NOVA SCHOOL OF LAW

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

VARIA

CONTACT TRACING APPS: IS IT THE KEY STRATEGY FOR PREVENTING FURTHER SPREAD OF COVID-19?

BEATRICE FRISON
Università degli Studi di Ferrara (Italy)

ABSTRACT

Is it possible to rely on the Chinese model to tackle the epidemic in the Western world, where the problem of the protection of individual rights is at the heart of political thinking and of the liberal legal-constitutional tradition?
The purpose of this research is to examine the use of mobile tracking and contact tracing technologies in the fight to contain contagion during the Covid-19 pandemic, as they are about to be introduced in Italy, in France and other European countries, following the effectiveness of the Chinese Strategy. I will also try to highlight the problems related to the use and dissemination of mass surveillance techniques, that could profoundly affect the Fundamental rights and individual freedoms, explaining how it is possible for a democracy to respond effectively to the emergency, without any yielding to authoritarian temptations.

KEYWORDS

Covid-19 - contact tracing - tracing Apps - fundamental rights - privacy - data access

TABLE OF CONTENTS

1. Introduction and model of analysis:

Three months into the SARS-CoV-2 (COVID-19) pandemic, infections and deaths continue to rise globally, surpassing over 300 thousand deaths. A vaccine for the virus is currently estimated to be found in one or two years, and, if we do not want to have a prolonged period (extended to 12 or more months) of home-isolation policies, it is necessary to allow for other strategies for the containment of the contagion. There is a growing consensus, even within the public health community, concerning the need of a combined strategy of medical and

technological tools to provide us with response at a scale that can outpace the speed and proliferation of the SARS-CoV-2 virus. A process of identifying exposed individuals who have come into contact with diagnosed individuals, called "contact tracing," has been shown to effectively enable suppression of new cases of SARS-CoV-2 (COVID19).

A biological test for each of the suspected cases with virus-related symptoms shall be carried out to detect the infected, and traditionally this testing loop has been managed manually by health-care providers through "contact tracing," where medical professionals interview the person who tests positive for the virus and informs those who may have come into contact with a patient to alert them to quarantine and to seek a test. It is evident that this method is not effective in the long term, since it is not possible to trace all the human contacts that the infected subject has had, so to slow down the reinfection rate for this novel virus, we need novel approaches. Countries like China and South Korea demonstrate that the use of digital technology, specifically that deployed on personal devices through Apps or other services, can highly accelerate the identification and management of the virus by notifying citizens of their possible exposure to the virus. Different models of tracking apps have emerged with different technological features and privacy implications:

The mobile technology of Tracing is used to trace physical contacts between people. Using Bluetooth, a technology that enables digital devices to communicate with each other over short distances, it can measure the distance between smartphones on the basis of the strength of the radio signals and thus detect encounters between users (proximity tracing).

Tracking, instead, is based on forms of geolocation of the user, so is about gaining insights in real time. A tracking app can, for example, determine a person's current location using geodata (e.g. via GPS coordinates or radio cell location). If it additionally tracks who has been where and when, it even allows to create detailed movement profiles, so it monitors when users come into contact with each other.

While there is well-justified concern that such systems might enable mass surveillance, a variety of solutions have developed recently with intentional privacy controls incorporated.[1]

I will take into account models from China and the rest of the Asian world, and the founding principles of what will soon be introduced in Europe, based on the following analysis model:

[1]'Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks' Harvard University's research, https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf, p.7

A) Privacy:

1) capillarity of control : 1.1) available services (different types of apps and services)
1.2) consent to data processing
1.3) anonymization (data deidentification techniques)
1.4) percentage of the population having to install it

2) localization : 2.1) how your location is detected: scanner in public spaces
geolocation (Maps)
Bluetooth
Cellphone tower
2.2) for how long your position remains shared
2.3) access to your routine habitudes (places, shops, restaurants, sports)
2.4) information about your family members, work colleagues and friends
2.5) notice of places to avoid (i.e. park or supermarkets in peak hours)

3) personal situation : 3.1) access to health conditions
3.2) assistance in case of infected people
3.3) warning in case of contact with infected people (isolation)

4) personal characters : 4.1) collected in public spaces (cameras and drone)
4.2) collected in private collective spaces
4.3) collected by apps

B) What can be done with this data:

1) efficiency of controls : 1.1) videos
1.2) drone
1.3) police
1.4) citizens themselves

2) punishment : 2.1) reproach from authorities
2.2) fine (administrative penalties)
2.3) prison
2.4) beatings and corporal punishment
2.5) capital punishment

