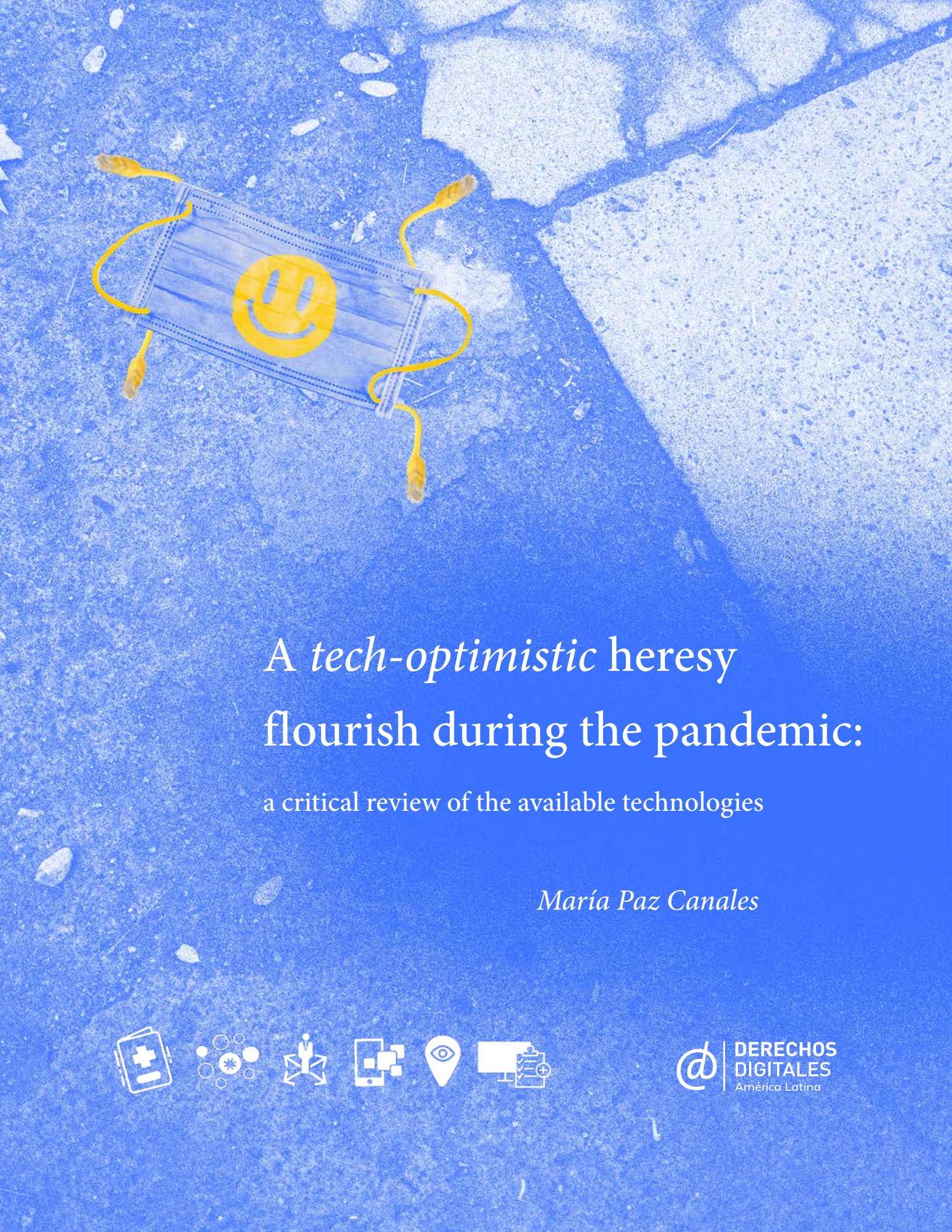

A *tech-optimistic* heresy flourish during the pandemic:

a critical review of the available technologies

María Paz Canales

@ DERECHOS DIGITALES América Latina

A *tech-optimistic* heresy flourish during the pandemic:

a critical review of the available technologies

María Paz Canales

Text by María Paz Canales.
Edited by Vladimir Garay.
Cover and publication design by Constanza Figueroa.
Translated by Rocío López.
The icons "Apps" by Bin Hur, "Network" by Josh Sorosky, "Diagnose" by jeehan@design, "Decision making" by Chrystina Angeline, "Passport" by de Chanut is Industries, "Surveillance" by Max Hancock, "Location" by Adrien Coquet, and "Virus" by mim studio are part of The Noun Project and were used in the designing of this publication.

Originally published in Spanish in June, 2020.
The English version was published in September, 2020.

CONTENTS

As I write these lines from the comfort and privilege of my confinement, in Chile 174,293 infections and 3,323 deaths are registered, and every minute a Brazilian dies from a Coronavirus infection. Around the world, there are already more than seven million infected. America registers the highest number of infections in the world, being the United States and Brazil within the three nations with the highest number of infected people, and more than 150,000 deaths. In Chile, the government organizes the arrival of basic supplies boxes to the population after extending the total lockdown for another week in the metropolitan area and other provinces of the country. Weeks ago, the message HAMBRE[1] (hunger) was displayed in one of the tallest and most symbolic buildings in Santiago.

It has always been said fear is a bad advisor. In the current circumstances, fear of famine and death is real and concrete, even more in a Latin America deprived of social protection networks that assure those who cannot go out to work that they will receive the support that allows them to feed themselves and their families, at least until it is safe to go out again. The combination of a pandemic with precarious economies based in daily incomes, and health services in which little investment has been made, are the ingredients for a perfect storm.

The techno-optimistic heresy finds fertile ground in the fear and the systemic complexity of the problem described above, rooted in the structural weaknesses of Latin America. It is much more difficult to envision ways to overcome them than being seduced by the utopia of a technical shortcut that offers us to isolate at least part of the problem -allowing us confronting the monster by parts- and that even offers us to depoliticize the discussion.

And why techno-optimistic heresy? Through this lines I will try to explain why placing the trust in the ability of technology to provide useful and efficient solutions in the context of a pandemic contradicts the principles and established rules of science, which requires solid evidence before embracing the effectiveness of a solution or establishing the causal relationship between an action (technological intervention) and its effect (mitigation of the pandemic).

1 24 Horas, Estudio lumínico que proyectó "Hambre" en edificio de Telefónica acusa censura y anuncia recurso de protección, 20 de mayo de 2020, available at: <https://www.24horas.cl/coronavirus/estudio-luminico-que-proyecto-hambre-en-edificio-de-telefonica-acusa-censura-y-anuncia-recurso-de-proteccion-4190598>

A basic typology

After weeks of following and participating in discussions with experts from multiple disciplines, and without intending to be exhaustive, I propose to classify the different roles[2] that technology has been assigned in the framework of pandemic control, according to their degree of intrusiveness in the exercise of people's rights, ordered from the least to the greatest:

- Health information
- Self-symptom check
- Integrated data for public health policy decision making
- Contact traceability
- Mobility and work passports
- Confinement enforcement

Each of these spheres has a range of technological implementation possibilities, and each has been subject to different levels of scrutiny by experts from different disciplines. They also awaken a diversity of reactions from citizens, who have seen them proliferate in their different local contexts, and different impacts on the exercise of human rights that deserve to be evaluated.

2 I have arbitrarily excluded those categories referring to improvement of diagnostic capacity (development of rapid tests, diagnostic capacity through AI), palliative treatments (retrovirals, palliative drugs, palliative use of plasma) and health infrastructure (ventilators, masks, safety suits) all these specific technologies for health services.

Health information

Regarding the availability of information on Sars-Cov-2, the leadership has been run by the World Health Organization (WHO) through real time availability of proven scientific information —within what the recent experience of interacting with the virus makes possible— about the identified symptoms, treatment procedures, protocols for reducing exposure to infection, advances in immunization and palliative treatments. The WHO has advanced in this work of information coverage through its website, but also with the recent launch of two applications[3] and the integration of chatbot functionalities to messaging platforms,[4] with the aim of providing accessible information to the general public, but also to the health personnel in charge of dealing with a new virus, without prior specific training and facing day by day learning, at the expense of their own lives and their patients.

