Supported by a grant from
OMIDYAR NETWORK

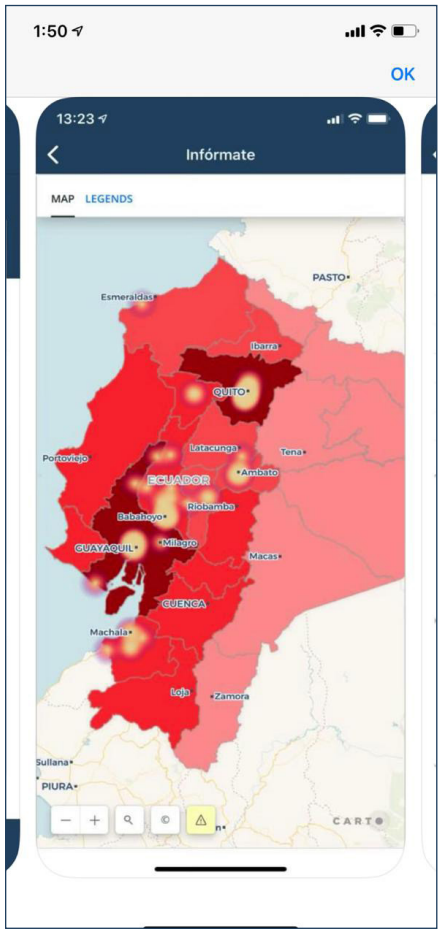
Ecuador's SaludEC

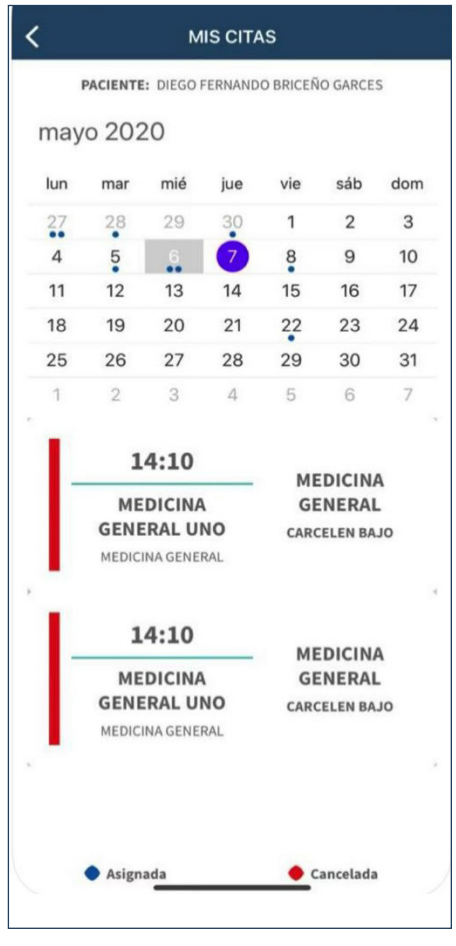
SaludEC is an app created by the Ecuadorian government intended to monitor COVID-19 cases in the country. The app was developed by a private sector company, under the supervision of the public telecommunications company CNT EP, and it was commissioned as part of a provision for broad technological solutions for the healthcare sector. The app was widely promoted in the country for citizens' adoption, including a nationally broadcasted presentation of the app by President Moreno, as well as by the ministers of health and telecommunications.

The app has three main objectives: (a) to allow citizens to perform a COVID-19 self-diagnosis; (b) to provide to citizens with recommendations for COVID-19's treatment; and (c) to allow citizens to schedule medical appointments in public health centres for COVID-19 related cases, as well as non-related treatments, such as Psychology, Obstetrics, and Dentistry. The app is currently available for Android and Apple operating systems and had been downloaded more than 100.000 times by May 11, 2020, representing around 5% of the overall population of 17.5 million people[1].

From the citizens' perspective, the main benefit of using the app is the ability to perform a self-diagnosis assessment and to receive official information and recommendations for COVID-19's treatment, as well as to schedule and follow up medical appointments[2]. From the government's side, the main objective is to gather geolocalized data generated by citizens to support real-time decision-making on COVID-19, and to digitalize the service of public health appointments.