C) who has access to this data:

1) Government: 1.1) bear the costs of the App and services or buys data from private entities
1.2)assess whether the strategy put in place to limit the spread of the virus is effective
1.3) decide what directives and codes of behavior give to the population
1.4) allows timely detention of new outbreaks
1.5) allows coordination with foreign authorities

2) Police :2.1) ensure compliance with the rules
2.2) allows timely intervention in case of violation of the rules
2.3)evaluate the self-discipline of the population (ability to follow the rules)

3)health system: 3.1) trace at which stage of infection the contact occurred
3.2) figure out what kind of contact was (prolonged, in a closed space, open-air contact, use of the personal protective equipment)
3.3) discover for how long a person remain infected
3.4) evaluate the possibility of being infected again
3.5) warning of the hospital after the contagion (voluntary or automatic)
3.6) giving assistance in case of symptoms (through advices provided by the App, emergency numbers or through arrival of the health care personnel at home)

4) Employers : 4.1)absence from work due to illness or symptoms
4.2) inform all employees of the possible contagion
4.3) implementation of workplace controls and reorganization of shift work

4.4) subsidies and economic aid (financial support to sick workers)
4.5)improve the efficiency of remote work (decrease of absences, serenity of the employees, increase of productivity, and so on)

5)Media : 5.1) censure about this data
5.2) inform the community of the development of the contagion
5.3) intimidate the population and invite them to respect the rules
5.4) inform the population of the stages of the disease, taking as example the cases of infected

6)epidemiologists and research groups: 6.1) reconstruction of the interactions between those infected
6.2) analysis of the most affected ages groups
6.3) analysis of the contagion curve
6.4) forecast of future inflow of contagion

2. Different contact tracing techniques

Contact tracing describes a variety of techniques used to identify people who may have come into contact with a positively diagnosed person, and taking appropriate action to inform, isolate, and treat those contacts. Contact tracing is commonly used to reduce the spread of tuberculosis, measles, HIV, and other diseases. The goal of tracing is to identify and isolate not only those who are known to have a disease, but also to try to get ahead of the spread of the disease by priority testing those with whom a COVID-positive person has been in close contact during the incubation period. Data shows that if only those with symptoms are identified and isolated, the spread of the disease won't stop, as it is likely that they have already passed the illness to others. Traditionally, contact tracing is done manually, but this approach works well only when there is a small number of infected people, so even if it has been used in the past for outbreaks of Ebola, SARS and HIV, manual contact tracing has been proven insufficient to contain COVID-19 on its own, both theoretically and in practice. Manual contact tracing relies on human memory, and for a

highly infectious disease with a long incubation period it becomes difficult to remember contacts; symptoms, besides, appear days and sometimes weeks after that individual becomes contagious, and probably after several chains of infection have occurred. Secondly manual contact tracing takes time and COVID-19 is a virus that spreads very quickly; thirdly this type of tracing requires trained human resources and our medical system does not have enough people for a COVID-19 scale epidemic. In light of this, the development of IT solutions appears to be more effective, because once someone is identified as Sars-CoV-2 positive is required to be kept in isolation for a minimum period of 14 days, or longer if he develops symptoms, and all his contacts will be informed and should also be incentivized to quarantine while they await the result of their test, and only after receiving a negative test should resume their usual activities. Digital contact tracing is more accurate, because it no longer relies on individual's memory to create a list of contacts, it is faster because subjects who have come into contact with the infected person are alerted simultaneously and immediately, and it is also a low cost method because it does not require an increase in healthcare staff and follows-up can be done automatically in cases where medical care is not needed.
Using Apps and services to track down infected people and identify high-risk individuals has worked in several countries and most core functionality relies on Bluetooth or GPS.

3. Chinese model – mobile location data tracing (GPS systems)

China has not developed an app in its own right, but has inserted the tracking functionality in existing apps, which through GPS geolocation allow you to see which are the riskiest places for the coronavirus. This service can be found on different platforms, all difficult to reach by those who live outside the borders of China. There are maps of Baidu[2], the main Chinese search engine, and those of Wechat, the messaging app with over a billion active users, and then maps of other independent apps like AvMap. Many of these are based on data provided by national bodies such as the China Electronics Technology Group

[2] Link to the Chinese website: https://www.baidu.com

Corporation (CETC).[3] The option 'coronavirus' has been inserted directly in the most popular map apps in the country and allows you to see where cases of infection have been recorded. The geolocation is very precise and allows you to see exactly in which buildings the coronavirus arrived. A precision that can lead to paranoia, since the risk is to leave in the hands of any user all the possibilities to trace the identity of the infected.