In our region, the WHO effort is aligned with the information services locally developed by some countries through web pages and mobile applications. This is the case of Argentina, Bolivia, Chile, Colombia, Peru, Uruguay, among others.[5]

On the dark side of this informational function of technology are the disastrous actions promoted by irresponsible political authorities, which promote the consumption of products or drugs of doubtful efficacy, putting the health of the population at risk,[6] as well as the thoughtless actions of people who in fear, share false information generating more confusion and anguish about the origin,[7] the risks of contagion,[8] the geopolitical spread of the virus[9] and possible palliative remedies.[10] Opposing to these villains of information in a pandemic -or infodemic[11] as it has been called- the other side is offered by the information verification efforts and digital literacy efforts to develop critical skills in the consumption of information by the population de-

3 Available in: <https://www.who.int/es/news-room/detail/13-05-2020-launch-of-the-who-academy-and-the-who-info-mobile-applications>

4 See The World Health Organization launches WHO Health Alert on WhatsApp, available at: <https://www.whatsapp.com/coronavirus/who>

5 Alex arguelles, ¡El tecnoptimismo volvió! En forma de coron-apps, Derechos Digitales, April 3, 2020, available at: <https://www.derechosdigitales.org/14368/el-tecnoptimismo-volvio-en-forma-de-coron-apps/>. Carolina Aguerre, La delgada y móvil frontera de las Corona-Apps en América Latina, Analisis Carolina 30/2020, May 19, 2020, available at: <https://www.fundacioncarolina.es/wp-content/uploads/2020/05/AC-30.-2020.pdf>

6 BBC, Coronavirus: Outcry after Trump suggests injecting disinfectant as treatment, April 24, 2020, available at: <https://www.bbc.com/news/world-us-canada-52407177>. Fernando del Rincón, ¿Por qué Bolsonaro promueve la hidroxicloroquina contra el coronavirus como lo hace Trump?, CNN, May 21, 2020, available at: <https://cnnespanol.cnn.com/video/brasil-eeuu-hidroxicloroquina-jair-bolsonaro-donald-trump-miguel-lago-entrevista-fernando-del-rincon-conclusiones/>

7 Ben Gilbert, A bizarre conspiracy theory puts Bill Gates at the center of the coronavirus crisis — and major conservative pundits are circulating it, Business Insider, April 19, 2020, available at: <https://www.businessinsider.com/coronavirus-conspiracy-bill-gates-infowars-2020-4>

8 EU DisinfoLab, COVID-19 and 5G: A case study of platforms' content moderation of conspiracy theories, April 14, de 2020, available at: <https://www.disinfo.eu/publications/coronavirus-and-5g-a-case-study-of-platforms-content-moderation-of-conspiracy-theories>

9 Max Fisher, Teorías de la conspiración del coronavirus: por qué prosperan y por qué son peligrosas, New York Times, April 13, availabe at: <https://www.nytimes.com/es/2020/04/13/espanol/mundo/coronavirus-conspiracion-fake-news.html>

10 Gianella Tapullima, Curas falsas: los remedios fraudulentos y otras mentiras sobre el Covid-19, Ojo público, April 5, 2020, available at: <https://ojo-publico.com/1730/curas-falsas-los-remedios-fraudulentos-contra-el-covid-19>

11 Marianne Díaz, Desinformacion y salud publica en tiempos de pandemia, Derechos Digitales, available at: <https://www.derechosdigitales.org/14405/desinformacion-y-salud-publica-en-tiempos-de-pandemia/>

ployed by civil society organizations,[12] and even —with greater or lesser success— by private platforms[13] that serve as a means of circulating information.

With all these nuances, the role of technology in facilitating the delivery of information is the functionality of the clearest benefit for the purposes of control and mitigation of the pandemic and, as a general rule, the capacity of technology will function as an amplifier of the previous trust of those who provide the information already enjoy or not. There is no technology that can alleviate the lack of confidence in scientific information or in the political decisions that are communicated through it. In this sense, technological intervention will be as strong as the social legitimacy enjoyed by the senders of the message, be it the press, international organizations, technology companies or national governments.

Self-symptom check

Moving one step further in the complexity of the answers offered by technology, we are faced with web services or applications that aim to collect information on symptoms from the people who use them, in order to generate personalized health recommendations in the format of self-symptom checks.

The possibilities here can range from the suggestion of making an appointment in health services, recommending an action of voluntary social isolation or simply reinforcing general recommendations for hand washing or social distancing. It is about advancing the offer of telemedicine services, which have been talked about for a long time,[14] but are now being developed under the pressure of an ongoing pandemic.

This is when the complexities of isolated technology intervention begin to become more apparent. A technological self-diagnosis tool is a double-edged sword: depending on the information it collects, the way in which the algorithm determines the level of risk and how the decision tree that leads to the different recommendations has been programmed, it can generate a number relevant number of false positives, that is, people who mistakenly believe to be ill and attend health services, saturating them. But there is also an accumulation of false negatives, that is, people confident in the diagnostic capacity of the application that is not tested in a timely manner and engage in risk of contagion with others.

Furthermore, self-diagnosis can only provide a successful strategy in mitigating the pandemic when it is accompanied by the ability to absorb demands for care created by it. The lack of enough testing capacity and health care derived from the massive use of self-diagnostic technology may end up generating additional risks of contagion through the massive attendance of the population to already saturated health services, in addition to a questioning of trust in the system if it proves incapable of responding to the demand created by technology.

Another additional risk that laids in the calibration of the technologies that facilitate self-diagnosis is the effectiveness of the communication that they develop: is their language accessible and clear for all groups of people regardless of their level of education, linguistic diversity, physical limitations or digital literacy?

Finally, the design of the self-diagnostic technologies implemented in the region has been highly intensive in the collection of personal data to generate the personalized recommendations that they deliver,

12 See https://saludconlupa.com/comprueba/un-antidoto-para-la-desinformacion/

13 See https://www.whatsapp.com/coronavirus

14 See The World Health Organization launches WHO Health Alert on WhatsApp, available in: <https://www.whatsapp.com/coronavirus/who>

specifically sensitive health data. The requested information does not only cover current symptoms associated to COVID-19, but also other information on general and pre-existing health conditions, which puts users at risk of not only present but also future discrimination, in relation to access to employment opportunities, access to health insurance and, in general, any activity that considers health conditions as a risk factor.

Even though these applications and services are presented by the authorities in most cases as for voluntary use, in order to fulfill their function they require that they are fed with information that determines the physical, gender and health characteristics of each user. Where does that data go? What conditions are offered to guarantee its exclusive use for COVID-19 diagnosis? How is its security and privacy guaranteed? Self-diagnosis technologies must be evaluated in this integrated framework, not only in their aspects of impact on privacy, but also in the exercise of the right of access to health and non-discrimination in the exercise of other rights, such as those that have been addressed here.

Integrated data for public health policy decision making

In the context of a pandemic, expert voices in data analysis point out that 'light is the best disinfectant' and, therefore, demand that public policy decisions taken to face the pandemic be accompanied by greater transparency from the authorities regarding the information that feeds them. In particular, in Latin America —with governments that are often corrupt, incompetent or with a poor record of rights protection— civil society demands more information about the evolution of the pandemic in order to monitor the decision-making of the authorities.

On the other side, protected by the principle that a greater amount of information contributes to better quality in decision-making, the authorities also seek to make use of their regulatory schemes (some enabled by the declaration of states of emergency and constitutional exception) and its technical possibilities to consolidate and cross-access to public data previously in its possession, although for other purposes, and even access data in the hands of information and communication technology (ICT) companies, to nurture their strategies against the pandemic.[15] The latter, of course, have not wanted to be absent from the effort and collaborate with the available information, to deploy the power of data for good that they already have been exploring since before the pandemic.[16]

So there it seems to be a relative consensus regarding this need to access, cross and share data. What could go wrong? The information to be accessed refers to the most sensitive aspects of human activity: their housing, their forms of movement, habits, their personal networks and their health condition. The access and use of this information requires to be weighed according to the impact on each of the aspects of the lives at stake.

