TECHNOLOGIES IN THE FIGHT AGAINST COVID19. A COST-BENEFIT ANALYSIS

(This document is a translation from the original in Spanish El uso de las tecnologías en la lucha contra el COVID19)

May 2020

C/Jorge Juan 6 http://www.aepd.es
28001 – Madrid https://sedeagpd.gob.es

I. CONTENTS

II. INTRODUCTION

Before implementing any technological solutions to deal with COVID-19, it is essential that they are integrated into a strategy of realistic, effective legal and organizational measures. Such measures must be proportional, legitimate and based on scientific assessments.

Proportionality is assessed by cost-benefit analysis for the society in general and the rights and freedoms of the individual. The health benefit must be measured based on a real chance to limit the spread of the infection, with the possibility to regain freedom of action, and to protect the health of individuals.

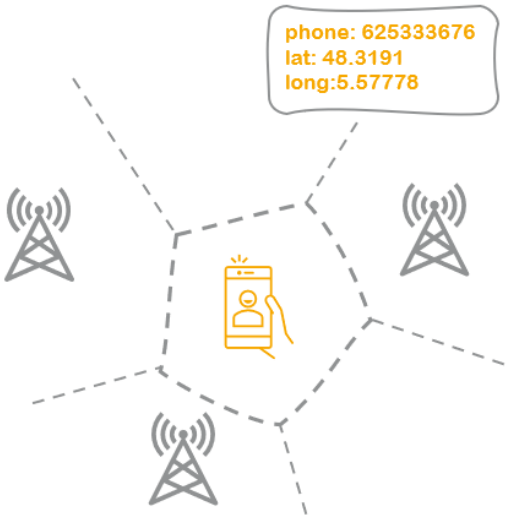
Health data are high value, so it is necessary to prevent abuses from third parties leading to situations of loss of freedoms, discrimination, or other damages. They can harm the personal situation of citizens, taking advantage of the uncertainty feelings caused by an emergency situation.

In this document, a brief analysis will be carried out about some of the technologies in the fight against COVID-19. The purpose is didactic, without pretending to be exhaustive in its assessment. The pretended benefits of these technologies are going to be balanced with the costs in the privacy of the individuals. The document will assess:

- Geolocation information collected from telecommunications operators
- Geolocation from social networks
- Apps, webs and chatbots for auto-test or medical appointments
- Contagion Information Collection Apps
- Contact tracing apps
- Digital Immunity Passports
- Infrared cameras

III. GEOLOCATION OF MOBILE PHONES BY TELECOMMUNICATIONS OPERATORS

This technique is used by mobile telephony operators, providing anonymised information about the location of their users in the telephone cells, that are defined by their antennas. Operators usually collect geolocation data from their customers. They calculate it using the strength the signals of each mobile phone reach the different antennas of an area. Using this information, which is necessary to provide the service, an operator can estimate which telephone numbers are in each cell at a given time. Even, it gives an approximate location of any active mobile phone in a cell. This information, without being anonymized, can be requested by Security Forces always through a judicial order. On the other hand, anonymized data have been used by the National Statistics Institute[1] for mobility studies. During the COVID-19 crisis management, the Governments[2] and the European Commission[3] have requested asked to the telecom operators to provide this kind of anonymized information with the purpose of monitoring population movements.



DOES THIS DATA REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

This data should not pose a greater threat than they previously represented with an appropriate level of anonymization. In other words, there is always the possibility of incomplete anonymisation, poor control of the processors or a cyberattack that would place users' mobile phones in the hands of a third party. Moreover, this risk existed before the pandemic. By increasing the use of these anonymised data, there may be a higher risk, but not exponentially greater.