Among the various maps, there is also an official one launched directly by the Council of State (the Chinese Government) along with the National Health Commission and the China Electronics Technology Group Corporation: Close contact detector. To register here you must use your name and your identity card number. Once you enter your data, the system will say, crossing several databases, if in recent weeks you have come into contact with people infected with the virus. The App does not cover supermarkets or shopping malls, but particular attention shall be paid to the use of public transport, in particular trains and aircraft: Every passenger on a flight seated up to three rows away from a sick person or suspected person is considered to be in close contact and therefore potentially at risk of being infected.

Also Alipay, Alibaba's mobile payment system, which the Chinese commonly and predominantly use in metropolises instead of cash or credit cards, has developed a tracking feature via GPS geolocation, called Alypay Health Code[4] because it allows the user to obtain a Health Code. People in China sign up through Ant's popular wallet app, Alipay, and are assigned a color code — green, yellow or red — that indicates their health status. After users fill in a form on Alipay with personal details, the software generates a QR code in one of three colors. A green code enables its holder to move about unrestricted, with yellow code is required to stay home for seven days, while Red means a two-week quarantine. The assigned color can change not only depending on the health status of the user but also, for example, if you live in an area where a cluster of the disease has been identified.

An official webpage with questions and answers about the service says a yellow or red code may be given to someone who has had contact with an infected person, visited a virus hot

[3] With fifteen years of rapid development, CETC has become the only large-scale technology corporation in China covering all fields in electronic information. It is the most powerful national central corporation in the fields of defense electronics, security electronics and informatization with the market covering more than 110 countries and regions in the world. CETC website: http://en.cetc.com.cn/enzgdzkj/about_us/introduction29/index.html

[4] Link to Chinese website: http://www.xinhuanet.com/tech/2020-02/19/c_1125596647.htm

zone or reported having symptoms in the sign-up form. This suggests that the system draws on informations about coronavirus cases and government-held data on plane, train and bus bookings.

It has become nearly impossible to get around without showing your Aliplay code; the system was introduced on 25 February 2020 in 200 Chinese cities and is now being progressively extended throughout the country[5]. A New York Times analysis of the software's code found that the system does more than decide in real time whether someone poses a contagion risk[6]; this analysis found that as soon as a user grants the software access to personal data, a piece of the program labeled "reportInfoAndLocationToPolice" sends the person's location, city name and an identifying code number to a server; the Time's analysis also found that each time a person's code is scanned- at a health checkpoint, for instance- his or her current location appears to be sent to the system's servers. This could allow the authorities to track people's movement over time. Furthermore, the software does not make clear to users its connection to the police, but according to China's state-run Xinhua news agency and an official police social media account, law enforcement authorities were a crucial partner in the system's development.

The Health Code functionality has as a salient feature to enter with all probability to be part of the Social Credit System (SCS) the much-discussed initiative of the Chinese government created in order to develop a national system to classify the reputation of citizens and companies[7].

[5] official website providing the national health code, https://mp.weixin.qq.com/s/amB7fBxLw8KSR9DcUsbTWg

[6] https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html for the NY Times It also appears to share information with the police, setting a template for new forms of automated social control that could persist long after the epidemic subsides.f

[7] For years the Chinese government has been mobilizing to implement a system of social control, the Social credit system aimed at monitoring citizens, institutions and businesses through a complex system of control and evaluation. Initial reports suggest the system utilizes numerical score as the reward and punishment mechanism; the credit score of each user is determined by various positive elements (social services, volunteering) which will correspond to a positive rating, then free or guaranteed services, and negative elements (fines, unpaid debts) which, causing a negative rating, preclude the purchase of internal plane tickets, fast trains, hotel reservation and so on. As of June 2019, according to the National Development and Reform Commission of China, 26.82 million air tickets as well as 5.96 million high-speed rail tickets have been denied to people who were deemed "untrustworthy (失信)" (on a blacklist), and 4.37 million "untrustworthy" people have chosen to fulfill their duties required by the law. In general, it takes 2–5 years to