To advance in a proportionate approach to the use of data in the context of public policy, it must start by embracing the purpose of using the data as a guiding principle for its collection. Not necessarily collecting and crossing more data is the most appropriate strategy to achieve better public policy objectives. The data referring to identified or identifiable persons (called personal data) implies high risks not only of privacy, but also of discrimination and impairment in the exercise of other human rights in the present and the future.

15 Orange, Why is (big) phone data so valuable in combatting the COVID-19 pandemic? April 3 2020, available at: <https://www.orange.com/en/newsroom/news/2020/why-big-phone-data-so-valuable-combatting-covid-19-pandemic>

16 See https://dataforgood.fb.com/

Anonymization, which refers to the unlinking of information from the individual identity of its owner in a more or less irreversible way, can be a palliative of the aforementioned risks, but must be carried out properly and must be accompanied by operational security processes, which has been shown to present significant technical challenges.[17] On the other hand, the aggregate or statistical data can be presented with sufficient segmentation or categorization to be perfectly useful for making public policy decisions, in relation to the allocation of health resources, testing capacity or decree of mandatory confinement measures, without putting privacy at risk and considerably limiting the risks of affecting other rights.

Solutions such as DAVID-19, proposed by the Inter-American Development Bank with the global alliance for the development of the blockchain ecosystem for Latin America and the Caribbean (LAC-Chain)[18] follow this line of search for technological alternatives that try to leverage public policies with the data usage. The tool, based on its first stage in the voluntary contribution of information on the health status and the performance of quarantine, works like a survey through a web page and a mobile application.

Presenting itself as an assistance in making better public policy decisions in the region, DAVID-19 aims to "build, without exposing personal data, a regional map of how COVID-19 moves and evolves in real time. The idea is to collect the information provided to understand who has followed the quarantine, who has shown symptoms, and so on".

For the public policy objectives analyzed so far, the quality of the collected data ends up as a fundamental problem and not easy to solve, precisely because of the limitations of the available technology and the social context where these solutions are inserted. As it will be later addressed, when it comes to local context, the quality of public policy decisions based on the collection and cross-checking of data depends on the quality of the data, its precision and its representativeness of the population, and this depends on the conditions of access to technology, both in terms of connectivity and penetration of the specific tool through which the data is collected.

What data is collected by this type of technology? The data coming from connected people, who have their own devices and are digitally literate, the data of vulnerable populations who lack these factors are not taken into account. Thus, what will be the quality of the public policies based on these data? This is essential to be taken into consideration to avoid public policy decisions based on the data collected through these technologies which lead to an additional marginalization of traditionally excluded groups, such as women, children, the elderly, indigenous groups, rural communities, among others.

One of the most appealing data categories that are touched on in this type of technological response is geolocation information, which also plays an essential role in other categories which will be reviewed here, such as contact traceability, mobility passports and confinement enforcement. Geolocation data can be obtained through information collected manually or through information technologies. My address in a national identity registry is information that geolocates me in my residence, but the information from my mobile phone GPS or the cell phone towers that facilitate its connection do so in real time wherever I go.

In the context of a pandemic, the geolocation of individuals with COVID-19 exposes them to direct

17 Montjoye, Yves-Alexandre et al. On the privacy-conscientious use of mobile phone data. Scientific Data. 5. 180286. DOI 10.1038/sdata.2018.286, available at: <https://www.researchgate.net/scientific-contributions/37748419_Yves-Alexandre_de_Montjoye>

18 See https://mellamodavid19.org/

risks of discrimination and even violence.[19] However, geolocation information in aggregate or anonymized form can be not only useful, but also vital for better public policy decision-making that determines economic and health intervention actions for the benefit of the population, and for better decision-making. individual decisions regarding places or times for less risky mobility.[20]

The core then is to understand what for this information is useful and under what conditions,[21] since, as we will review in the following sections, due to its technical limitations, such information has more risks than benefits if it is intended to be used for other purposes, such as contact traceability or confinement enforcement.

It is key to this matter that, in recent times, companies that provide mobile services have begun to develop corporate responsibility policies for human rights protection, principles and practices that precisely aim to facilitate access to geolocation information of its services in a compatible manner with respect for fundamental rights, while being useful for the development of public policies. In the context of COVID-19, the guide developed in this regard by the International Association of mobile operators GSMA stands out.[22]

In our region, problematic cases of attempts to access data in the hands of telecommunications operators by states can be seen in Colombia and Brazil. In the case of Colombia, the Superintendency of Industry and Commerce issued External Circular 001 of March 23, 2020, which authorizes telephone operators to supply information to the National Planning Department and other state entities that require it to "attend, prevent, treat or control the spread of COVID-19 (coronavirus) and mitigate its effects ".[23] The justification for this measure at a local domestic has been the delivery of economic aid from the State facing the emergency.[24] Civil society organizations have rejected this circular, pointing out that it involves risks of discrimination, undue surveillance, invasion of privacy and does not provide minimum guarantees regarding the treatment of said information.[25]

In Brazil, the Supreme Court suspended a government order requiring telephone operators to share customer personal information with the country's statistics agency, allegedly to collect more comprehensive data during the pandemic. Faced with the administratively decreed measure, voices were raised regarding

19 María José Hermosilla, Violencia y discriminación: ¿Qué gatilla la agresividad que muestran algunas personas en medio de la pandemia? Emol, April 23, 2020, available at: <https://www.emol.com/noticias/Tendencias/2020/04/23/984027/Discriminacion-Coronavirus-Chile-Contagiados.html>

20 Mana Azarmi & Andy Crawford, Use of Aggregated Location Information and COVID-19: What We've Learned, Cautions about Data Use, and Guidance for Companies, Center for Democracy and Technology, May 29, 2020, available at: <https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf>

21 Caroline O. Buckee et al, Aggregated mobility data could help fight COVID-19, Science 145-146, April 10, 2020, available at: <https://science.sciencemag.org/content/368/6487/145.2/tab-pdf>

22 GSMA. The GSMA COVID-19 Privacy Guidelines, April 2020, available at: <https://www.gsma.com/publicpolicy/wp-content/uploads/2020/04/The-GSMA-COVID-19-Privacy-Guidelines.pdf>

23 Text available at: <https://www.sic.gov.co/sites/default/files/normatividad/032020/Circular%20001.pdf>

24 Joan López, Ingreso solidario: Un experimento del Estado para evitar discusión política sobre beneficios sociales por COVID 19, Fundación Karisma, May 26, 2020, available at: <https://web.karisma.org.co/ingresos-solidario-o-una-barrera-mas-para-la-exigibilidad-de-beneficios-sociales-en-tiempos-de-pandemia/>

25 Organizaciones de la sociedad civil rechazan circular de la SIC sobre uso de datos personales para controlar la pandemia, available at: <https://web.karisma.org.co/organizaciones-de-la-sociedad-civil-rechazan-circular-de-la-sic-sobre-uso-de-datos-personales-para-controlar-la-pandemia/>

the lack of proportionality and transparency regarding the use of the information,[26] which was confirmed in the decision of the Supreme Court that considered the measure contrary to the constitutional protection of personal data, specifically targeting the lack of clarity of the purpose using the data to which the measure gave access and of safeguards in its handling.[27]

It is crucial what ICT companies are able to offer in terms of transparency about the information that is requested by governments and delivered to the authorities in the context of a pandemic. Following the Guiding Principles on Business and Human Rights developed by the UN in 2011, companies must be governed in their actions by three axes: "protect, respect and remedy." For the effective validity of this mandate, corporate transparency is essential, covering the actions of ICT companies, which use people's data as a basic input.

In recent years, some ICT companies have developed the practice of publishing transparency reports, which has been a useful tool for users to understand the challenges and threats in protecting their rights. In the context of a pandemic, in which requests for access to data from users of some of these companies are proliferating, mobile service operators have begun to develop specific transparency[28] reports. It is particularly interesting to know what path other technology companies such as Google[29] or Facebook[30] will take, which through their services and applications, collect abundant geolocation information, which is also being demanded or voluntarily provided to different governments and scientific communities.

