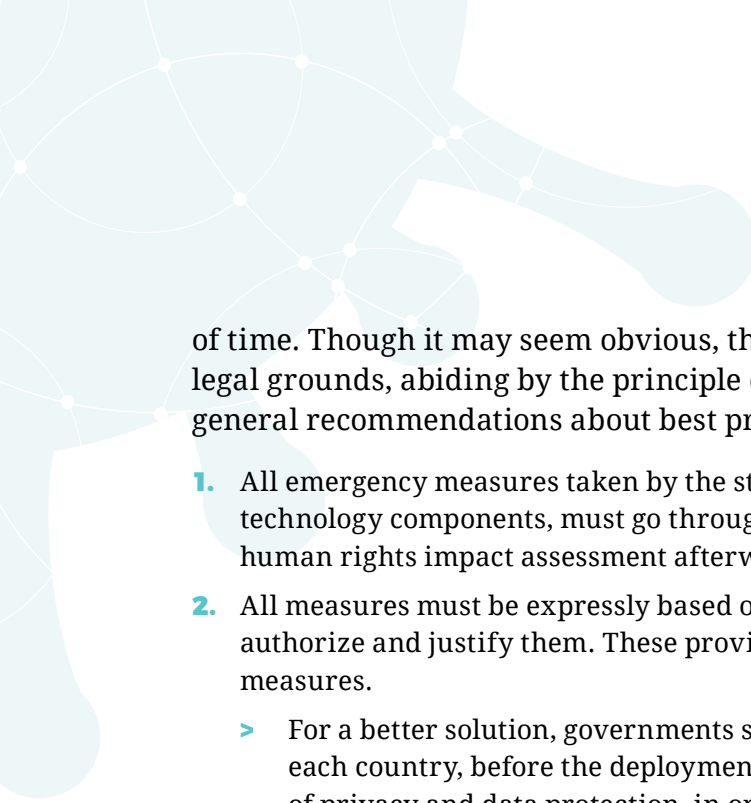
The technologies analyzed in this report shed light on some issues that must be solved in future public health strategies:

- > security issues and risks to privacy in the design of apps;
- > context-specific to the social and economic situation of the countries in the region;
- > problems with the strict compliance with the legislation on data protection and lack of specialized regulation in some countries;
- > limited transparency about the development and deployment of technology solutions, as well as about the agreements executed between private companies and the public administration; and
- > lack of consistency in the use of apps as a general health strategy.

These are some of the flaws found through the comptroller functions of many regional organizations.

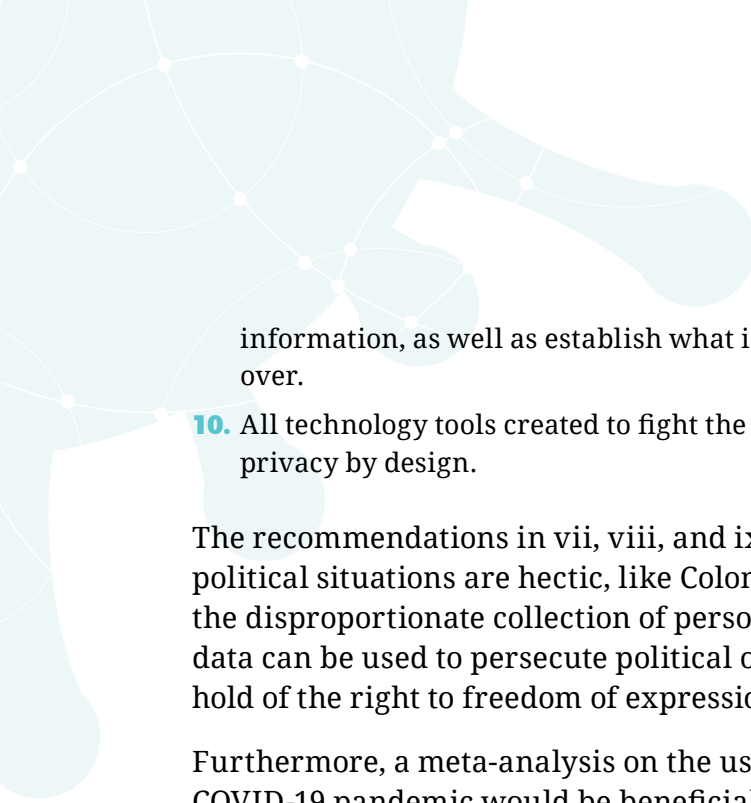
It is clear that the right to privacy is not absolute and that, in the context of the emergency, some invasions of this right, when public health is at stake, are tolerable. However, this does not mean that such invasions should undermine people's privacy and their right to informational self-determination. It is thus necessary that all measures taken to fight the pandemic and any future emergencies be adequate, necessary and proportionate, with a clear and consensual purpose, for a limited period





of time. Though it may seem obvious, the measures should be also based on sufficient legal grounds, abiding by the principle of legality. In that sense, the following are some general recommendations about best practices when using these technologies:

1. All emergency measures taken by the state authorities, including the ones that have technology components, must go through a prior assessment mechanism and include a human rights impact assessment afterward.
2. All measures must be expressly based on the constitutional and legal provisions that authorize and justify them. These provisions should also expressly mention the limits to the measures.
  - > For a better solution, governments should consult with the data protection authorities in each country, before the deployment of any technology that could infringe the principles of privacy and data protection, in order to maintain a balance between privacy invasions and the observance of human rights.
3. The agreements executed between private companies and government institutions must be public, through both active transparency and the right to access to information, so that people know what information is being collected, to what end, what its benefit is, with whom it is being shared, and to provide them with complaint mechanisms.
  - > Promoting the involvement of several sectors of society, with different interests, in the discussions about data processing, and guaranteeing mechanisms for monitoring and evaluation, to determine whether the public interest purposes have been met or whether there is a negative impact brought about by the use of these technologies and the collection and processing of data.
4. All technology developments and all technology purchases must make the apps' source code available for external auditing, understand how the tool works, and identify and fix vulnerabilities.
5. Regardless of the health measures that are applicable to the whole population, as a rule of thumb, the use of technology apps must be voluntary.
6. Before deploying a technology solution, the socio-economic context of the place where it will be deployed must be analyzed to avoid discrimination against certain population sectors.
7. When a measure involves collecting people's information, including people who use communication technologies, it must exclusively adhere to the purposes of fighting the pandemic and be part of a clear health strategy.
8. State policy, in the context of the health emergency, must have explicit commitments regarding personal information processing, including privacy and personal data processing policy when it comes to technology measures, fully observing the principles of data protection, regardless of the existing general data protection laws in each country.
9. State policy, in the emergency context, including its technology components, must set clear and specific terms relative to the termination of the collection and storage of people's



information, as well as establish what is going to happen to the data once the emergency is over.

- 10.** All technology tools created to fight the emergency must comply with the requirement of privacy by design.

The recommendations in vii, viii, and ix gain more relevance in countries where socio-political situations are hectic, like Colombia and El Salvador, due to the risks posed by the disproportionate collection of personal data. This is because, in these contexts, such data can be used to persecute political opponents, human rights advocates, or to keep hold of the right to freedom of expression of the general population.

Furthermore, a meta-analysis on the use of technologies as part of the tools to fight the COVID-19 pandemic would be beneficial from the human rights perspective. Second, it would be appropriate to conduct a study to provide solid evidence about the difference, if any, in the impacts of personal data collection in countries that have specific data protection laws and the ones that do not have such regulations. Third, it would be useful to take a multidisciplinary approach to assess the effectiveness of these tools as a measure to stop the spread of the disease, and to analyze in detail the privacy invasions caused by such tools. Last, we should study the impact that the measures adopted by mobile phone operators had on the mitigation of Internet connection problems.

The more studies are conducted on this topic, the better the information and recommendations we can provide to the authorities and those in charge of public policy in Latin America.



# ANNEX I. LIST OF THE MAIN APPS USED IN THE COVID-19 CONTEXT

App Name	Purpose of the App	Legal Instrument	Overview	Main Concerns
<b>Argentina</b>				
Cuidar App	The app was created to fight the COVID-19 emergency.	Administrative Decision 432/2020 of March 24, 2020.	Its objective is to diagnose COVID-19 symptoms and provide health information to the population. It is also used to store the certificate for circulation.	Concerns about its Android version include: 1) it requests a great number of permissions; for example: access to (approximate and exact) geolocation, calendar, contacts, mic, camera, full access to the network with the capacity to see network connections, audio configuration, auto-start when turning on the device and disabling snooze mode; 2) a vulnerability was reported as regards the generation of the single-use validation token associated with the device.
<b>Bolivia</b>				
Bolivia Segura	The app was created to fight the COVID-19 emergency.	Law for the prevention, containment and treatment of the coronavirus. Law N° 1.293 of April 1, 2020.	Official government app to provide information and statistics about the evolution of the pandemic and serve as a self-assessment online tool.	1) The app allowed access to data by third parties with lawful purposes, without expressly stating who these third parties could be and what these “lawful purposes” were; 2) it lacked data protection security measures; 3) it lacked a process to access the data entered by the user; and 4) it was interoperable with other institutions, like the SEGIP and the Ministry of Health, having no data protection law in place to ensure the appropriate use of data and security mechanisms.
<b>Brasil</b>				
Coronavirus-SUS	The app was created to fight the COVID-19 emergency.	Law N° 13.979 of February 6, 2020.	Initially, it only had informational functions. Later, it added contact tracing functions.	1) lack of certainty about the non-collection of personal data as indicated by its privacy policy; 2) lack of clarity as to what the role of Amazon Web Services is and with whom it shares data; 3) part of the information is not encrypted.



Colombia				
CoronApp	App built on the basis of an existing 2017 app's source code.	Decree 417 of March 17, 2020.	A tool to provide people with information about COVID-19 in Colombia; report symptoms; generate a movement passport and trace contacts.	1) lack of information on how data security and privacy are managed; 2) lack of certainty on the duration of the processing and on what happens with the data once the emergency is over; 3) very general reference to the compliance with legal obligations for data protection in the terms of use; 4) the protocol used, though centralized, did not tackle the privacy issue, as the identifiers of devices near the user, which were stored in a local base in the device, were generated by a server that could de-anonymize identifiers, thus making the user identifiable.
Ecuador				
Ecuador Así	The app was created to fight the COVID-19 emergency.	Executive Decree 1.017 of March 16, 2020.	A tool for the notification of close-proximity contacts through bluetooth.	1) Not enough information on what data will be used, by whom and under what conditions; 2) not enough information on security measures; and 3) emergency text messages from the <i>Servicio Nacional de Gestión de Riesgos y Emergencias</i> (National Service for Risk and Emergency Management, or SNGRE) are sent without the user's consent.
El Salvador				
No app was developed. Only a chatbot called SIVI was deployed.				