User registration is mandatory to access the app, including the request to access the device's location data. Identity data required during the registration process include the user's full name, national ID, email, and mobile number. Registration is denied if the user's location is outside the territory of Ecuador[3].





APPLYING THE FRAMEWORK

We apply an evaluation test framework below to understand the governance of digital identity systems. The framework was developed by the Centre for Internet and Society (CIS), and it has been applied to other cases of digital identity in the past[4].

TEST SUMMARY

Broadly speaking, the SaludEC has very limited performance in all three tests.

- The app operates without a specific legislative mandate. The app is backed by an executive emergency decree, which has basic and generic authorization for the app's purpose and uses.
- The app has limited provision to rights-based principles, such as data minimization, access to data and mitigation mechanisms.
- In terms of risk assessment, the app has no potential harms to individuals or society mapped. This means that, in case of digital ID misuses, there is no plan of action in place.

LESSONS LEARNED

- By combining geolocation, self-diagnosis and telemedicine services, the application tries to address multiple strategies at the expense of user data security. In the absence of a data protection law in Ecuador, the use of satellite or GPS tracking for health issues should be subject to constitutional provisions[5].
- The user consent method used in the app is unclear and insufficient for its purpose[6]. It is essential that the app´s Terms of Use inform users about the collection and treatment of sensitive data.
- The app requires the user to have a valid ID and be based physically in the country's territory. This is an unjustified burden for having access to urgent health services.

1. RULE OF LAW TESTS

Below are the most basic tests to ensure that a rule of law framework exists to govern the use of SaludEC.

1.1 LEGISLATIVE MANDATE

Is the use of digital identity systems codified in valid law? For this test to be satisfied, the use must be codified in valid law — the parent legislation or other supporting legislation which is in accordance with the scheme envisioned by the parent legislation.

The legislative mandate backing the SaluEC is limited.

The app is not backed by an enacted law, being supported instead by a presidential emergency decree issued on March 16, 2020. The emergency act declared a state of exception throughout the territory (Presidential Decree of State of Exception No. 1017)[7], and instituted several restrictive measures affecting individual rights as a necessary measure to contain the spread of COVID-19.

The aforementioned decree has provisions supporting the app's geolocation and georeferencing use. Article 11 authorizes, in particular, the government to use data from satellite and mobile telephone platforms to "monitor people who tested positive for the virus, those who have been in close contact with someone who tested positive, as well as those who have symptoms, and those subjected to mandatory isolation for having entered the country from abroad."[8]

The decree makes no specific mention to the SaludEC app[9], and no legal provision makes reference to data protection provisions. The topic only appears in the app's Term of Use, that states SaludEC is compliant to "the legal postulates of processing of personal data'' and makes a direct reference to Article 11 of the Decree n°1017.

1.2 LEGITIMATE AIM

Does the law have a legitimate aim? For this test to be satisfied, the use of the identity data must fall under a legitimate aim.

The legitimate aim of the aforementioned emergency executive decree is to curb the COVID-19 outbreak in the country. Broadly speaking, both pieces of legislation are supportive of the app's general purpose.

The decree also stipulates that the state of emergency will last 60 days from March 16. Nonetheless, the decree does not define the future of the data collected during the period after the decree expires.

1.3 DEFINING PURPOSES

Does the law clearly define the purposes for which the ID can be used for? For this test to be satisfied, the purpose for use and control of the identity data must be clearly specified through a legislative process.

The aforementioned decree makes no mention to the specific purpose of the app, and provides no analysis of how the legal mandate supports the app's purposes. Specifically, in terms of Digital ID data, there is no defined purpose related to the nature of data, nor mention of possible abuses related to surveillance, limits of personal data collection or retention.

1.4 DEFINING ACTORS

Does the law clearly define all the actors that can use or manage the ID? For this test to be satisfied, the actors who use and control the use of ID, must be clearly specified through a legislative process.