If cooperation is sought through the delivery of aggregated data by ICT companies to the states, this should be done under transparency policies in which users are informed in advance what aggregated data is being considered to be delivered to the authority, in addition to open channels of dialogue that allow questions and doubts to be resolved. The information provided to the public must be sufficient to allow them to understand what is the usefulness of the data that is being disclosed, what are the safeguards taken to protect individual privacy of users, to whom access to the data will be given and under what security guards. There is also a responsibility of companies to ensure that the data is representative of all segments of society, or, if not, this is made explicit to avoid being erroneously used for the purpose of making public policy decisions that lead to further marginalization we have talked about.

Contact traceability

Most of the analysis and discussion have focused on this limited segment of technology solutions. At this point, it is possible to assume a certain degree of familiarity of the audience with the concept of contact

26 OAB ingressa no STF pela inconstitucionalidade da MP que promove quebra de sigilo de dados telefônicos, AOB, April 20, 2020, available at: <https://www.oab.org.br/noticia/58071/oab-ingressa-no-stf-pela-inconstitucionalidade-da-mp-que-promove-quebra-de-sigilo-de-dados-telefonicos>

27 Rafael Zanata y Mariana Marques Rielli., "Please do not share": Brazilian Supreme Federal Court rules in favor of privacy, Access Now, May 14, 2020, available at: <https://www.accessnow.org/brazilian-supreme-federal-court-rules-in-favor-of-privacy/>

28 Telia Company, freedom of expression and the right to privacy in times of covid-19 – up-dated information on related initiatives and government requests. Up-date june 1st 2020, available at: <https://www.teliacompany.com/en/sustainability/responsible-business/freedom-of-expression/#ts-section-74004>

29 Karen Hao, How Facebook and Google are helping the CDC forecast coronavirus, MIT Technology Review, April 9, 2020, available at: <https://www.technologyreview.com/2020/04/09/998924/facebook-and-google-share-data-to-forecast-coronavirus/>

30 See Covid-19 Mobility Reports, Google, available at: <https://www.google.com/covid19/mobility/>

traceability, but it is worth to remember that this is a technique that allows identifying the close contacts of an individual who has been diagnosed as a carrier of an infectious disease, to be able to take health actions regarding such contacts in order to limit the risks of continued transmission of the disease. It is a long-standing method of application for epidemiology, through manual contacts made by human notifiers, through face-to-face or telephone interviews.

Contact tracing apps are nothing but the technologicalization of the traditional epidemiological traceability activity. However, what they do is precisely separate the traceability activity from human contact, which has always been essential for the success of such strategies, since they rely on the knowledge and training of specialized health personnel and the possibility of contextually understanding the information that the interviewees provide, to more accurately measure their probability of contagion.

The apps that are created to generate notifications of exposure of potential contacts that may be infected with COVID-19 replace human criterion with an algorithm that defines a potential risk score, based on variables such as the distance of the contact, the time of the exposure, the repetition of the contact and the time elapsed between the diagnosis and the moment of exposure of the contact; based on this risk, they make recommendations for health actions for the user, such as staying in preventive quarantine, taking a test, attending a health service, among others.

This model seems quite attractive so far, but if each of the previous components is analyzed, the limitations of these technologies emerge. First, to be truly effective, a high adoption by citizens is required; specific scientific studies indicate that between 40% and 60% of the population must use them in order to have a relevant impact on the health strategy,[31] even though lower rates would be useful in cases where they are applied along with other traditional strategies.[32] This is problematic from the outset, considering the availability of internet connection, smartphones and digital literacy among the most vulnerable sectors of the population in Latin America and other less developed countries. Does it make sense to invest in developing this technology to cover only the most privileged sectors of society making historically marginalized groups invisible through the collected data?

Second, Bluetooth[33] is the technology that has gained greater acceptance for the development of these apps so far -basically because not only GPS[34] but also the information from cellphone towers lack precision to measure contacts of less than two meters, which is the relevant distance for COVID-19 transmission.[35] Specifically, the Bluetooth low energy (BLE) protocol has been considered for the development of contact tracing solutions due to its precision and energy saving, but it must be taken into consideration that,

31 Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, Christophe Fraser, Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science08, May 2020, available in: <https://science.sciencemag.org/content/early/2020/03/30/science.abb6936/tab-pdf>

32 Patrick Howell O'Neill, No, coronavirus apps don't need 60% adoption to be effective, MIT Technology Review, June 5, 2020, available at: <https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/>

33 See Privacy International, Bluetooth tracking and COVID-19: A tech primer, 31 de marzo 2020, available at: <https://www.privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer>

34 National Coordination Office for Space-Based Positioning, Navigation, and Timing, Official U.S. government information about the Global Positioning System (GPS) and related topics, GPS Accuracy, April 22, 2020, available at: <https://www.gps.gov/systems/gps/performance/accuracy/>

35 Jay Stanley & Jennifer Stisa Granick, The Limits of Location Tracking in an Epidemic, ACLU, April 8, 2020, available at: <https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf>

despite having been developed since 2010, version 5.0 with the longest signal range is only present in the most modern smartphones, manufactured from 2017 onwards.[36]

Furthermore, Bluetooth technology is not safe from inaccuracies.[37] Just activating it on your phone makes your neighbor's cell phone or speakers detected, even if they are separated by a wall and they have seen each other during quarantine so far. So, even this technology yields multiple false positives, which could end up collapsing health services, as well as multiple false negatives, which can generate a placebo effect that results in a detrimental impact on the population, which, trusting in the use of the app, ends relaxing other essential measures, such as social distancing or hand washing.

Third, for the operation of these apps it is possible - although not necessary - to collect a large amount of information from their users, which depends on their design and commitment to respect privacy, and their exclusive use for the purpose of pandemic mitigation. This is where the issue gets considerably tangled up and has been poorly handled by those who have been promoting the use of these technologies in many countries. The objective of these apps should be limited to the identification of contact possibilities between people at risk of transmission of COVID-19. For this, it is not necessary to know the identity of the people or their location.

The WHO developed a work in this matter with a multidisciplinary committee of experts, who developed a guidance of ethical principles, technical considerations and context requirements that are consistent with these principles in order to achieve the equitable and appropriate use of these technologies with the purpose of informing public health programs and governments that are considering to develop or implement digital traceability technologies for tracking COVID-19 contacts.[38]

Such principles are useful and help decision-making and were developed taking into account the different technical alternatives available up to now, according to the different technical projects that, against the clock, have been developed around the world to respond to the challenges of the pandemic. Let us briefly examine these different technical alternatives from a critical perspective.

As we have already seen, in addition to their greater granularity compared to GPS and cellphone towers technologies, the protocols developed on the basis of BLE technology —such as those used in Singapore, Australia, the interface developed by Apple / Google and several of the proposed in Europe— achieve privacy protection objectives with greater clarity since they do not collect location information or the identity of the people who use the app that connects them to users. What they do is allow to collect identifiers that are created randomly and stored temporarily and locally on the devices, and are only communicated to the health authority (in centralized systems) or to other users (in decentralized systems) when a user receives a positive diagnosis.

The essential elements of these systems are: (i) devices held by users that generate and store ephem-

36 Alberto García, No todos los móviles tienen el mismo Bluetooth 5: cómo diferenciarlo, ADSLZone, April 1, 2020, available in: <https://www.adslzone.net/2019/04/01/bluetooth-5-funciones-opcionales-diferencias/>

37 Douglas J. Leith & Stephen Farrell, Coronavirus Contact Tracing: Evaluating ThePotential Of Using Bluetooth Received Signal Strength For Proximity Detection, School of Computer Science & Statistics, Trinity College Dublin, Ireland, May 6, 2020, available at: <https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf>

38 World Health Organization, Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, May 28, 2020, available at: <https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf>

eral random identifiers; (ii) a back-end service operator that allows communication between devices and the confirmation of cases of infection through encrypted communications (in the case of centralized models, an authority plays this role and provides more than just back-end, adding information storage and filtering); and, (iii) an app that allows communication with users. It is usually conceived that an authority is in charge of this component, in order to make it part of the pandemic capabilities response, allowing the calibration of the computed risk and the health recommendations accordingly.

