Supported by a grant from
OMIDYAR NETWORK

Perú en tus manos

During the COVID-19 crisis, the Peruvian government launched three main digital initiatives: (i) the app *Perú en tus manos*, to monitor cases of coronavirus in the country; (ii) the platform of self-evaluation to assess symptoms, to take on or rule out cases; and (iii) the platform developed by the National Institute of Health to consult the results of patients who were tested for COVID-19. Our case study addresses the role of these three activities, focusing on the app, and discussing the two platforms whenever relevant to our overall assessment.

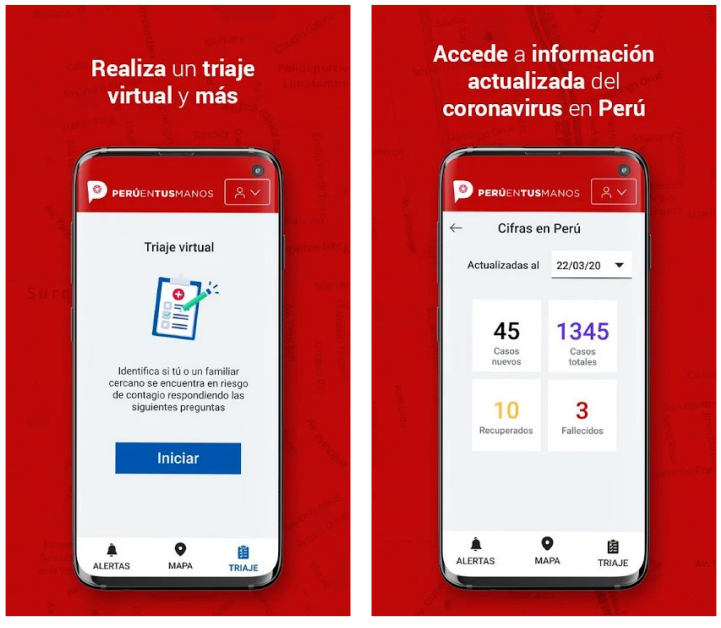
The app *Peru en tus manos* was launched as a part of the digital strategy designed by the multisectoral Working Group "Te Cuido Peru" led by the Ministry of Defense, which aims to provide assistance to people affected by COVID-19[1]. The app is managed by the Digital Government Secretary and has three main objectives: (a) to alert citizens about the various risk areas with affected population; (b) to provide a mechanism for self-diagnosis of citizens' symptoms; (c) to give guidance and information on the advance of coronavirus in Peru. The app is available for Android, Huawei and Apple operating systems and had been downloaded more than one million times before May 14, around 3% of the overall population of 31.99 million people.

The main benefit for citizens using the app is to perform a self-diagnosis assessment, be aware of the most infected areas in the country with COVID-19, and to report back their health status if needed. Users are invited to perform a daily follow-up on their condition in the app, and, if necessary, receive telemedicine support by on-call health specialists. As for the government, the main benefit in using the app is to gather geolocalized health data generated by citizens, generate heat-maps and use the intel to organize prevention measures. The app also provides emergency call-lines for users to ask for assistance, and help with symptoms.

User registration is mandatory for accessing the app. Identity data required during the registration process include national ID and a mobile number for Peruvians. As for foreigners it requires a mobile number, nationality, and either a passport or CE number. The app collects other types of personal data, such as GPS and Bluetooth records, which can be used to infer the user's geolocalization, and other individuals who have been in proximity with the phone (i.e. contact-tracing)[2].

In the app's Terms of Use (ToU)[3] it is stated that all information collected by the app are treated anonymously, and that all data uses are done accordingly to the country's data protection framework. The ToU also sets data use restrictions, such as a limitation to use the data for health purposes and for the duration of the COVID-19 crisis only. However, this is still insufficient, considering that ToUs can be changed unilaterally and without notification.

The app was developed in association with private sector experts in mobile applications, artificial intelligence and data analysis, as well with national and international academic experts.



APPLYING THE FRAMEWORK

We apply below an evaluation test framework to understand the governance of digital identity systems, developed by the Center for Internet and Society (CIS). This test identifies the case study characteristics and its uses, and has been applied to other cases of digital identity in other regions, themes and contexts[4].

TEST SUMMARY

Broadly speaking the *Perú en tus manos app* has a limited legal mandate, meaning it has some provisions of rights-based principles such as data minimization and no risk assessment or potential harms mapped.

- The app operates without a specific legislative mandate. It was backed by emergency decrees, which has basic and generic definitions about the app's purpose and uses.
- The app has limited provision of rights-based principles, such as data minimization, access to data and mitigation mechanisms. Even though the decree is silent on those issues, the ToU addresses that the control over data will only last during the State of Emergency declared by the government or until user consent is revoked.
- In terms of risk assessment, the app has no mapped potential harms to individuals and society.