The decree does not provide information on defining the actors who can use or manage the app. The only instance where actors appear is in the app's Terms of Use, that states that the app owner, Prichsouth Tecnologias Del Sur S. A., has specific authorization to collect, store and process data.

1.5 REGULATING PRIVATE ACTORS

Is this use of the ID system by private actors adequately regulated? For this test to be satisfied, the use of ID by private actors is envisioned with adequate regulation.

Neither the aforementioned decree nor the app's Terms of Use includes provisions for private sector actors using the data. Even so, it should be acknowledged that the app is owned by a private sector company.

1.6 DATA SPECIFICATION

Does the law clearly define the nature of data that will be collected? For this test to be satisfied, the use of identity data must be accompanied by clear specification of the personal data to be collected and processed.

The aforementioned decree does not clearly define the nature of data collected. Article 11 of said decree mentions the use of satellite monitoring and georeferencing data collection, and the purpose of tracking individuals as part of COVID-19 containment measures.

The app's ToU lists the collection of users' identity data, including the ID number, home address, emergency contacts (phone and email numbers), date of birth, gender, marital status, and "other basic data" (left unspecified). The ToU also states that it will collect geolocation and georeferencing data, and that health data related to COVID-19 symptoms for the health evaluation test. The app's Privacy Policy also states the collection of identity data such as name, contact and demographic information. For telemedicine services, additional information may be requested, including for example addresses for sending physical communication.

1.7 NOTIFICATION MECHANISMS

Does the ID system provide adequate user notification mechanisms for this use case? For this test to be satisfied there must be user notification both for use and for any data breach.

The aforementioned decree has no provision for a notification mechanism. The app's Term of Use also has no provision for notification mechanisms, except for the mechanisms of the ToU updates, which states that the ToU can be updated and only cases of "substantial changes" need to be accepted again by the user. No document has reference to an email and phone number that can receive complaints and requests, nor mentions details of procedural processes, such as deadlines or administrative decision revision cases.

1.8 RIGHTS TO ACCESS

Do individuals have rights to access, confirmation, correction and opt out? For this test to be satisfied, individual holders' rights to their data are adequately guaranteed, even though they are not permitted to opt out of the system entirely.

The aforementioned decree does not provide provisions of rights to access.

1.9 REDRESSAL MECHANISMS

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the use of identity data? For this test to be satisfied there is a need for an adequate redressal mechanism, whether it is through the legislation governing this specific use, or through other laws such as the data protection law.

No redressal mechanism is mentioned in the aforementioned decree nor in the app's Terms of Use.

2. RIGHTS BASED TESTS

This section identifies key rights-based principles related to privacy and digital ID use.

2.1 DATA MINIMIZATION

Are principles of data minimization followed in the collection, use, and retention of personal data for this use case? For this test to be satisfied, there are rules in place to determine the appropriate amount of data to be collected and its retention period.

In general, the SaludEC does not address data minimization concerns.

The app's Terms of Use lists the personal data collected during the registration process (i.e. home address, emergency contacts, date of birth, sex, marital status). However, it includes the option to collect " other basic data". Full registration is also mandatory to gain access to the app. These are practices that go against data minimization principles.

The ToU also lists geolocation and georeferencing data collection, but gives no specific limitation to the use, access and collection of the data.

2.2 ACCESS TO DATA

Does the law specify access that various private and public actors have to personal data in this use case? For this test to be satisfied there should be mandates to control access to data.

The aforementioned decree does not specify who has access to the collected data, including location data collected with the use of satellite and mobile telephony services. The app's privacy policy has nonetheless a provision that forbids information sharing without user's consent, unless when required by court order.

2.3 EXCLUSIONS

Is the use of digital ID to access services exclusionary in this use case? For this test to be satisfied

individuals should be allowed to use other forms of ID, as well as given greater say in controlling the access to their data.

The app makes registration mandatory to app users, which includes having a valid national ID and having a device's location set within the country's national territory. This means that foreigners, Ecuadorean nationals located outside the country, or those who do not have a national ID are excluded from all the app's functionalities.