A team of experts[8] from MIT Technology Review, a magazine owned by the Massachusetts Institute of Technology, developed 'Covid Tracing Tracker', a database to capture details of every significant automated contact tracing effort around the world. Is evident that there is very little information available to the public about how China's technology works, and the Chinese health code system does not meet any of the criteria used by them to compare Apps developed worldwide: the Chinese system is not downloaded on a voluntary basis, the control is not restricted or minimized, there isn't any support algorithm for data destruction, and there is no transparency in the management and disclosure of the data collected[9].
The use of systems like this, which include GPS, cell tower triangulation and Wi-Fi access point triangulation, can be used to create a location history for an individual and can be compared to other locations histories to check for potential interactions. The largest advantage of these systems is that a significant proportion of phones are already recording location data, either to Google Maps Timeline or encrypted local storage, or both. This allows users to install an App today and receive warnings about exposures that may have happened in the preceding week or two, and, maybe more important, allows those who test positive to install an App after that diagnosis[10].Compared to Bluetooth, geolocation can be used to tell users which areas to avoid, but is less accurate in identifying when two people have been in close contact with each other, because it has a much wider and less precise radius of action than Bluetooth localization. Moreover, geolocation-based systems are less

be removed from the blacklist, but early removal is also possible if the blacklisted person has done enough remedies. Certain personal information of the blacklisted people is deliberately made accessible to the society and is displayed online as well as at various public venues such as movie theaters and buses, while some cities have also banned children of "untrustworthy" residents from attending private schools and even universities. On the other hand, people with high credit ratings may receive rewards such as less waiting time at hospitals and governmental agencies, discounts at hotels, greater likelihood of receiving employment offers and so on. Critics of the system claim that it oversteps the rule of law and infringes the legal rights of residents and organizations, especially the right to reputation, the right to privacy as well as personal dignity, and that the system may be a tool for comprehensive government surveillance and for suppression of dissent from the Communist Party of China.

[8] Patrick Howell O'Neill, Tate Ryan-Mosley and Bobbie Johnson have worked with a range of experts to understand the technologies and polices involved.
[9] MIT Technology Review Covid Tracing Traker is available here: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/
[10] https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf

secure because location information is more difficult to anonymise properly. A centralized database, as in the case of the Chinese model, puts the privacy of individuals at high risk because the government can very easily abuse these data and use them for purposes other than those for which they were collected. A possible alternative is that GPS could be used as a memory aid for manual contact tracing interviews, so users are in full control of information shared, avoiding unnecessary information transfer; but also in this case, tracing data would be collected by a central authority. However, it is possible to mitigate security risks through cryptographic methods and encrypted computation, that allows users to track their location history in a way that never leaves their device, with fully decentralized systems. According to this approach, users can contribute limited location information (such as only visits to public spaces) that gets aggregated into a heatmap that can be shared with other users, who receive automatic alerts when they are entering a Covid-19 hotspot. Anyway, any system declaring to anonymize data should be carefully verified, and, despite this, there is always a risk that the authority that processed the data can trace personal information through deanonymization techniques. For this reason, some projects that started to be developed with a GPS system, decided to switch over to Bluetooth system (contact tracing model) more recently, which turns out to be safer. Moreover, Bluetooth has an accuracy advantage over GPS for in-person contacts; it works reliably under-ground, indoors, and in motion, and will only detect users within a certain radius (about 30 meters). GPS system may involve people in very distant parts (e.i. distant areas of the same building), and for this reason the system risks to be inundated with false positives. In addition, Bluetooth has a privacy advantage over GPS, because the only information involved is contact tokens[11], which can be crypto- graphically secured in a way that is less vulnerable to de-anonymization than geolocation.

[11] A token is a pseudorandom numerical code generator at regular intervals (in the order of a few tens of seconds) according to an algorithm that, among the various factors, takes into account the passage of time thanks to an internal clock.

4. Contact tracing by Bluetooth - Singaporean model

The contact tracing model has been used as firstly by Singapore, which, through an App, identifies contacts between people regardless of their location, using Bluetooth technology. On March 20, 2020, the Singaporean Ministry of Health released the TraceTogether app for Android and iOS[12], that tracks via Bluetooth when two app users have been in close proximity: when a person reports that has been diagnosed with Covid-19, the app allows the Ministry of Health to identify anyone who has been registered near them. It operates by exchanging tokens between nearby phones via a Bluetooth connection, and these tokens are also sent to a central server. These tokens are time-varying random strings, associated with an individual for some amount of time before they are refreshed. Should an individual be diagnosed with COVID-19, the health officials will ask[13] them to release their data on the app, which includes a list of all the tokens the app has received from nearby phones. Because the government keeps a database linking tokens to phone numbers and identities, it can trace back from this list of tokens to users who may have been exposed. By using time-varying tokens, the app does keep the users private from each other. A user has no way of knowing who the tokens stored in their app belong to, except by linking them to the time the token was received. However, the app provides little to no privacy for infected individuals; after an infected individual is compelled to release their data, the Singaporean government can build a list of all the other people they have been in contact with.[14] This is a Centralized model with serious privacy issues, in fact user ID is assigned by the central authority; ID interactions are recorded locally, and COVID-positive users send their IDs to the Singaporean government, populating a database that records personal medical information.
A different approach that guarantees a higher level of privacy could be a system where users create and broadcast their own constantly changing random IDs, and Covid-positive