LESSONS LEARNED

- **The lack of a specific legislative mandate backing the app is a danger for data protection.** Without a codified act, use restrictions, such as defining purposes and data limitations to use the data for health, are subjected to the ToU's unpredictability. Instead, in Peru, these can be modified unilaterally without notification to users.
- **The association of geolocation and health data poses a risk for users.** In Peru, the application seeks to solve two issues at once: to map potential COVID-19 patients and to provide telemedicine support. From a digital identity and identification perspective, this is concerning because it allows the profiling of individuals, and may also compromise sensitive information related to users' intimacy.
- **Requiring geolocation data to access the app is a risk.** The application, by itself, provides important health information to users, it gives guidance on the spread of coronavirus in Peru. Conditioning basic health data to the provision of geolocalization increases the risk of exclusion.
- **The legal mandate sets a temporary mandate for the app's use.** The legal mandate that backs the app sets that the government mission only continues during the suppression of the COVID-19 spread. This sets a time limit for the legal mandate, meaning that when the spread is over, the mandate is also over. This is a good practice that sets limitations for the exceptional use of identity data and geolocation data collected by the app. That said, the limited provisions set by the legal mandate are not observed in the policy implementation, meaning that most likely the app was designed and used as a permanent (not temporary) public policy.

1. RULE OF LAW TESTS

Below are most basic tests to ensure that a rule of law framework exists to govern the use of *Perú en tus manos*.

1.1 LEGISLATIVE MANDATE

Is the use of digital identity system 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 *Perú en tus manos* app is limited.

The app is not backed by an enacted law, and is supported instead by the presidential decree issued on April 14, 2020, that institutes the Working Group "Te Cuido Peru" (Supreme Decree 068/2020), and by another issued three days later (Supreme Decree 070/2020) that provides complementary measures on geolocalization.

The decrees set two main legal frameworks to support the app's use: the constitutional provision for government initiative on health policies (namely Const. Art. 7 and 9) and the federal law provision for health

action (Statutory Health Law, No. 26842/97). In terms of data protection legislation, the decrees make direct mentions to the Data Protection Law (Law No. 29733/11, article 14), the National Digital Transformation System (Emergency Decree No. 6/2020), and the Digital Trust Framework (Emergency Decree No. 7/2020).

The Peru en tus manos app is not cited directly by the documents, but the Supreme Decree 68/2020 ("DS 68/2020") which establishes that the Working Group will have a digital platform in charge of providing geolocalization of people (Article 3, subsection 3.10), while the Supreme Decree 70/2020 ("DS 70/2020") authorizes the Digital Government Secretary, the entity that runs the application, to receive anonymous patient data from the health authorities (Article 4, subsection 4.3).

There is, however, no provision in the decrees of the conditions and circumstances in which the authorities are empowered to resort to the app, nor gives provisions against its abuse related to the collection, storage, use, or sharing of the digital ID information.

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 both decrees is ultimately to promote and protect citizen's health by stopping the spread of the virus.

The DS 068/2020 stipulates additional measures to ensure compulsory social immobilization. The document contains general prerogatives that allow monitoring and clinical surveillance to the fulfillment of the purpose of the Working Group (Article 3, subsection 3.10). The DS 070/2020 states that given the high dissemination risk of COVID-19, it is necessary to identify and accompany confirmed or suspected cases. According to this, the collection and treatment of personal data (geolocalization) would be justified.

This is aligned with the use of identity data by the app. The ToU emphasizes that the collection of data is an important contribution to provide information and help users face the current public health emergency (regarding COVID-19 related symptoms), as well as alerting users on the areas with higher risk of contagion. Broadly speaking, both decrees are supportive of the app's general purpose.

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.

Neither the first nor the second decree mentions the specific purpose of the app. Specifically in terms of Digital ID data, there is no reference to the nature of data required to fulfill the app's legitimate aim, nor does it mention eventual abuses related to surveillance, or the limit of personal data collection or retention. Both documents touch briefly on generic reasons for monitoring and collecting data, without setting out a clear and detailed purpose.

In the ToU, the purpose of the app is clearly defined and mentions specifically that the data collected will be treated merely for the purposes stated, such as provide information to prevent spread of COVID-19; establish a telemedicine channel; keep a record for statistical and profiling reasons; and attend to users questions.

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.

Neither of the decrees specify which actors can use or manage the app. The DS 68/2020 vaguely defines that the Working Group will come up with a geolocalization platform, without further specification. Likewise, the DS 70/2020 only states that the Secretary of Digital Government is responsible for supervising the use of technologies in platforms and applications (Article 5.4). There are, however, no obligations or specific restrictions to actors using or managing the app in the legislation.

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.

The Decrees do not include provisions for private sector actors using the data, other than those involved directly in public sector activities. Additionally, the ToU merely states that the data will be stored in Google Inc. servers.

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 ID must be accompanied by clear specification of the personal data to be collected and processed.

The decrees do not define the nature of collected data nor make any mention to data specification. There are only generic mentions about allowing the collection of geolocalization data, without further specification.