---

1 Https://www.ine.es/ss/Satellite?L=es_ES&c=INEmasNoticia_C&cid=1259952394212&idp=1254736092060&pagename=masINE%2FmasLayout The INE conducts a pilot study on mobility based on aggregated mobile telephony data

2 Https://www.boe.es/boe/dias/2020/03/28/pdfs/BOE-A-2020-4162.pdf .Order SND/297/2020 of 27 March

3 Https://www.politico.com/news/2020/03/24/europe-mobile-data-coronavirus-146074 European Commission tells carriers to hand over mobile data in coronavirus fight

DO THESE DATA REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

The assessment of population mobility patterns, including where people move, when they work or where they spend weekends, can be always helpful for a public body. Health resources, or police forces are elements that could be dynamically dimensioned with a good mobility model. For example, how these resources should be deployed when an event such as a football match or a demonstration takes place. However, their usefulness in the pandemic must be assessed constantly facing the changing scenarios of global or partial confinement.

One option that has been pointed out is the possibility that anonymised geolocation data would be used to observe global movements, but considering the possibility that the police might request re-identification in certain cases in accordance with the criteria established by the health authorities to ensure control of the epidemic.

IV. GEOLOCATION OF MOBILES FROM SOCIAL NETWORKS

The geolocation of mobiles from social media data is not a novelty. Website administrators can find out the IP addresses from which we access the Internet, and they usually do it for advertising purposes. Some large vendors such as Facebook or[4] Google have[5] recently published aggregated data in the form of large dashboards.

DOES THIS DATA REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

While the processing of location data in the social networks could be a threat to privacy, it is not exclusively of this moment or of this situation. This threat may be more critical if this information is enriched with personal information obtained from the activity in user profiles or some actions are taken on their profiles based in some kind of inferences regarding infection. The terms of use and privacy policies of these services are not an adequate legal basis for these data processing.

DO THESE DATA REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

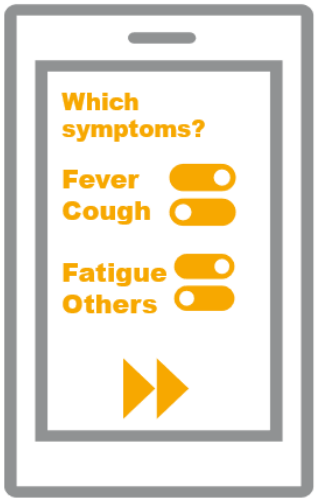
This data could be an aid to the authorities provided if the information collected is in accordance with a purpose previously defined by the health authorities. The authorities are

[4] Https://covid-survey.dataforgood.fb.com/ Facebook & Carnegie Mellon University COVID-19 Symptom Map
[5] https://google.com/covid19-map/?hl=en Coronavirus disease map (COVID-19)

the ones that should define from granularity to the data format, to be able to use them to their prevention and control strategies. In any case, it should be assessed if it represents a real improvement over other sources of information that might already be available to the authorities.

V. APPS, WEBS AND CHATBOTS FOR AUTO-TEST OR APPOINTMENT

Within this broad group of solutions would be mobile applications or apps[6], webs and chatbots which implement test questions and answers, information queries, or even registration of appointments in healthcare services. In this document, they are all grouped into the same category, because they are perhaps, from a technological point of view, the least innovative solutions. On the other hand, we can consider that they may be among the most widely used.



DO THESE APPLICATIONS REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

Threats to privacy may arise depending on how these apps are implemented and what are the real purposes. Threats may appear because of the urgency in providing operational solutions that relax controls and requirements to protect citizens' data. In some of these applications, potential threats to privacy have been encountered in the implementation of privacy policies[7]. Besides, it should not be forgotten that an app or a web is only an interface to display and bring data to a server, and that is where is carried out the hidden job of processing the requests.

DO THESE DATA REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

In general, when these apps are well built, they do represent a great benefit because they bring information and health care to people needing their services. As a side effect, other channels such as telephone are released from traffic, so that they can be used by people who are unable to access the Internet due to their age or circumstances. In addition to those mentioned above, another risk would be to invisibilise these people who do not know or do not possess a computer or mobile phone, and leave them without services.

[6]Examples in Spain are https://www.coronamadrid.com/ https://www.euskadi.eus/coronavirus-app-covid-eus/web01-a2korona/es/

[7] Https://blog.appcensus.io/2020/04/19/spanish-covid-19-apps/ Analysis of Spanish AppCensus apps.

VI. VOLUNTARY INFORMATION CONTAGION APPS (COVAPPS)

In this category there would be some mobile applications that have emerged in some cases from citizen initiatives[8]. Their aim is to make their own maps about propagation and statistics of COVID-19 using data voluntarily provided by users. They request collaboration to users in order to download these applications and upload their location data, and some other data about their possible infection. Thus, they are contributing to build maps and dashboards with information that, in theory, is not filtered by the authorities[9].

DO THESE APPLICATIONS REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

These apps could be a threat if the purposes they declare are not as altruistic as those they promote, or if due vulnerabilities in the design due to fast development there aren't enough guarantees of privacy. We cannot forget that health data and precise locations are being uploaded to Internet servers. If the quantity and quality of this data were sufficient, due to a significant number of users, the conclusions could identify areas with a high level of infection or toxic areas. It could represent a social stigma for their inhabitants or their businesses.[10]For this reason, it is necessary to have a significant amount of data, and guarantees that nobody, in a malicious way, is providing false or manipulated information to benefit or harm everyone.

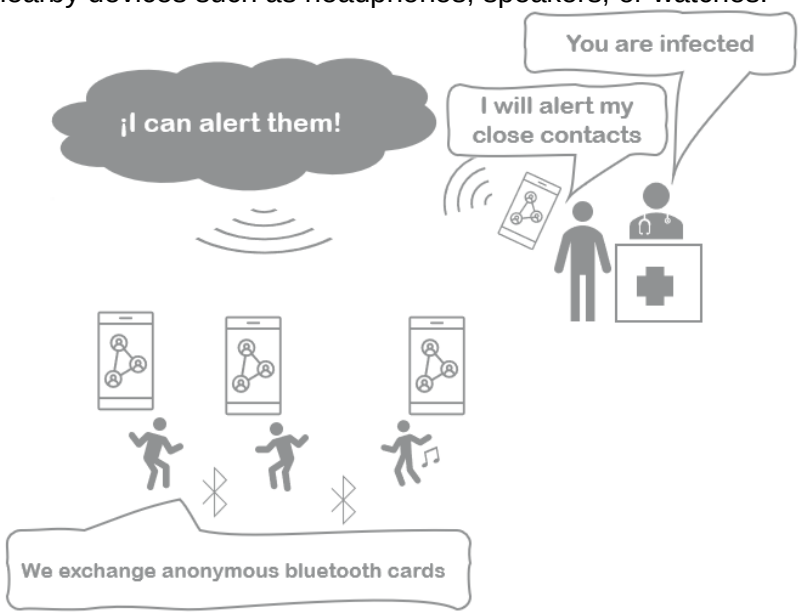
DO THESE DATA REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

Some private initiatives justify their action in the hypothetical inaction or lack of confidence of the authorities. However, taking into account the voluntary and uncontrolled use of this apps, it is never possible to know the reliability of the information they offer, so they can contribute to the dissemination of fake news and misinformation.

[8] https://github.blog/2020-03-23-open-collaboration-on-covid-19/ Open collaboration on COVID-19
[9] https://covidtracking.com/about-project The COVID Tracking Project
[10] Https://twitter.com/rcalo/status/1240028937008209920 Ryan Calo: Apps that purport to track people infected with COVID-19 are a terrible idea imo for several reasons.

VII. CONTACT TRACING APPS BY BLUETOOTH

This type of application uses the bluetooth technology of mobile phones that allows connection to nearby devices such as headphones, speakers, or watches.



In this case, the apps use the Bluetooth device to send a user's "card" to other mobile phones present on their way, and, at the same time, collect the "cards" of those mobile phones. Each card does not have a real user ID, but a nickname. In this way, each mobile has a collection of anonymous "cards" of the people with whom they have met in their work, in a public transport or in their free time. If a certain user finds out that he is infected, he has the possibility to "declare" it through the app to a central server. At that time, those people who were in contact with him in the last few days are supposed to receive a warning assessing what actions to take, such as being confined, contacting your health services or taking a test.

Several strategies[11] have been depicted to implement this technology, which basically vary in who has control over the identities and network of contactees by each user. There are options in which the control over data rely on the user himself (decentralised), and other solutions that offer a centralised control of the data, supposedly by an authority.

In the technical debate about what kind of solution will be applied in Europe, a new factor has entered recently. The giants Google and Apple have partnered to offer a tracking solution[12] *or contact trace using their iOS* and Android systems. Among other factors, this is due to the iOS system that severely limits third-party solutions that use Bluetooth in the background. Subsequently, if some sort of adaptation is not made, IPhone users could not properly use applications developed by other than Apple[13].

[11] Https://github.com/DP-3T/documents DPT3T and https://github.com/ROBERT-proximity-tracing Robert are good examples of Contact Trace implementation.

[12] Https://www.apple.com/covid19/contacttracing/ Privacy-Preserving Contact Tracing

[13] Https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0 Bluetooth phone apps for tracking COVID-19 show modest early results

DO THESE APPLICATIONS REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

The main threats to[14] the privacy of this type of solution are: the development of maps of relationships between people, re-identification by implicit location, the vulnerability of protocols at the time to design almost anonymous "cards", and releasing the signals of the contagions in a way that does not identify in any case who is infected. It should be noted that the processing of the information not only affects the user of the application, but also other people with whom he has been in contact. That is why this processing must comply with the principles of data protection.

There are studies[15] on the robustness of cryptography and anonymization protocols. They show there is always a possibility that, by applying sufficient time and computing capacity, they can break and associate anonymous nicknames with phone numbers and people. From the point of view of privacy, the more processing is done on the server part, the less control has the user on his own data. Therefore, centralized solutions always seem less respectful of privacy than distributed solutions[1617]. Another of the greatest threats of the centralized accumulation of data come from the risk of an abuse by an unethical company, the expansive purposes of the data processing or a cyberattack that leaks information.

DO THESE DATA REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

Once again, it must be emphasised that technical solutions cannot be considered in isolation. The success of such solutions is based on many factors that do not depend on technology. Firstly, the involvement of many users is necessary. Some studies show[18] that the minimum potential users must be at least 60 % of a population which, considering children and the elderly, include almost all mobile users. On the other hand, it depends on making a responsible statement of the personal situation of infection, preferably supervised by a professional, to avoid disinformation strategies. Finally, it is necessary to have access to Covid-19 tests, not only for all users, but also to be able to update the information periodically and so that, those who are notified of having been in contact with an infected, can carry out the test promptly.

In the current situation in European countries, it does not appear that these applications will be successful in the short term, as a global strategy to combat the pandemic. If we think of a future scenario, when the disease will be much more controlled, it could have its success in specific collectives such as school students, professionals from a company, or groups of friends who voluntarily decide to use the app. We can think of the similarity of the WhatsApp groups commonly shared by parents of children at schools, and for which they are advised, for example, if there is a nearby child with any infection or parasites. A use-case that carries out several data protection problems too.

---

[14] Https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf Mobile applications to support contact tracing in the EU's fight against COVID-19. eHealth Network

[15] Https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems. The DP-3T Project

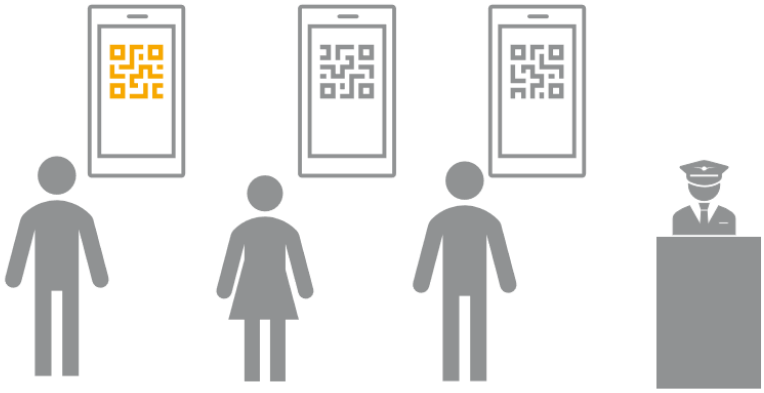
[16]Letter from the European Data Protection Committee https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

[17]Communication from the Commission:Guidance on mobile applications to support the fight against the covid-19 pandemic with regard to data https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)

[18] Https://science.sciencemag.org/content/early/2020/04/09/science.abb6936.full Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Another clarification quote is https://www.straitstimes.com/tech/google-launches-new-tool-to-help-public-health-officials-plan-social-distancing-measures

VIII. IMMUNITY PASSPORTS

Some countries have begun to consider the use of apps[19] like a passport or a paper safe-conduct. They display a color code or QR code on the screen, allowing to a watchman, or to an access control system, to decide if the holder may or may not pass. This procedure is similar to that used with airport boarding passes, but instead of showing that a user has a valid plane ticket or is included in a shipping list, it reveals if the carrier is infected, or presumably immunized[20] against the disease.



DO THESE APPLICATIONS REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

These mobile apps are anticipating a future with mobile ID cards. In addition, they have the added risk of including and displaying health data, to all the risks arising from the vulnerabilities of such systems: access to the hands of cybercriminals, crossing with other data such as geolocation data, metadata processing, remote access or simply not being available for many people who cannot/don't want to use of smartphones.

Unlike a boarding pass delivery, medical tests to determine whether a person is suffering or having overcome the disease should be face-to-face, and when the health personnel performs them, they could give to the patient a paper certificate or any low-tech/low-risk media to show when required, along with his/her identity card. A mobile identity system can only have advantages when download can be done at longer distance or if the information it manages changes rapidly, like a digital purse, which is not the case.

DO THESE APPLICATIONS REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

The immunity passport includes sensitive data. It has also the mission of serving as a safe-conduct of access. There are reports[21] that predict the progress of mobile health applications (mHealth) allowing, for example, a patient to bring their medical records to a doctor and receive treatment. Similarly, the exercise of certain activities such as intense work or intense physical activity may require the candidate to show a medical certificate

[19] Https://www.bbc.com/mundo/noticias-52215521 , https://www.infobae.com/america/ciencia-america/2020/04/01/que-son-los-pasaportes-de-inmunidad-del-coronavirus-covid-19-que-se-estudian-en-alemania-para-regresar-a-la-normalidad/ news about possible adoption of passports in China, Germany, Italy, Great Britain, USA or Chile.

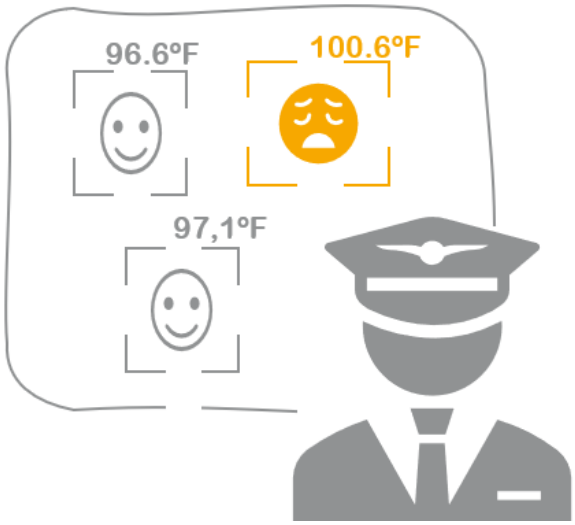
[20] Https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19 WHO says there is not enough evidence of antibody immunity.