[12] "Help speed up contact tracing with TraceTogether," Singapore Government Blog, March 2020. [Online]. Available: https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether.
[13] 'ask' is a bit of a misnomer, because it's a crime in Singapore not to assist the Ministry of Health in mapping one's movement.
[14] 'Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs', Cornell University, 04/2020 , available here: https://arxiv.org/abs/2003.11511

users send their token generator to a centralized server, which broadcasts the generator for cross-checking.[15] In this way the central authority does not hold users's personal data and is not able to identify them.
A completely decentralized approach, instead, would allow a fully respect for the privacy of individuals, since in the absence of a central database, the government would not have access to user data. One solution would be to develop an App based on a peer-to-peer system[16] , where each user broadcasts and receives self-made tokens, recording interactions, and Covid-positive user's tokens are disseminated to people they were in contact with, without any centralized database storing them.

5. European approach

At European level has been set up the PEPP-PT (acronym of Pan European Privacy Persevering proximity Tracing)[17], a team that includes 130 researchers from eight European countries, that works for the development of contact tracing Apps. PEPP-PT was created to assist national initiatives and its mechanisms will have these core features: Interoperability to support tracing local infection ('Pan European'), anonymization and GDPR[18] compliance ('Privacy-Persevering'), and delivery of epidemiological data to fight

[15] https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf
[16] A parity computer network that has no central server, and all Peer have the same role. Using this configuration, any node is able to automatically start a transaction without passing through a central server.
[17] PEPP-PT is an organization that will be incorporated as a non-profit in Switzerland; it was created to provide a solution to the Covid-19 crisis that adheres to strong European privacy and data protection laws and principles through a service that is available to all European countries, managers of infectious disease response and developers. Website available here: https://www.pepp-pt.org/
[18] The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects inside the EEA. The GDPR was adopted on 14 April 2016, and became enforceable beginning 25 May 2018. As the GDPR is a regulation, not a directive, it is

the pandemic ('Proximity Tracing'). "Our goal is to provide a common framework to the fundamental digital applications of the global fight against COVID-19," said Hans-Christian Boos, founder of the automation company Arago and digital consultant to the German government. " The PEPP-PT platform that can be used by others, in addition to the founders, allows an approach to digital tracking of anonymous proximity and respectful of privacy, is in full compliance with the GDPR and can also be used when travelling from one country to another". To ensure privacy is protected, the system anonymously records the person with whom you have been in close contact for at least fifteen minutes, using Bluetooth. In this way, if one of these persons declares himself sick, the application will send a notification without revealing the identity of the infected person and vice versa; this allows testing or spontaneous quarantine to limit the spread of the virus. More specifically, as regards PEPP-PT's mechanism, each PEPP-PT phone broadcasts over a short distance a temporarily valid, authenticated and anonymous identifier (ID) that cannot be connected to a user. Proximity between phones of other PEPP-PT users are estimated by measuring radio signals (Bluetooth, etc.) using algorithms. When PEPP-PT phone A is in epidemiologically sufficient proximity to PEPP-PT phone B over an epidemiologically sufficient period of time, as determined by the measurements, the anonymous ID of phone B is recorded in the encrypted proximity history stored locally on phone A (and vice versa). No geolocation, no personal information or other data are logged that would allow the identification of the user, in compliance with the Regulation (EU) 2016/679 and, as regards the deletion of the proximity history, the PEPP-PT official website says that older events are deleted when they become epidemiologically unimportant.[19]
This model provides two operating modes of the proximity history:
If a user is not tested or has tested negative, the anonymous proximity history remains encrypted on the user's phone and cannot be viewed or transmitted by anybody. At any point in time, only the proximity history that could be relevant for virus transmission is saved, and earlier history is continuously deleted.

directly binding and applicable, but does provide flexibility for certain aspects of the regulation to be adjusted by individual member states.

[19] PEPP-PT does not specify how long the proximity history remains recorded in the system of each user, it says only that this proximity history cannot be viewed by anyone, not even by the user himself.