The ToU lists the data collected during the registration process (i.e. government ID card number, zip code and phone number), geolocation of mobile phone (obtained through GPS and Bluetooth records), and health-related data (i.e. symptoms, medical history and diagnostics). During the app's use we also identified additional data (not mentioned in the ToU) being collected[5], including the collection of Bluetooth records, which was only implemented by the government for contact-tracing later on[6].

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 app's Term of Use has provisions for setting a generic notification mechanism for data collection. The ToU makes reference to an email that can receive complaints and requests on data protection (Section 10), but apart from that brings no mention of procedural process details, 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 legal mandate provides no specific provision of rights to access. Section 10 of the Terms of Use however does mention that data owners can exercise their access rights of ratification, cancellation, opposition or even withdraw consent granted at any time by contacting a government agency by email, as indicated in the document, but provides no detailed mechanism for rights to access *per se*.

1.9 REDRESSAL MECHANISMS

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

No redressal mechanism or access and correction of information is mentioned in the decrees.

The ToU states that in case the user considers that their rights were violated, they can submit a claim to the National Authority of Personal Data Protection through email (Section 10).

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, Peru en tus manos addresses some data minimization concerns.

The ToU lists personal data collected during the registration process (i.e. civil identification number and mobile number) and also collects geolocalization and healthcare related data. Despite not providing much detail, the document does cover what data is collected, and it seems to be the proper amount for the uses established in the ToU. The app also requires access to Bluetooth records, which can be used for contact tracing. Yet, the collection of this type of data was not included in the ToU, nor was the use of this data for contact tracing (but was added later on by the government without proper user notification or consent). All these practices go against data minimization practices at that time.

Finally, sensitive information collected by the app is not described fully in detail in the ToU, sensitive health information is included briefly, such as pre-existing conditions, but without further elaboration. This is also troubling for data minimization practices.

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.

Neither the decrees nor the ToU provide a clear definition of who has access to data. The ToU states that only public service actors can have access to the collected data, under the conditions of following the purpose for which they were collected (Article 5). The control over data will only last during the State of Emergency declared by the government or until user consent is revoked.

Even though there are no provisions regarding how third parties can gain access to data storage and data processing, the ToU states that the data collected will be stored in Google Inc. servers.

Also, in spite of the ToU for the temporary use of data collection and processing, there is no provision for the destruction or anonymization of data when the limit period is over, providing no mechanisms for when and how access to data will be interrupted.

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 current version of the *Peru en tus manos* is not mandatory and is accessible for residents and foreigners, but requires them to have a mobile number from Peru. All the information on the app, including basic health information is only provided after the registration process. This means that those who do not have or do not want to share their identification card and other information are automatically excluded from any application functionality, such as prevention measures or the map with the most affected zones, since these are only available after registration.

Also, the use of the app is conditioned to a data plan for the geolocation tool. There is mention of plans in place with mobile operators to find options to reduce data consumption[7].

As an alternative form of accessing health information, there are the aforementioned (i) platform provided by the National Institute of Health that enables users to access their COVID exam results online; and (ii) the self-diagnostics platform. Those services provide additional support on health information without requiring registration. For both, only the ID number is required as a form of identification.

3. RISKS BASED TESTS

This section is centered on the perceived or existing risks related to privacy, welfare, equality and inclusion. Such risks usually have limited legal provision, though there is now an increasing focus on harms assessment 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 stating that the government did a risk assessment before launching the app. Based on the limited legal provision we found, and the rights based analysis that shows few provisions for data protection, it is unlikely that a risk assessment test had been run before the app's release.

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 presence of a robust data protection framework that governs specific personal data to adequately reduces the risks.

In Peru, there is in place a Personal Data Protection law 2011 (Law 29733/2011). In its Article 13.1, there is provision for information processing policies that are particularly central to Peru en tus manos. It states that "the treatment of personal data must occur in full respect with fundamental rights of users and the rights referred in this law. The same applies to its use by third-parties". Peru also has in place the National Digital Transformation System and the Digital Trust Framework to prevent digital risks.

Despite the legal framework in place, DS 70/2020 raised some criticism due to the lack of clear rules for the processing of personal data of those who report symptoms to the State via telephone or Internet[8]. Therefore, even with a robust legal framework to address privacy concerns, there is still privacy risk mitigation provisions to be done.

As it drew international attention due its privacy risks[9], an observation about one of the aforementioned platforms is important here. As stated previously, the National Health Institute of Peru developed a platform where it is possible to consult the health results of patients who were tested for COVID-19 by entering their national identity document and the captcha code. The information was easily accessible as with only the ID number, it is possible that individuals and/or companies can search for private patient data. After receiving criticism, the national authorities included a second authenticator to prevent mass downloads and protect people's information. To connect to the platform, an SMS-based code was introduced.

3.3 DATA BREACH

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

In the ToU there is no specific mention 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.

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 of breach of the ID system, or the linking of personal data to sensible information related to users' healthcare data.