[21] Https://www.who.int/goe/publications/goe_mhealth_web.pdf.New horizons for health through mobile technologies.WHO 2011.

before entering. A well-managed use of apps for health certifications or records, which keeps them up-to-date, safe and interoperable, will have some usefulness in specific areas. It will be necessary that the access to such information will be made by personnel involved in public policies for the control of the pandemic. However, as in all applications that require the use of smartphones, and evidence of a reliable test of infection or antibodies, we are far from reaching the whole population, so we can only wonder about the benefits they could have in very specific areas.

IX. INFRARED CAMERAS FOR MASSIVE TEMPERATURE READINGS

In recent weeks, the debate over facial-recognised video surveillance cameras has been shifted by the debate around other types of cameras that add the ability to measure the temperature from individuals crossing an area[22], in many cases without requiring any action on their part. These cameras identify human faces using artificial intelligence algorithms. They discriminate faces from other elements in the image and reveal the approximate body temperature of each individual.



DO THESE SYSTEMS REPRESENT A THREAT TO PRIVACY IN THE PANDEMIC CRISIS?

AEPD has already expressed its[23] concern about the use of these devices and the need to have the prior criteria of the health authorities before their implementation. The use of cameras or other devices to record the temperature of individuals involves the processing of special categories of data, and it must respect the principles of legality, purpose limitation and accuracy.

The thermal camera and data collection can only be understood as part of a larger processing. Nobody can take a person's health data and process it spontaneously in a public place, simply because he thinks it is the best for his customers or users. In these cases, we will have a risk of discrimination, stigmatisation and perhaps public dissemination of health data. All this can be aggravated by the risk of leaking sensitive information and the conflict with those people understanding that measure as a violation of their rights.

[22] Https://iberia.dahuasecurity.com/thermal/ Body Temperature Monitoring Solution.An example.

[23] Https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos AEPD release regarding temperature intake by shops, workplaces, and other establishments

In some environments, such as occupational risk prevention regulations, temperature-measuring could be useful within the framework of more extensive measures. It also could require other additional checks and guarantees that, in any case, the rights and freedoms established in the GDPR will be fulfilled.

DO THESE SYSTEMS REPRESENT AN IMPORTANT BENEFIT IN THE PANDEMIC CRISIS?

Fever is one of the most likely clinical evidence associated with a symptomatic Coronavirus infection,[24]. Nevertheless, it should also be considered that the percentage of asymptomatic infected persons is huge[25] and the high temperature may be associated with other pathologies[26]. These measures should be applied with some criteria laid down by the health authorities regarding the significant value of fever and what other symptoms have to be tested. If these systems are operated without enough precision or by unskilled personnel, they could create a false sense of safety, enabling contact with truly infected persons.

X. CONCLUSION

In this document, it has been carried out a brief review of the main technologies proposed in the fight against the pandemic. It does not pretend to be a deep analysis of them. Rather the purpose has been to compile those options that are considered to control its expansion.

Our society is at a critical turning point, not only because of the pandemic situation, but also in relation to our model of rights and freedoms. Therefore, it is esential to be especially careful when adopting measures that can have irreversible consequences, and which may be guided by urgency, fear or, worse of all, other interests.

At this point, it should be remembered that using information technologies cannot be understood in isolation, but always in the context of a processing with a well-defined and fair purpose. Any personal data processing must implement in the framework of a global strategy based on scientific evidence, assessing its proportionality in relation to its effectiveness, efficiency and it should assess objectively the necessary organizational and material resources available. In addition, it should always bear in mind that the principles laid down in the General Data Protection Regulation are mandatory.

[24] Https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30198-5/fulltext Clinical and epidemiological features of 36 children with coronavirus disease 2019 (COVID-19) in Zhejiang, China:an observational cohort study

[25] Https://www.medrxiv.org/content/10.1101/2020.02.03.20020248v2 Estimation of the asymptomatic ratio of novel coronavirus infections (COVID-19)

[26] In addition to being easily concealable by using antithermals https://www.noticel.com/ahora/20200406/tomaron-medicamentos-para-ocultar-fiebre-y-ahora-estan-hospitalizados-por-covid-19/