If a user has been confirmed to be Covid-19 positive, the health authorities will contact him and provide him with a TAN code; the user uses this code to voluntary provide information to the national trust service that permits the notification to people recorded in the proximity history, and hences potentially infected.
Unlike the most invasive surveillance technology used in countries with lower privacy standards, European software allows you to encrypt your data and anonymize your personal information, according to some of the organizations involved, including the Fraunhofer Heinrich Hertz Institute in Berlin and the Ecole Polytechnique Fédérale in Lausanne. Two phones never exchange data directly, while user identifiers are often changed. This avoids abuse by third parties, including governments, and ensures that data protection standards do not suffer irreparable damage while Europe faces the pandemic.
The Italian, German and French governments are among those that have indicated they're baking PEPP-PT for national apps; these apps will play a key role in containing and slowing down COVID-19 infections "once national blockade measures have succeeded in flattening the spread curve of the pandemic"[20].
First, account should be taken of the purposes for which contact tracing is carried out, that is, to stem the spread of the virus. Secondly, the way in which it is implemented must be taken into account. It means that the data collected and their possible crossing must be done by ensuring compliance with the provisions of Reg. EU 2016/679, as I said before. Another important point concerns the time frame during which these data are collected and used: they may be used only for the period necessary to contain the virus.
In this case the most suitable legal basis is represented by art. 9 GDPR (processing of special categories of personal data) with reference to health data, namely special data, prohibits the processing, but being, however, in a situation of real health emergency at global level, the normative reference is paragraph 2 of art. 9, that at letter i) provides that '*processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy*'[21].

[20] B. Ruffilli, op. cit. available here: https://www.lastampa.it/tecnologia/news/2020/04/01/news/ecco-l-app-europea-per-il-tracciamento-che-combatte-il-coronavirus-rispettando-la-privacy-1.38665734
[21] This derogation is recognised by 2016/679 Regulation.

The provision of art. 9 GDPR is linked to a series of guarantees that can also be identified in the recitals and, in particular, in no. 46 which provides that the processing of personal data is '*regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person*'. Within the category of sensitive and particular data, enjoy a particular form of protection those relating to the health of a subject[22]. Analyzing instead the following paragraph 4 of art. 9 GDPR[23], is highlighted how Member States can act by introducing more restrictive conditions or measures in particular with regard to health data, for example when a state is faced with emergencies such as the one we are experiencing. The treatment of health data must be provided by law and regulated in such a way as to ensure, in addition to safety measures, pseudonymization[24].

6. Privacy risks and other critical issues

Despite these guarantees, no technical solution can absolutely guarantee privacy. Experimentation and oversight will be crucial to make a realistic assessment of possible vulnerabilities. There are several limits which risk jeopardizing these precautions one the one hand, and one the other hand substantially reducing the effectiveness of the system:

i. a user who declares himself positive or ill loses anonymity and is identified and registered in the central servers.

[22] The definition of health data is provided by art. 4 paragraph 1 no. 15) '*data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'*.

[23] Art.9 paragraph 4 '*Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health*'.

[24] The definition of pseudonymization is provided by art. 4 paragraph 1 no. 5) '*pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.*

ii. The anonymity of an infected person with whom one has had contact is not always guaranteed[25].
iii. There is a problem of parasitic applications: for example, other apps installed on a phone may try to listen in on a tracing application and send data to a third party, such as in south Korea: in this case the Open Data has allowed unscrupulous developers to track and make public the movements of infected people such as the Corona100m App, downloaded by more than million users. For the same reasons, again in Korea, there were forms of social discrimination such as that occurred against members of a religious sect, where a cluster of disease had developed after a large meeting.

That being said, the hope is that a system can be developed that has fewer privacy failure points than traditional manual contact tracing, and more privacy protections than GPS location based tracking, and that allows people to opt in based on a realistic understanding the risks.

Another aspect to take into account is that in Europe, contrary to what happens in China, the use of these Apps should be optional. Here there are two opposite risks. On the one hand it is estimated that to be effective the system must be used by 50-60% of the population, which can't be taken for granted, since only an average of 70% of the population has a smartphone and that not all are practical in the use of Bluetooth. Furthermore, the fact that non-negligible groups are excluded, essentially for economic and educational reasons, constitutes class discrimination, weakens the fight against the pandemic[26]. On the other hand, despite the download is on a voluntary basis, pressure and interference are put to encourage its use, as in the case of Italy. The application chosen by the Italian government for the contact tracing of positive subjects is called 'Immuni', and is developed by the Italian company Bending Spoons; the download will be free and on a voluntary basis when it will become available. The Ministry of Health has

[25] The infected can be easily identified when you meet a small number of people or if you turn on Bluetooth only on certain occasions.