Also, although the app is free to download and use, users must have internet access, and data plans to use it.

3. RISKS BASED TESTS

This section is centred on the perceived or existing risks related to privacy, welfare, equality and inclusion. Such risks usually have limited legal provisions, though there is now an increasing focus on harm assessments in prominent frameworks such as the GDPR.

3.1 RISK ASSESSMENT

Is this use case regulated taking into account its potential risks? For this test to be satisfied the use of digital ID must be accompanied with a proper risk assessment.

There is no publicly available information demonstrating that the government did a risk assessment before launching the app.

Running and releasing the app's Risk assessment would allow accounting for tangible harms to individuals, have clear provisions on prevention and appropriate recovery for harms if they occur. It should also take into account risks of profiling, surveillance, human execution errors, and unauthorized uses.

3.2 PRIVACY RISK MITIGATION

Is there a national data protection law in place? For this test to be satisfied there should be the presence of a robust data protection framework that governs specific personal data to adequately reduce the risks.

Ecuador does not have a national data protection law in place, but its Constitution has provisions for confidentiality of both personal information, and health-related data. The Constitution states that health-data can only be shared within personal authorisation, or as required by law (Article 66, paragraphs 11, 19 and 20).

The country's criminal law also has provisions for protecting personal and confidential information[10]. As a result of the pandemic, the country has issued infra-legal regulation to cope with COVID-19 health emergency data, in general[11].

3.3 DATA BREACH

For this test to succeed, privacy by design systems should be in place to minimize the harms from data breach.

None of the documents analysed (executive decree n° 1017, SaludEC app's ToU and the general provisions of the Ministry of Health website privacy policy - MSP) refer to systems in place to minimize the harms from data breach. The ToU does mention aspects related to that, such as the provision to store health data in a dedicated data infrastructure, but ignores other clear liabilities, such as data encryption and data breach notification systems.

The MSP's privacy policy only undertakes keeping user information secure through "advanced" and "constantly updated" systems to ensure that there will be no unauthorized access (Use of the information collected).

3.4 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure or breach of the ID system?

There are no mitigation strategies to address failure in case of a breach of the ID system, or linking of personal data to sensitive information related to users' healthcare data.

---

1. https://www.ecuadorencifras.gob.ec/estadisticas/

2. This was already possible digitally but it was staggered through the app. See more in: https://www.telecomunicaciones.gob.ec/casi-2-millones-de-ecuatorianos-recibieron-atencion-a-traves-de-las-herramientas-tecnologicas-implementadas-para-enfrentar-al-covid-19/

3. https://www.telecomunicaciones.gob.ec/casi-2-millones-de-ecuatorianos-recibieron-atencion-a-traves-de-las-herramientas-tecnologicas-implementadas-para-enfrentar-al-covid-19/

4. For a detailed description of the tests, see https://digitalid.design/evaluation-framework-02.html. For an applied version of the test in the health sector, see https://digitalid.design/evaluation-framework-case-studies/healthcare.html

5. Health-related information cannot be used without the authorization of the data owner or their representatives, except for medical care (Constitution Article 66, paragraph 11).

6. The SaludEC Terms of Use accessed from an app store is different from the privacy policy that users are asked to accept when registering on SaludEC's first screen. The former refers to the SaludEC app specifically while the latter establishes a generic privacy policy for the Ministry of Public Health of Ecuador online services users.

7. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Decreto_presidencial_No_1017_17-Marzo-2020.pdf

8. “Artículo 11.-Para el cumplimiento de las restricciones del presente Decreto se podrán utilizar plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena sanitaria y/o aislamiento obligatorio, que incumplan las restricciones dispuestas, a fin de ponerlas a disposición de las autoridades judiciales y administrativas competentes.”Apud.

9. On March 20, 2020, the Ecuador Constitutional Court (CC) issued its favourable opinion of Constitutionality of the Executive Decree 1017 (Dictamen 1-20-EE/20A). However, the CC requested caution in the use of technological means to monitor compliance with the restrictions indicated in the executive decree.