Let's briefly review the variants of BLE-based exposure notification or contact tracing protocols that have been proposed, with particular emphasis on the discussion of the benefits and risks of decentralized, centralized, or hybrid solutions, as well as the growing discussions about interoperability as an essential condition for their success and contribution to mitigating the pandemic.

Without being exhaustive, the main decentralized protocols that have gained notoriety in the search for exposure notification systems are up to date: DP3T,[39] developed by a consortium of European academics; PACT,[40] developed by a consortium of academics from the United States; the application interface (API) developed jointly by Apple and Google,[41] developed as an interoperability effort by the tech giants; and TCN Protocol,[42] also developed in the United States by a coalition of security experts. The basic components of all these solutions are the same as those already described and they all operate in a decentralized way, that is, the storage of ephemeral identifiers occurs locally in the devices and, in case of infection diagnosis, the identifiers of the infected person are transmitted so that the devices of those who have been exposed to contact with the device of the diagnosed patient can recognize them and, according to the computed risk, generate a notification to its owner.

The main advantages of these decentralized systems are the minimization of collected information (exclusively ephemeral identifiers, but not location, or other information that allows identify users), which prevents abuse of authority through the use of data for purposes other than those related with health; localized and temporary storage on the device for around 15 days, according to the epidemiological relevance determined to date, thereby preventing the possibility of malicious monitoring of infected people; and that the system ensures its automatic dismantling since there is no data stored centrally, with which, if there is no longer people infected, there will no longer be any information available to feed the system. On this last point, it is necessary to draw attention to the fact that, according to what has been reported by the companies, the API offered by Apple / Google allows a regional disabling of its functionality by design.

All decentralized solutions require an interface to users through an app that communicates with them. In the case of the solution provided by Apple / Google, the companies have chosen not to take over this component of the system, leaving the responsibility for such developments to the local authorities. This option opens the door for local governments implementations to incorporate other information gathering requirements into their apps that exceed the design and privacy preserving characteristics presented by the

39 Carmela Troncoso et al. Decentralized Privacy Preserving Proximity Tracing. May 25, 2020, available at: <https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf>

40 Justin Chan et al. PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing, May 7, 2020, available at: <https://arxiv.org/pdf/2004.03544.pdf>

41 Apple & Google, Privacy-Preserving Contact Tracing, April 2020, available at: <https://www.apple.com/covid19/contacttracing/>

42 TCN coalition, TCN Protocol, April 2020, available in: <https://github.com/TCNCoalition/TCN>

model explained here.

Even though Apple / Google present terms and conditions of use that are intended to shield the use of this technology in ways that are not aligned with privacy protection in their API[43] - they require voluntary use, not for other purposes, ban discriminatory use, establish a technical impossibility of accessing the location of the devices and automatically accessing the contact list—, it remains to be seen what will be the effective adherence of local authorities to such conditions, as well as what will be the actions of companies to ensure due respect to such conditions when the implementation of applications under this technology begins to be deployed.[44]

Among the centralized protocols that have been deployed to date, the most notorious is BlueTrace,[45] adopted by Australia (CovidSafe) and Singapore (TraceTogether), also based on the collection of BLE signals, but with centralized registration and storage by the health authority of the identifiers associated with a phone number. An interesting element of centralized models like this one is that they allow to combine the information from the app with others gathered from the interviews carried out through the manual identification of contacts.

The protocol works as follows: users transmit random IDs and collect IDs in their proximity. Then, upon receiving a positive diagnosis, the user reports the authority all identifiers collected in her vicinity during the relevant infection window. The authority then alerts the users who generated these identifications. A symmetric encryption system is used for temporary identifications, the key of which is exclusively in the possession of the authority. The user can revoke her consent at any time, eliminating her number from the registry and, with it, the possibility of associating the ephemeral identifiers generated with her identity.

Open Trace is the open source version of the TraceTogether application, originally launched by Singapore, and which was one of the first to be deployed and ignited the debate about the use of mobile applications for contact traceability. Poland is among the countries that have implemented this protocol through its ProteGO Safe app.[46] A recent technical study shows that the application works using the Firebase Analytics services provided by Google, which allows that company to have access to individualized user information, even if it is only shared in aggregate form to the authority.[47]

ROBERT is another centralized protocol based on BLE developed in France, under the premise that, in addition to being a technological solution that preserves privacy, it must be one that allows controlling the possibilities of external attacks on the system that reduce its stability and trust. It was presented as a critical alternative to the security drawbacks caused by external attacks, the main weakness of the decentralized systems examined above, since ephemeral identifications can be artificially generated and injected into the

43 See GoogleCOVID-19ExposureNoticationsServiceAdditionalTerms, May4, 2020, available at: <https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf>

44 When this document was written Germany, Austria, Italy, Grece, Portugal and Switzerland were evaluating possibilities of implementation. In Latin America Uruguay has been mentioned as a potential location to implement.

45 Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, Tang Anh Quy, BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders, Government Technology Agency of Singapore, April 9, 2020, available at: <https://bluetrace.io/>

46 Malgorzata Fraser, Coronavirus contact tracing reignites Polish privacy debate, DW, May 30, 2020, available at: <https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913>

47 Douglas J. Leith & Stephen Farrell, Coronavirus Contact Tracing App Privacy: WhatData Is Shared By The Singapore OpenTrace App?, School of Computer Science & Statistics,Trinity College Dublin, Ireland, April 28, 2020, available at: <https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf>

system in order to make a specific group of individuals appear at risk of exposure and be massively notified (called the risk of "terrorist attack").[48] The protocol is based on a scheme that combines a federated server infrastructure and temporary anonymous identifiers, with the control and administration of risk scores and notifications by the health authority server, which according to its authors provides high robustness, flexibility and efficiency.[49]

Introduced as an evolution of ROBERT, the DESIRE[50] hybrid protocol, developed collaboratively by French and German academics, decentralizes most of the necessary operations in the exposure notification system. The main difference with ROBERT is that secret and cryptographically generated Private Encounter Tokens (PET) are created to encode encounters. The function of the server is simply to match the PETs generated by the diagnosed users with the PETs provided by the requesting users, information that is stored encrypted on the server, but controlled by keys stored in the devices (asymmetric cryptography). This improvement is proposed in order to generate better protection against malicious users and authorities. However, as in ROBERT, risk scores and notifications are still managed and controlled by the server under the control of the health authority.

Finally, although these are not technical protocols per se, but rather the combination of the use of different technologies and information sources, the case of solutions developed in India, South Korea and New Zealand are worth noting. Aarogya Setu is the mandatory app implemented to access workplaces in India. The app uses Bluetooth signals to record contacts in the way described above, but also uses GPS location data to augment the information collected and build a centralized database of the spread of the infection, an approach that most countries avoid for privacy reasons. It also mimics China's health QR code system - which we will examine later - with a feature that rates a person's likely health status in green, orange, or red colors to indicate whether a person is safe, high-risk, or a carrier of the virus. By administrative provision of the Indian Ministry of Technology, the government agency that developed it, the app is free to share personal data from the app with other government agencies and public health institutions.[51]

In South Korea, an app has been implemented that uses the information from cellphone towers to trace contacts and enhance traditional traceability through interviews. The authority combines location data from mobile phones, credit card transaction records and CCTV recordings to track and assess people who may have recently come into contact with an infected person. This has been accompanied by the publication of detailed maps showing precise movements of infected people, encouraging others who may have been in contact with them to undergo tests, but also causing serious social consequences due to the risk of re-identification of infected people.[52]

48 See Ross Anderson, Contact Tracing in the Real World, April 12, 2020, Light Blue Touchpaper, available at: <https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/>

49 PRIVATICS team, ROBERT: ROBust and privacy-presERving proximity Tracing, April 19, 2020, available at: <https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf>

50 Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, Cédric Lauradoux, et al. DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralizedand decentralized systems, May 12, 2020, available at: <https://hal.inria.fr/hal-02570382/file/DESIRE-specification-EN-v1_0.pdf>

51 Sankalp Phartiyal, India follows China's lead to widen use of coronavirus tracing app, Reuters, May 14, 2020, available at: <https://www.reuters.com/article/us-health-coronavirus-india-app/india-follows-chinas-lead-to-widen-use-of-coronavirus-tracing-app-idUSKBN22Q110>

52 BBC, Coronavirus privacy: Are South Korea's alerts too revealing?, BBC News, March 5, 2020, available at: <https://www.bbc.com/news/world-asia-51733145>

New Zealand has adopted an interesting approach based on the principle of amplifying the capacity of human tracers working for the health system. To do this, it mixes elements of the QR technology implemented in China, but the information is not stored centrally, but locally on the users' devices, such as a record of each of the locations that the user visits in which you will need to scan the QR code. If an infection is determined, the information on the visited places will be required by health personnel to cross it with the user record available in the location record. Remarkably, the New Zealand government added a privacy impact assessment to the launch of its app and announced that this will be an ongoing process during the deployment of such technology.[53]

As it can be concluded from this very tight review, all the available technical alternatives involve risks in their operation necessary to calibrate when developing their implementation, and although decentralized solutions have been accompanied by a greater technical consensus due to their privacy preserving characteristics and limitation of the possibility of misuse by authority, when it comes to analyzing attacks of greater sophistication they are not immune to security risks. Likewise, its efficiency will depend on the configuration of the algorithm in charge of determining the risk of infection, which continues to be in the hands of a competent health authority in every case.

Finally, the interoperability of solutions is a component that has become essential in the face of the progressive lifting of restrictive border crossing measures and the proliferation of different technological solutions, even within the same country or region.[54] In Europe, the member states of eHealth Network have highlighted the need for interoperability within the region, and a group of experts working on different decentralized protocols have begun to explore technical alternatives to achieve such interoperability.[55] Discussions of technological sovereignty are mixed in the combination of the different proposed solutions, including the convenience of relying on the technology provided by the American giants Apple / Google, and the proliferation of protocols, both for centralized as decentralized and hybrid solutions add additional complexity to the possibility of achieving interoperability.

However, we agree that interoperability will be the final test of effectiveness that this technology for contact tracing will have to deal with when facing a world that tries to reactivate itself and reach its long-awaited new normality.

Mobility and work passports

Immunity passports look for creating a degree of certainty that allows people to go out and spur economic reactivation, as well as social activities. Its issuing depends on the existence of methods to measure the immunity developed by the population against an infectious disease. Its goal is precisely to discriminate between those who have immunity and those who do not, relating mobility and employment opportunities to that classification. Thus, they seek to impose an artificial restriction on who can participate in social and economic activities, and who cannot.

53 Ministry of Health of New Zeland, COVID-19 Contact Tracing Application, Privacy Impact Assessment, May 15, 2020, available at: <https://www.health.govt.nz/system/files/documents/pages/nz_covid_tracer_pia_18_may_2020.pdf>

54 Ulrich Luckas et al. Interoperability of decentralized proximity tracing systems across regions, May 15, 2020, available at: <https://drive.google.com/file/d/1mGfE7rMKNmc51TG4ceE9PHEggN8rHOXk/edit>

55 Ibid.

That is why experts draw attention to the risk that immunity passports may create a nocive incentive for people to seek infection, especially the most vulnerable, who cannot afford a period of exclusion from the workforce, deepening pre-existing social inequalities.[56] Situations of corruption or institutional weakness in Latin America and other less developed countries could deepen the damage in economic and social rights as a result of COVID-19 in the most vulnerable groups by the use of these types of tools.

China was the first country to implement this type of tool in the context of the pandemic, through a color-coded traffic light system, associated with a QR code that is linked to the identity of each person and that allows to regulate her mobility in public spaces. Having a green code is required to travel from one province to another, and public service buildings and services can condition peoples' access to holding a green code. There is no transparency regarding the risk factors and the weighting that determines the allocation of colors. In addition to storing mobility information, the application records health information declared by the patient and her medical record. The tool is also integrated into widely adopted pre-existing platforms in that country, such as the Alipay payment platform and the WeChat messaging platform.[57] In recent days, some local governments announced their intention to make the system permanent to monitor the health of their population within their city.[58]

Recently, as an addition to the previously deployed technologies in South Korea since the onset of the pandemic, the disease and disaster control authority announced its plan to introduce an electronic registration system through QR codes to maintain monitoring of COVID-19 patients, to control entry into facilities considered high risk for the spread of SARS-CoV-2, including entertainment venues. Civil society in that country has expressed concern that the government is trying to establish a more comprehensive surveillance and control system in the name of preventing the epidemic.[59]

In the UK, public-private initiatives have been announced to develop epidemiological passports based on facial recognition technology.[60] The app developed by the UK health service already allows its activation through facial recognition, for which it requires users to send a photograph of themselves from an official document, such as their passport or driver license, to load to the database that could be used for immunity passports.[61]

The WHO has expressed concern about the development of immunity passports, noting the insufficient information about the development of antibodies to SARS-CoV-2, with the risks of misclassification in the immunity levels of the population that could imply. Through this type of certifications, a wrong message about immunity of the population may end up being communicated in the event of a second wave of infec-

56 Alexandra L Phelan, COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges, The Lancet Vol 395, May 23, available at: <https://www.thelancet.com/action/showPdf?pii=S0140-6736%2820%2931034-5>

57 Helen Davidson, China's coronavirus health code apps raise concerns over privacy, The Guardian, April 1, 2020, available at: <https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>

58 Helen Davidson, Chinese city plans to turn coronavirus app into permanent health tracker, The Guardian, May 26, available at: <https://www.theguardian.com/world/2020/may/26/chinese-city-plans-to-turn-coronavirus-app-into-permanent-health-tracker>

59 Miru Lee, In the era of COVID-19, is S.Korea's 'new normal' a digital surveillance state? Jinbo Net, May 26, 2020, available at: <http://act.jinbo.net/wp/43070/>

60 Kate Proctor and Hannah Devlin, Coronavirus UK: health passports 'possible in months', The Guardian, May 4, 2020, available in: <https://www.theguardian.com/politics/2020/may/03/coronavirus-health-passports-for-uk-possible-in-months>

61 Jane Wakefield, Coronavirus: NHS app paves the way for 'immunity passports', BBC, May 27, 2020, available at: <https://www.bbc.com/news/technology-52807414>

tion, generating the risk that the population could ignore the more general public health advice and, thereby increasing the risks of continuous transmission.[62]

In Latin America, Chile had noticeably announced the preparation of a digital immunity card, however, the initiative was later suspended due to the questions raised from the WHO.[63]

The level of scientific uncertainty about the development of immunity to SARS-CoV-2, as well as the devastating economic and social consequences that the implementation of this type of initiative could have, call for extreme caution in its evaluation, which in case of being implemented subsequently could only be necessary and proportionate if they are developed in a regulatory framework that prevents their use for discriminatory purposes incompatible with human rights. There is vast previous experience from the regulations for the protection of workers' rights about the risks of employment decisions based on health conditions, and that experience will undoubtedly be useful to calibrate the rights at stake. These passports should not result in a social control tool that restricts population mobility in contexts of political dissent or an additional tool to impose abusive restrictions on migration, to call just a few of the potential negative impacts of these implementations.