[26] The weak population groups include the elderly, families with low incomes, homeless, people who are not self-sufficient, unregulated immigrants and so on. With regard to the last-mentioned category, The Portuguese Government has decided to grant residence permits to all immigrants who have already applied for them, at least until 1 July, to ensure that they can best deal with the coronavirus emergency. The government of Antonio Costa has approved the sanatorium for asylum seekers and for all foreigners without residence permit who have applied for access to health services.

ruled out any form of imposition for the installation of the app, and denied the news that the government's technical-scientific commission on coronavirus was going to formalize a proposal to make the app mandatory. The idea to make the app a necessary condition for being able to benefit from mobility advantages, was also denied by the working group that dealt with evaluating the legal profiles of the app; the working group strongly advised against both making its installation mandatory and implementing forms of incentive that restrict citizens' access to services that are otherwise freely available, or that constrain the exercise of freedom in the adoption of the app. Incentives such as greater freedom of movement, or facilities such as tax reductions or economic bonuses for those who download the app, might be unconstitutional[27]. The working group that investigated the legal profiles of contact tracing suggested, however, to introduce forms of 'soft incentive' for the App's installation, for example participation in a lottery, together with an awareness campaign. In my opinion some incentives could be, for example the possibility of receiving a bonus to download for free Apps for which, otherwise, you have to pay, or the increase in internet traffic available to the user. I believe that an awareness campaign is also needed to encourage people to cooperate in limiting the spread of the virus by downloading this App. To promote the App's download, video tutorials may be created and broadcast by official channels, in order to guide step by step the user in the installation, and assistance centers could also be set up to support users in using the App. Maintaining public trust in public health authorities and encouraging public cooperation in efforts to mitigate the virus, highlights the need to avoid a law-enforcement based, punitive approach to containment, which can be highly damaging and have far-reaching consequences for citizen wellbeing and trust.

At European level the guidelines have been laid down, in particular *Guidelines 04/2020 "on the use of location data and contact tracing tools in the context of COVID-19 outbreak"*[28], where is highlighted the need to ensure data protection, in particular in cases

[27] with regard to the Italian constitution, tax rules aimed at discouraging certain behaviours are of doubtful constitutionality in relation to art.53

[28] PDB, Guidelines 04/2020, 21 April 2020. Point 1, paragraph 4 "*the EPDB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness necessity, and proportionality must guide any measures adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19*".

of health emergency such as the one we are experiencing, to create the conditions for the social acceptability of actions or solutions aimed at guarantee the public health. This recognized the role that technology can play in such a complex case, that is to be a 'tool' to fight the virus and that its aim is not to control, but to strengthen this battle that the states and citizen are facing.

7. Right to data access and conclusions

An important aspect to focus our attention on is: When the user receives from the App a notification that informs him of the potential exposure to a contagion, will he have to put himself in quarantine on a fiduciary basis? Will he be obligated to a nominal identification? The first option, the voluntary one, implies that health authorities do not know the identity of the potential infected. In the second case, however, it is assumed that the authorities could also provide for sanctions against those who do not comply with the obligation to quarantine, as happens in China, where personal data are shared with the central authority. An analysis of the New York Times[29] has found that when the user grants access to personal data a portion of code named "reportInfoAndLocationToPolice" sends the name of the city, geolocation and a unique identification code to a server, to which law enforcement also has access. The latter, in fact, as explained by the state news agency Xinhua, would have been essential partners for the implementation of the system.
It is clear that in an emergent state, even in our democracies, the public power shows a marked predilection for the extensive use of technology for population surveillance, but would it be lawful to make your data available to the state for the control of a pandemic? Interference in the privacy of the citizen is likely to be more dangerous in terms of potential discrimination, and in relation to the correlation between the latter and the fact that the institution also has the regulatory power.
In addition, from a purely IT point of view, once a system of contact tracing centralizing the data of citizens, there is no absolute guarantee that data breach will not occur, putting at

[29] analysis available here: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

risk the information collected: in this case would be jeopardized data concerning the health, movements and personal relationships, whether this happens accidentally (an error) or for illicit purposes (an intentional action by hackers).