Confinement enforcement

The electronic bracelet as a formula to control compliance with confinement measures is being used in Bulgaria, South Korea and Hong Kong.[64] In South Korea, the measure appears to be punitive in nature, as it is ordered in the event of detections of prior non-compliance with confinement orders, a situation in which the offender can choose to use the bracelet as an alternative to not be taken to a sanitary residence where compliance with their quarantine is monitored.[65]

In Poland, quarantined people are required to download an app and use it to comply with recurring prompts to take a selfie with a time and place stamp, and then send the photo to the government. Failure to comply with this requirement may result in police intervention at home of the infected person and getting a fine. The data collected by the app is kept for six years and can be accessed by the police, governors, the Center for Technology Information, the National Center for Health Information Systems and the subcontractor developing the application.[66]

In Israel, technology previously deployed by intelligence services against terrorism attempted to be repourposed for quarantine enforcement, within the framework of the declaration of a State of Emergency[67]

62 Immunity passports" in the context of COVID-19, April 24, 2020, available at: <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19>

63 Christian Leal, Gobierno posterga por posible "discriminación odiosa" entrega de polémico carnet Covid-19, Biobio, May 10, 2020, available at: <https://www.biobiochile.cl/noticias/nacional/chile/2020/05/10/gobierno-posterga-por-posible-discriminacion-odiosa-entrega-de-polemico-carnet-covid-19.shtml>

64 BBC News, Coronavirus: People-tracking wristbands tested to enforce lockdown, April 24, 2020, available at: <https://www.bbc.com/news/technology-52409893>

65 Park Han-na, Tracking wristband launched to deter quarantine breakers, The Korea Herald, available at: < http://www.koreaherald.com/view.php?ud=20200427000967>

66 Katri Uibu, Poland is making its citizens use a 'selfie' app during the coronavirus crisis, April 24, 2020, available at: <https://www.abc.net.au/news/2020-04-25/coronavirus-poland-tracking-quarantine-selfie-app/12173884>

67 BBC News, Coronavirus: Israel halts police phone tracking over privacy concerns, April 23, 2020, available at: <https://www.bbc.com/news/technology-52395886>

and, while it was in force, led to the arrest of more than 200 people,[68] before being declared illegal by the Supreme Court. Additionally, drones are used to patrol and verify compliance with quarantines, [69] similar to what would be happening in Paraguay, through the private donation to the Ministry of the Interior of one of those devices.[70]

In Taiwan, a 'digital fence' system was adopted in February, whereby the location of anyone who must undergo mandatory quarantine is controlled via their cellphone signal. The measure has been implemented in the context of the specific regulations in that country for disease control and the government has promised to dismantle the system once the emergency is over, and not to use that data for criminal investigations.[71]

Something similar was announced in Ecuador as part of the Decree through which a state of emergency was declared, in which it was stated that "[in] order to comply with the restrictions of this Decree, satellite and mobile phone platforms may be used to monitor the location of people in a state of sanitary quarantine and / or compulsory isolation, who do not comply with the established restrictions, in order to make them available to the competent judicial and administrative authorities". Civil society in the region reacted with concern to this announcement, noting that this measure is particularly serious in a context in which, despite the guarantee of privacy enshrined in article 66 numerals 11, 19 and 20 of the Constitution, Ecuador lacks of to date a legal regulation and an independent technical authority that allows adequate oversight that the measures to be implemented respect the principles of adequacy, necessity and proportionality compatible with the rule of law.[72]

The use of surveillance technologies to enforce confinement presents a clear question of proportionality in the use of force by the State. Measures that restrict freedom based on a health condition cannot mean an opportunity to restrict public freedom and rights of the affected people, who are not responsible for any crime.

The normalization of these levels of individual surveillance based on public health constitutes a precedent of limitation of freedom that can easily be repurposed in the future for the most diverse goals by the dominant political forces, an issue that will always end up entailing a disproportionate risk of impact on minorities and vulnerable groups, and the threat of replacing democracies with authoritarianism without checks.

68 Maayan Lubell, Israel's top court says government must legislate COVID-19 phone-tracking, Reuters, April 26, 2020, available at: <https://www.reuters.com/article/us-health-coronavirus-israel-monitoring/israels-top-court-says-government-must-legislate-covid-19-phone-tracking-idUSKCN2280RN>

69 Joseph Krauss, Israeli police use drones to enforce virus quarantines, raising privacy concerns, The times of Israel, April14, 2020, available at: <https://www.timesofisrael.com/israeli-police-using-drones-to-enforce-coronavirus-quarantines/>

70 Katri Uibu, Poland is making its citizens use a 'selfie' app during the coronavirus crisis, April 24, 2020, available at: <https://www.abc.net.au/news/2020-04-25/coronavirus-poland-tracking-quarantine-selfie-app/12173884>

71 Arthur Shay, Cell site location information helps digital fencing against COVID-19 pandemic, ILO, April 24, 2020, available at: <https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Taiwan/Shay-Partners/Cell-site-location-information-helps-digital-fencing-against-COVID-19-pandemic>

72 Derechos Digitales, Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos, March 18m 2020, available in: <https://www.derechosdigitales.org/14285/ecuador-las-tecnologias-de-vigilancia-en-contexto-de-pandemia-no-deben-poner-en-riesgo-los-derechos-humanos/>

One App to rule them all

A marked strategy in the different governmental initiatives for technological implementations that have flourished in the region —and in the world— has been to combine different functions from those identified in the proposed typology in one app. There are many applications that range from the delivery of general information on measurements to questionnaires or chatbots that allow interaction for self-diagnosis, and at the same time collect geolocation information through the GPS activation request, which can later be used in aggregate form for public policy decisions, while the most daring are intended to ensure compliance with quarantines.

This packaging approach makes it difficult to clearly identify the risks and benefits of technologies that intended to seduce us. It also makes consent even more problematic in terms of being able to choose among the offered functionalities those that are less problematic. As happens in the field of competition and protection of consumer rights, these packaging should be limited, since it impacts people's agency in a matter as relevant as their health information.

The last worrying issue in this regard is the risk that this packaging formula will include the economic benefits that are being distributed to the most vulnerable populations to ensure their subsistence during the pandemic. Any conditioning of access to social benefits to the download and use of these technologies should be prohibited, as access to the aid of the State is subject to the waiver of rights in a discriminatory manner with the most vulnerable segments of the population, whose consent will be completely void. The same can be said of the conditioning of the use of these applications for the exercise of the right to mobility in public spaces or access to employment opportunities that I have already referred to.

Between the public and the private: human rights as a guiding principle

Geolocation data in the hands of ICT companies suddenly appear covered by public interest and the willingness of companies to collaborate with the authority in the provision of useful data to combat the pandemic must be done under the prism of necessity and proportionality also raised for data in the hands of governments.

The initiative of private companies and the response to the requests from the states must be evaluated within the framework of the United Nations Guiding Principles on Human Rights and Business (UNGP). Some companies, such as those of mobile services grouped in the GSMA, have understood it this way, through the publication of a set of guiding principles on the requirement of user data in the context of a pandemic, to which we have already referred. Along the same lines are the efforts of companies that provide services in Europe that have tried to collaborate with authorities at the local and regional level, but without putting the privacy of their users at risk.[73]

The repurposing of previously supplied surveillance technologies to combat the pandemic is another problematic aspect in public-private collaboration. In the United States, Clearview offers facial recognition solutions pre-developed for public safety purposes to serve as contact tracing. The Clearview AI[74] database is made up of images and data taken from social media accounts, without the explicit permission of their owners.

For its part, Palantir offers data intelligence services to health authorities in the United States and the United Kingdom.[75] While NSO -an Israeli company with a highly problematic record, whose spyware has been used against journalists and activists around the world - proposes to repurpose its surveillance technology towards a new non-military product, which seeks to establish contact tracing through the use of mobile phone geolocation data.[76]

It is quite problematic that these companies attempt to whitewash their image on the occasion of the pandemic by establishing relationships that could be projected over time, through surveillance technologies that can be quickly repurposed to other forms of social control once the pandemic is over, with the advantage of having been installed in the imaginary of the citizenship as protection devices. There is an imperative imposed by the UNGPs on the deployment of these surveillance technologies to be carried out after a human rights impact assessment, which allows companies to satisfy their three pillars "protect, respect and remedy."

73 Joakim Reiter, Correct use of telecom data can help in this crisis, Político, March 27, 2020, available at: <https://www.politico.eu/sponsored-content/correct-use-of-telecom-data-can-help-in-this-crisis/>

74 Jacob Ward and Chiara Sottile, A facial recognition company wants to help with contact tracing. A senator has questions, NBC News, April 30, 2020, available at: <https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291>

75 Thomas Brewster, Palantir, The $20 Billion, Peter Thiel-Backed Big Data Giant, Is Providing Coronavirus Monitoring To The CDC, Forbes, March 31, 2020, available at: <https://www.forbes.com/sites/thomasbrewster/2020/03/31/palantir-the-20-billion-peter-thiel-backed-big-data-giant-is-providing-a-coronavirus-monitoring-tool-to-the-cdc/#96059961595a>

76 Gwen Ackerman and Yaacov Benmeleh, Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading, Bloomberg Technology, March 17, 2020, available at: <https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus>

Let's talk about local contexts

The elephant in the room when evaluating the role that technology can play in mitigating the pandemic is precisely the limitations of technology deployment in certain contexts and geographies.

It is not enough for a technology to prove itself useful in its technical capacity. The crucial question when making public policy decisions about its implementation is what are the possibilities and costs of deploying this technology in the short term required by an ongoing pandemic context. Countries that have been struggling for years to reduce their digital divide suddenly fall into the techno-optimistic heresy, ignoring the prevalence of that divide, which spans various layers, from infrastructure to digital skills available in different segments of the population.

Starting with connectivity, the proposed technologies must be suitable for deployment in consideration of internet access or mobile communications, which are intended to be used as the basis for their deployment. With vast segments of the population suffering access restrictions, for reasons of infrastructure, availability of services by commercial actors or low quality of service that interrupts the connectivity, the possibility of technologies to reach the population in the fight of the pandemic narrows.

Going one step further, the same is linked to the availability of devices per individual that allow the information available on it to be associated with its owner. In the world and in every country in Latin America, even those with the highest level of development, there is a non-reduced number of people who, due to age, economic condition, ethnic origin or even gender factors, do not have the possibility of accessing and controlling a device of a personal nature. What will their data say? How can they benefit from a technology that makes them invisible again?

We reach the most human layer of the problem, the digital skills to understand, control and generate trust links with technology are a considerable obstacle for placing it as a central piece in the strategy against the pandemic.

Linked to the factors above, the effectiveness of some of the proposed technologies - particularly those for contact tracing - rests on reaching a high level of penetration in the population, which is unrealistic in all those contexts in which there are considerable barriers in each of the aspects examined here.

It is in this ingredient of the analysis in which the techno-optimistic heresy manifests itself with greater force and clarity: the causal relationship is totally broken in a context in which the multiple existing barriers put a limit to the theoretical utility of technology, forcing to abandon the arrogance of those who preach it, not to discard it, but to relocate it in the modest place of complement that corresponds to it as a contributor to a broader strategy based on the amplification of human capacity.

The political paradigm that creates the pandemic: the risk and the opportunity

Several ones have warned about the fundamental changes that the role assigned to technology in a pandemic is generating in the narrative of the exercise of public freedoms.[77]

The restrictions are dressed in a white suit metaphorically equivalent to the uniform worn by the heroic health workers, in charge of the intensive care of those infected with COVID-19. If the surveillance that goes along with the deployment of technology is benevolent, what difference does it make to use the technology to which surveillance capitalism has already accustomed us, now for a laudable purpose: to preserve the lives of so many people who sail in the dark a sea infested by an invisible enemy.

The previous paragraph goes overboard with metaphors, it does so on purpose. The discourse that surrounds the deployment of technology in the context of a pandemic is so rich in metaphors that it blurs those arid limits that years of work on international human rights standards have tried to plant as a flag. It does not sound so convincing to speak of legality, necessity and proportionality or balancing of rights, when on the other side it is spoken of defeating the invisible enemy all together, of taking care of ourselves together.

We are all needed in the fight, the information collected for other uses by public or private agencies can be redirected to be used against the pandemic, past mistrust in the capacities and probity of the authorities must be put on hold, the confidentiality of health conditions can be relaxed, and companies that previously offered technology to spy on and intimidate journalists and human rights defenders, or to exercise discriminatory control of migrants and ethnic minorities, should be given the benefit of the doubt, since now they will use their abilities for the public good.

A trade-off narrative is set to lead us to normalize surveillance without political color, because we are all necessary in the fight. But this policy of surveillance at the service of the common good has a victim and it is not the virus. The limited capabilities of technology to contribute to the mitigation of the pandemic make them more likely to end up damaging the public liberties in the long term than SARS-CoV-2.

Particularly worrying is that surveillance technologies are deployed under emergency powers that appeal to the logic of war that allow exceptional situations in the balances and controls of those in public power, and that free them from the need to give account, transparency and supervision required in another context. This narrative is not entirely new; after a few years of heavy use in the fight against terrorism post 9/11 we have it back, fresh and reinvigorated by an invisible enemy even easier to fear and hate for his absence of humanity.

Surveillance technology makes it possible to decide who is allowed to participate in public life, who can work, who should stay home, who receives the financial aid that allows them to survive and who does not. None of this is typical of a society driven by democratic principles or respect for human rights. Rather, it seems an echo of the best sci fiction novels that predicted a future of authoritarianism and control in the name of the public good.

The risk is clear that these aseptic narratives about the role of technology capture progressives and neoliberals under the promise of making reality a world in which the authority of the day leads us through technology towards the future chosen for us, by our own good. What is the opportunity then? The one born

77 Evgeny Morozov, The tech 'solutions' for coronavirus take the surveillance state to the next level, The Guardian, April 15, 2020, available at: <https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt?CMP=share_btn_link

from that risk. We have the opportunity not to let ourselves be seduced by the heresy of techno-optimism and to demand more from the contexts that accompany the implementation of technology. No one advocates banishing technologies, but rather giving them the modest place that they deserve, in a political and regulatory context that allows limits to their uses and abuses.

The pandemic has reinforced the ubiquity of technology in our lives and this is the best opportunity to understand the urgent need to reclaim back individual and collective control of technology that is deployed from the public and private sector on our behalf.

A way forward

With the techno-optimistic heresy unveiled, we have to take charge of proposing solid bases so that the use of technology in the context of a pandemic is directed to unleash its maximum potential, however limited it may be, with respect to the rights of people, whose protection must be at the center of the pandemic mitigation strategy.

This requires that, either through ordinary or emergency legislation, technological solutions that use personal data as input in the context of a pandemic be required to satisfy the following components:

1. Strictly characterize the emergency situation and / or the term that enables access to personal and sensitive health data in the hands of the different organs of the State;
2. specify who will be in charge of the extraordinary access to such data;
3. detail what is the data to which extraordinary access is being requested to be used and how. And, if it is collected directly from their holders, that this is done voluntarily;
4. establish provisions for the termination of access and extraordinary use of data, with effective access control or elimination measures, where appropriate;
5. order specific operational security measures to prevent malicious access and use of data; and provide that the use of personal data is done under pseudonymization or disassociation techniques (with sufficiently robust anonymization algorithms) when it comes to offering publicly available information, in addition to having security as an essential requirement, including the encrypted transit of the information and its safe and resilient storage;
6. guarantee the representativeness of the data from which technology is fed and the decision-making of public policies that it feeds, taking into consideration the local contexts that account for the marginalization of vulnerable groups;
7. establish mechanisms for evaluating the technology implemented, in its effectiveness and technical precision, but also in its impact on the exercise of human rights and not just privacy; and,
8. Establish mechanisms of transparency, external control and accountability that allow to control and strongly sanction the deviation of purpose in the access and use of data.

These checks and balances return us to our old and well-known standards of legality, necessity and proportionality in limiting the exercise of human rights, which continue to constitute a positive obligation to promote and protect States in the context of a pandemic. Here the vaccine does not need to be invented, it is available in the international human rights standards of the Universal System and the Inter-American Human Rights system.[78]

78 Comisión Interamericana de Derechos Humanos, Resolución 1/20. Pandemia y Derechos Humanos en las Américas, April 10, 2020, available at: <https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>

Let's not let the techno-optimistic heresy that flourishes during the pandemic confuse us with its perfume.


DERECHOS
DIGITALES
América Latina