Some undemocratic States, first of all China, have been able to justify the adoption of tracking techniques to deal more effectively with the contagion, but in the near future such a surveillance apparatus for these regimes could prove to be a tool to control opponents, hinder the manifestations of dissent, limit public discussion, or otherwise intimidate potential dissidents. In a democratic country like ours, therefore, is it possible to imagine a system that fulfils the function of 'sustainable tracing' contacts? That acts in the protection of the fundamental rights of the citizen? Yes, there is a way to protect citizens' rights while implementing contact tracing policies based on the use of digital, without putting people's data at risk. The solution is based on the concept of *self-sovereign identity*: concept for which the information of the citizen is and remains in the hands of the citizen, and only the results of the processing of that information are shared. An intelligent contact tracing application, as seen above, does not have to store information collected in central servers to reconstruct the graph of infections. It must simply signal to the user that he has been in contact with a person at risk, and must ensure that it is the user - made aware of the risk - that communicates it to the health authorities for the due controls. This solution is based on the assumption that citizens are sufficiently responsible to get in touch with the authorities in case they risk being infected and are notified via the app.

The problem in the management of contact tracing is not deriving from the chosen technology, but from the cultural context; the need to focus on solidarity and civic sense of citizens is the real bet for the effectiveness of a contact tracing system that ensures total transparency and privacy.

Provided, of course, that the responsible action of the citizen corresponds to as much responsibility of the State in the best management of all the procedures following the self-reporting (for example, by minimizing voluntary isolation and accelerating testing times).

Therefore, to the basic question on how it is possible for a democracy to respond effectively to the emergency, I would answer with the words of Giuliano Amato[30], according to who the

[30] Giuliano Amato is an Italian politician who twice served as Prime Minister of Italy, first from 1992 to 1993 and again from 2000 to 2001. Later, he was Vice President of the Convention on the Future of Europe that drafted the European Constitution and headed the Amato Group. From 2006 to 2008, he was the Minister of

observance of restrictive measures in an authoritarian regime depends on an awareness of the strength of the repressive apparatus, while in a democracy, which, by its nature, can never be separated from the opinion and consent of citizens, it is necessary for the collective conscience to absorb the meaning of these measures and to make it its own.

the Interior in Romano Prodi's government. On 12 September 2013, President Giorgio Napolitano appointed him to the Constitutional Court of Italy, where he has served since then.

8. Bibliography

Law:
The General Data Protection Regulation (EU) 2016/679 (GDPR)

Research projects:
https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf
https://arxiv.org/pdf/2003.11511.pdf
https://www.store.rubbettinoeditore.it/downloadable/download/sample/sample_id/12/
http://www.giuri.unife.it/it/coronavirus/diritto-virale/sorveglianza-di-massa-e-prerogative-di-riservatezza-dellindividuo-durante-lemergenza-sars-cov-2-scenari-attuali-e-prospettive-future
http://www.giuri.unife.it/it/coronavirus/diritto-virale/democrazia-e-tutela-dei-diritti-fondamentali-ai-tempi-del-coronavirus
https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Webinar:
Covid-19 and data protection, 22 of April
Speakers: Gabriela Zanfir- Fortuna (Future Privacy Forum), Dennis-Kenji Kipker (University of Bremen)

Italian newspapers:
https://tedxcatania.com/diritti-inviolabili-e-doveri-inderogabili-un-confronto-tra-cina-e-italia-sul-covid-19/
https://www.agendadigitale.eu/cultura-digitale/immuni-come-funziona-lapp-italiana-contro-il-coronavirus/
https://www.open.online/2020/02/14/come-funzionano-le-app-cinesi-per-scoprire-se-avete-avuto-contatti-con-il-coronavirus/
https://www.ravennaedintorni.it/wp-content/uploads/2020/05/RD861-070520-WEB_OK-2.pdf?utm_source=www.ravennaedintorni.it&utm_medium=referral

https://www.globalproject.info/it/in_movimento/covid-and-human-tracking/22722
https://www.lastampa.it/tecnologia/news/2020/04/01/news/ecco-l-app-europea-per-il-tracciamento-che-combatte-il-coronavirus-rispettando-la-privacy-1.38665734

New York Times:
https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Official websites:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9295504
http://www.dirittoegiustizia.it/news/15/0000097985/La_tutela_dei_dati_personali_ai_tempi_del_Coronavirus_pandemia_versus_GDPR.html?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication
https://www.pepp-pt.org/

Chinese websites:
https://card.weibo.com/article/m/show/id/2309404476277724676278?_wb_client_=1
https://mp.weixin.qq.com/s/amB7fBxLw8KSR9DcUsbTWg
https://www.baidu.com
http://en.cetc.com.cn/enzgdzkj/about_us/introduction29/index.html
http://www.xinhuanet.com/tech/2020-02/19/c_1125596647.htm

Singapore Government agency website:
https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether