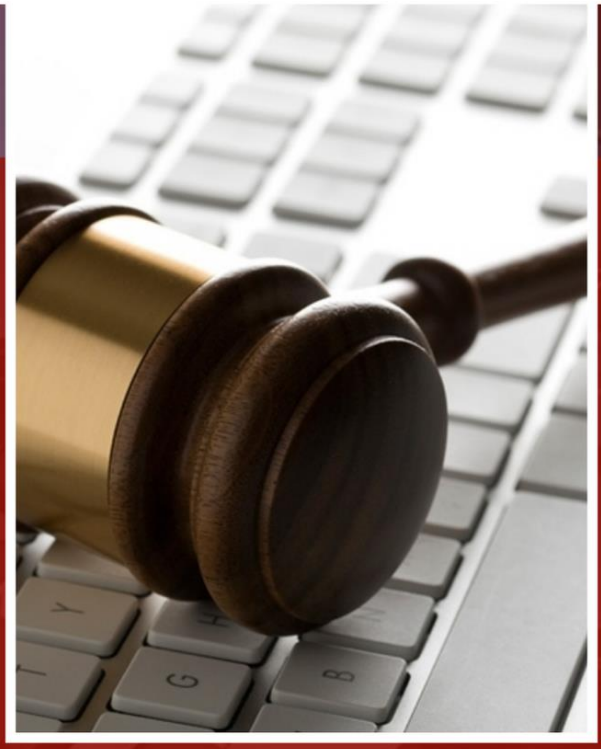
VOL. I/ISSUE I/2021

Cyberlaw University®

Education in Cyberlaw - A cut above the rest



A CYBERLAW UNIVERSITY INITIATIVE

CYBERLAW UNIVERSITY INTERNATIONAL E-JOURNAL

WWW.CYBERLAWUNIVERSITY.COM

CONTACT TRACING, MEDICAL DATA CONNECTED ISSUES & CHALLENGES

- **Abstract**

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing APPs - and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues Applicable to contact tracing across a range of key jurisdictions in real time.

Keywords: *Contact Tracing, COVID-19, Medical Data, Data Ownership, Privacy, Ethics, Cybersecurity, Culture of cybersecurity*

- **Introduction**

In the last decades we faced different pandemics from AIDS to Ebola in 2020 the term pandemic took the real meaning to be global and really creating a global concern, the "transversal" risk of death.

Scientific studies and evidences show that COVID-19 is more severe an illness than is seasonal influenza, and is more contagious than are seasonal influenza viruses, having a basic reproduction number (R0) nearly twice as high.

COVID-19 was declared a pandemic by WHO on March 11, 2020, the first non-influenza pandemic, affecting more than 200 countries and areas, with more than 5·9 million cases by May 31, 2020. Countries have developed strategies to deal with the COVID-19 pandemic that fit their epidemiological situations, capacities, and values.

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. Such "countermeasures", isolate infected people, locking down cities and countries, are not new, they recall medieval times plus some usual precautions in case of flue like to wash hands, keep a reasonable distance from other people, do not touch your mouth, nose or eyes with dirty hands and in case of close contact wear a surgery mask as Chinese and far eastern people use to wear since long time, nothing better and more up to date? Technology incredibly progressed though the time and more specifically cyber technology reinvented itself a number of times. We have crowd services, social media, IoT, sensors, AI, machine learning and any kind of privacy border line technology no chance to help fighting the pandemic? One of the first cyber tools to be identified was the contact tracing APPs rolled out to automate labour intensive tasks critical to containing the spread of the virus. Of course, the ability to trace in real-time our contacts impacts our privacy and in some way our freedom, let's get much more in detail on potential privacy infringements and the golden balance to be find between privacy and public health.

- **The Different Perception Of Privacy Issues**

We know that since long time ago our "activities" were traced[1], for instance, by credit card companies and later on by telecom operators, the pervasiveness of cyber tech increased a number of times such tracing opportunity, CCTV, IoT and sensors, mobile position aware devices enabled google to trace our daily life asking why we get to a specific location even showing some pictures we shoot there. Nevertheless, citizens are really concerned about privacy issues related to medical folders and contact tracing even if, they are not really concerned in case of sport and wellness APPs that use to transfer our medical data to some almost unknown centralised servers.

Unless we decide to move to the mountains, renouncing to today's technology, some tiny data that describes our behaviour and us will probably be tracked. No matter, you may say, we have nothing to hide, but what about the use, abuse or misuse others may do?

- **Contact Tracing Applications**

The pandemic moved the focus of already existent tracing application from security and marketing to interpersonal contacts, of course this sector was already active in the security field but become appealing to a wider set of software developers because of the incredibly wider potential application both on citizens and government side.

There are a number of issues and challenges connected with contact tracing applications. In the EU, the general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.

To start we can split into two main sectors both issues and challenges: citizens side and health authorities' side.

If on the citizens side the positive aspect is to be alerted if any existent contact is dangerous the key concern is about to limit the infringement of their privacy and have a clear trust relationship with the software company and the government including the unit responsible for storage of data. We all know that health[2] is probably to only sector where privacy is applicable even to the owner of data him or herself.

These privacy concerns mean even the choice to download / install and activate the application. For sure the discovery that time ago, the updated version of Android and IOS had a specific section devoted to connect with tracing APPs didn't enforce this trust relation knowing that anyway our phones are already traced by Telcos.

Since the start of the pandemic, governments and stakeholders involved in the fight against the virus, such as the scientific research community, have been relying on data analytics and digital technologies to address this novel threat. Governments and private actors turned toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns. In the EU, the GDPR data protection legal framework was designed to be flexible and, as

[1]Ronchi, A.(2019) , eCitizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer
[2]Ronchi, Alfredo M., (2019). e-Services: Toward a New Model of (Inter)active Community, ISBN 978- 3-030-01842-9, Springer (D)

such, is able to achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.
There are a number of paragraphs within the UN Declaration of Human Rights[3] related to the management of the pandemic let's recall two of them: *Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. Article 13: 1. Everyone has the right to freedom of movement and residence within the borders of each State; 2. Everyone has the right to leave any country, including his own, and to return to his country.*

Data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European, if not global, approach in response to the similar crisis, or at least put in place an interoperable framework.

On the side of health authorities apart from the need to ensure the full Institutional ownership of data ensuring no data leak or improper use, misuse of information, one of the key aspects is the widest installation and activation of the tracing tool. The return value of such campaign is useful and relevant only if a significant part of the citizens activates it.

A draft list of the key aspects to be considered is:

- Widespread number of citizens installing and activating the application;
- A comprehensive national epidemiologic strategy articulating instrumental support to the public health system, manual contact tracing;
- The model chosen (technology used, architecture retained, definition of 'proximity' between the devices, both in terms of distance and duration, etc.);
- Widespread access to mobile devices and connection (considerable segments of the population are unable to acquire or use them, in particular high-risk groups such as healthcare personnel, disabled and elderly people).

- **Specific regulations in Europe**

The Council of Europe issued a Joint Statement on Digital Contact Tracing on 28 April 2020 One month after the first Joint Declaration on the right to data protection in the context of the COVID-19 pandemic.

"*Recalling that the data protection standards, laid down by Convention 108 and its modernised version, Convention 108+, are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health, it is crucial to ensure that the necessary data protection safeguards are implemented when adopting extraordinary measures to protect public health*."

The council of Europe outlined that "*Regarding the use of mobile data and technology in the fight against COVID-19, specific measures are being deployed or otherwise proposed and include: use of mobile location data to evaluate movements of population or to enforce confinement measures,*

[3]United Nations (1948). *Universal Declaration of Human Rights*. [online] . Available at: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf. [Accessed 8 Feb. 2021].

use of devices as digital proof of immunity, symptoms' detection, self-testing, or finally digital tracing of the contacts of an infected person."

The European Union, in order to be compliant with Directive 95/46/EC (GDPR) adopted the following "*Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*" - Adopted on 21 April 2020.

The World Health Organisation didn't perform adequately providing late advice and controversial recommendations.

Key points of these guidelines are:

- Use of location data,
- Sources of location data;
- Focus on the use of anonymised data;
- Contact tracing applications;
- General legal analysis;
- Recommendations and functional requirements.

Plus, a guide for the analysis of contact tracing applications. The first paragraph of the guide states that "*publishers of contact tracing applications should consider the following criteria:*

- *The use of such an application must be strictly voluntary. It may not condition the access to any rights guaranteed by law. Individuals must have full control over their data at all times, and should be able to choose freely to use such an application.*
- *Contact tracing applications are likely to result in a high risk to the rights and freedoms of natural persons and to require a data protection impact assessment to be conducted prior to their deployment.*
- *Information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data*."
- *When a user is diagnosed infected with the SARS-Cov-2*[4] *virus, only the persons with whom the user has been in close contact within the epidemiologically relevant retention period for contact tracing, should be informed.*"

Successful initiative or not? Here are some figures (November 2020):

Country	**Name of the APP**	**Download**	**Population**
Italy	Immuni	7 mio	60.40 mio
United Kingdom	Nhs Covid-19	12 mio	66,65 mio
Germany	Corona Warn	18,8 mio	83 mio
France	StopCovid / TousAntiCovid	3 mio	66.99 mio

[4] Alias COVID-19

Swiss	SwissCovid	2,8 mio	8,55 mio

- **National initiatives**

Major part of the countries around the world decided to structure the fight against the pandemic on three main action lines:

- ❖ Health - healthcare guidelines and pharma;
- ❖ Laws and Regulations - ad hoc regulations and recommendations;
- ❖ Technology - information technology tools and APPs.

The health sector at national level, after a first unappropriated attempt to "close the borders" to the virus, issued general and specific recommendations to mitigate the risks trying to harmonize the different initiatives or at least take advantage from other's experiences and solutions.

The first two actions were not so different from the one taken on the occasion of historical pandemic, one of the attempts to create a new "weapon" to defeat the disease come from the technological sector. Tracing applications were already developed and running in the security sector from passengers shadowing to GPS or phone cell triangulation and more. The basic concept was to be able to trace citizens thanks to their mobile phones thank to an APP that will be able to alert them in case of dangerous contacts, all this without infringing privacy issues and potential malicious use of data.

As already outlined we waived some of rights to improve our safety or access some services and communication opportunity. The contact tracing APP can succeed only if a relevant number of citizens will install and activate it that means that a trust relationship between citizens and the "APP party" must be strong. Where "APP party" means the government, data managers and controllers, software developers and telecom operators. Let's have a look to some potential vulnerabilities.

- **Cybersecurity: APPs main vulnerabilities**

Hacking[5] a decade ago was exclusively reserved for the professionals, white-hat hackers, penetration testers; whose duty it was to break through the firewall of corporate and personal security. Nowadays the scenario is quite different, "professional" white-hat hackers are a small portion of hackers, basic hacking techniques are available on line on the Internet and more sophisticate or cutting edge are exchanged on the dark net, in addition the increasing "hacking as a service" offer is boosting business and "family[6]" affairs.

Dealing with COVID 19 contact tracking APPs since data strictly related to personal health conditions are taken into consideration, the choice of the safety model to be adopted is a paramount. What would happen if once a "Governmental APP" was installed, it was hacked and compromised the content of the smart phone itself by some criminal? Undermining the integrity of the APP could allow not only to steal or compromise data, but also to take full possession of the device of those who installed the software on their device. In Europe contact tracing applications are installed on voluntary basis as stated by EU regulations this "voluntary" mode of the APP implies that no

[5]Ronchi, A.(2019) , eCitizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer

[6]Illegal access to private email and mobile phone messages to find evidences of betryals and more.

negative consequences can be associated with a person's refusal to use the APP. Thus, screening tests, care, the ability to travel, access to certain services (e.g. public transport) cannot be made conditional on the use of contact tracing APPs. This has direct impact to employers, who may not subordinate certain rights to the use of these APPs, as this would amount to discrimination. Besides, an employer cannot compel their employees to download the APP.

First of all, it must be remembered that many defects in software applications, IT processes or communications protocols do not have a real solution and, due to a closed flaw, new ones are opened; it is the never-ending competition between attacks and counter measures. Due to this reason, cyber security observers attest every year to an exponential increase in cybercrime attacks on our devices, which are the preferred victims of hackers mainly due to their capillary presence and the reduced skills or will to invest time to protect them constantly. This even if smart phones and sometimes tablets are the custodians of our most precious sensitive data (IDs including digital ones, bank account access tools, credit cards, social security, etc.).

Recent reports by security companies Palo Alto Networks[7] and Bitdefender[8] attest to how cybercriminals focus their attacks on the countries hardest hit by Covid-19, such as Italy. The Clusit (Italian Association on Cybersecurity) 2020 Report[9] also underlines that the attacks no longer start from individual web pirates, but from organized groups that base their business, for example, on knowledge of a person's health conditions. The interest is therefore very high and it is easy to expect continuous cyber-attacks.

To secure APPs it will be necessary to verify that the most serious vulnerabilities have been carefully considered, including those listed below:

SIM Jacker: serious security flaw in the devices that use SIM cards for their operation, so not only phones, but also IoT products. How does the attack happen? Simply through an ad hoc SMS, sent by an attacker to his victim who, not noticing anything (the SMS does not appear!), Finds himself with a phone spying on him;

Sniffing BLE (Bluetooth Low Energy) Long-Lived: Vulnerability that exploits Bluetooth transmissions. This vulnerability is present in the Bluetooth protocol, in particular in the implementation of BLE chosen, as suggested by the European Data Protection Supervisor(EDPS)[10], to operate some contact tracking APPs. The attack allows you to spy on the victim by bypassing the protection used by the devices. In this way it is possible to track a person, collecting details in reference to his location and other potentially sensitive information;

Knob: defect in the Bluetooth standard, whereby in an outdated system an attacker can decrypt the information exchanged by the two devices and access our data, or listen to our conversations.

---

[7]https://www.paloaltonetworks.com[Accessed 8 Feb. 2021].
[8]Bitdefender.com. (2017). *Bitdefender - Global Leader in Cybersecurity Software*. [online] Available at: https://www.bitdefender.com/ [Accessed 8 Feb. 2021].

[9]Clusit (2020). *Rapporto Clusit*. [online] Clusit. Available at: https://clusit.it/rAPPorto-clusit/ [Accessed 8 Feb. 2021].

[10]European Data Protection Supervisor - European Data Protection Supervisor. (2021). *European Data Protection Supervisor*. [online] Available at: https://edps.europa.eu/ [Accessed 8 Feb. 2021].

ToRPEDO & PIERCER[11]: A group of researchers from Purdue University and the University of Iowa revealed that 4G and 5G network protocols suffer from a number of vulnerabilities that would allow hackers to access users' phone calls and track their location.

Additional concerns to be carefully considered relates to the use of a centralized server instead of a distributed or partially distributed one. The use of a centralised server increases the risk of possible cyber-attacks and the temptation to exploit this data for purposes other than those provided for by law. Of course due to the GDPR[12] and national regulations the server must be physically located in the EU and run under the European Data Protection Supervisor recommendations.

Potential discrimination – people who do not use the APP delivered on voluntary basis might not be able to work or access certain public places freely, meaning their consent was not freely given and therefore is void.

Potential "Big Brother" Surveillance – in the event that the APP is adopted by part of the population, it is feared that the Government may more easily impose it on the rest of the population against their will. Moreover, if the APP is not based on pure anonymization[13] – that means that it is at best pseudonymous[14], users will not be protected against any kind of individual surveillance[15].

Security acclimatization – once the APP is deployed and activated, it will be easier for the Government to add coercive functions to it (individual control of lockdown). Moreover, the APP could provide an incentive to subject one's body to constant surveillance, which will reinforce the social acceptability of other technologies, such as facial recognition or automated video surveillance, which are currently widely rejected. This is in some way what is usually termed "Bad ambassador effect". To what extent are we willing to give up our privacy and freedom to increase safety, security and top down control? Let's have a look to some contact tracing APPs.

- **Italyas at November 2, 2020**

On 29 April 2020 the Italian Government issued a law decree setting out the rules governing the adoption of a tracing APP (Law Decree no. 28 of 30 April 2020[16], the Decree). On June 15, after a beta test in four regions, the APP has been made available to citizens on voluntary basis.

---

11 Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information
12GDPR.eu. (2019). *General Data Protection Regulation (GDPR) Compliance Guidelines*. [online] Available at: https://gdpr.eu/ [Accessed 8 Feb. 2021].

[13]Department of Health and Social Care (2020). *NHS COVID-19 app: anonymisation, definitions and user data journeys*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys [Accessed 8 Feb. 2021].

[14]Prime Factors. (2020). *Psuedonymzation & Anonymization of Data - Prime Factors*. [online] Available at: https://www.primefactors.com/solutions/pseudonymization-anonymization/ [Accessed 8 Feb. 2021].

[15]Pseudonymous data is information that no longer allows the identification of an individual without additional information and is kept separate from it. In exchange for the lower level of privacy intrusion, the applicable requirements are less stringent.

[16]Gazzettaufficiale.it. (2020). *Gazzetta Ufficiale*. [online] Available at: https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg [Accessed 8 Feb. 2021].

User tracing APPs must comply with both GDPR and strict Italian rules on remote monitoring of employees (Private Sector). Main privacy concerns and potential misuse lie in data minimization, data security, re-identification risk and actual prevention of re-use of such data for other purposes. A government wide-spread concern was about ownership and localization, in addition the data controller must be the Ministry of Health, and that data must be stored in servers on the Italian territory.

The Data Privacy Authority[17] considers that the Decree on the APP complies with national regulations and with European Data Protection Board (EDPB)[18] guidelines. The Italian Data Processing Authority[19] has issued an opinion on the Decree, a note on the DPIA, and authorization to the Ministry of Health in its quality of data controller for the data processed through the APP.
The name of APP is Immuni[20]. The activation of the APP, as already stated, is voluntary and there is no need to use it to enter public spaces. Limitations are not mitigated by the use of the APP.

To download the APP few information are required (province of domicile and to be aged over 14) no registration/account required. As major part of the tracing APPs contacts is traced thanks to a Bluetooth interface, the GPS signal or any other position detection tool cannot be used accordingly with EU and national regulations. The APP generates a one-time identifier the "key" to be exchanged on the occasion of a contact with an active Immuni APP, data collected are stored in a semi-centralised data base. The Decree requires a 'suitable level of security" to be adopted. Anonymization or (if not possible) pseudonymization is required.

The centralised server stores the keys uploaded by infected users plus some other data while the keys of contacts are stored locally in the smart phone memory. The application uses the "privacy by design" approach and pursuant to the Decree, a data processing impact assessment has been carried out. Keys of contacts are stored on each device for 14 days. The same retention period applies to keys uploaded by infected users on the centralized server. In any event, no data can be retained until the end of the state of emergency and in any case not later than 31 December 2020 (new regulations will be issued).

How does this APP works mush more in detail? Once installed, the APP causes the smartphone to continuously emit a low energy Bluetooth signal (BLE), with a proximity identifier. When they come into contact with each other, smartphones record each other's proximity identifier in their memory, keeping track of that contact, how long it lasted and the distance between the devices.
The identification code is temporary and anonymous, it varies often to minimize continuous tracking risks and allows the APP to establish a contagion risk assessment for each contact, based on the information uploaded voluntarily by users.

---

[17]Garanteprivacy.it. (2016). *The Italian Data Protection Authority: Who We Are*. [online] Available at: https://www.garanteprivacy.it/home_en/who_we_are [Accessed 8 Feb. 2021].

[18]European Data Protection Board - European Data Protection Board. (2021). *European Data Protection Board*. [online] Available at: https://edpb.europa.eu/edpb_en [Accessed 8 Feb. 2021].

[19]Garanteprivacy.it. (2018). *Home*. [online] Available at: https://www.garanteprivacy.it/home_en [Accessed 8 Feb. 2021].

[20]Italia.it. (2020). *Immuni - Sito Ufficiale*. [online] Available at: https://www.immuni.italia.it/ [Accessed 8 Feb. 2021].

In fact, a user who tested positive for Covid-19 can personally upload the cryptographic keys to a server to trace his proximity identifier. For each user, the APP periodically downloads from the server the new cryptographic keys uploaded by users who tested positive for the virus, derives their proximity identifiers and checks if any of those identifiers correspond to those recorded in the smartphone memory in the previous days. If the APP registers that you have been close to someone positive for the virus, it will check if the duration and distance of the contact could have caused the infection. If so, the APP can send notification messages to instruct you to isolate yourself and contact the health authority.

In the beta and first version of the application a "clinical diary" function, where users can record the progress of their symptoms, was included, in the latest versions has been removed.
Accordingly, with the official figures on November 2020 the APP Immuni was downloaded by seven million citizens there are no data regarding the activation of the downloaded APPs.

- **France as at December 2, 2020**

On May 29, 2020 France government published a decree (*Decree No. 2020-650 of May 29, 2020 relating to data processing known as "StopCovid"*) setting the definitive legal framework for the implementation of the contact tracing APP. On June 2, 2020 INRIA[21] (National Institute for Research in Digital Science and Technology) released to the public the APP StopCovid.

On October 22, 2020 the Government presented a new version of the APP named "TousAntiCovid". Officially, as stated by the Health Ministry, TousAntiCovid is an update of the latest version of StopCovid. TousAntiCovid provides easy access to other tools including *"DepistageCovid"*, which provides a map of nearby testing centres and waiting times, and *"MesConseilsCovid"*, which provides personalised advice on how to protect oneself and others.

Both StopCovid and the following version TousAntiCovid[22] are available on voluntary basis, no information will be needed to download and register the APP.

The APP will generate ephemeral crypto-identifiers (e.g. every 15 minutes) associated to the terminal (and not the person) to trace contacts via Bluetooth, no GPS location aware systems are in use.Of course, if we look at the "anonymisation" of the user applying the Aristotelian syllogism the crypto-identifiers are associated to the terminal (and not to the person) and the terminal is associated to the person via IMEI, SIM, MAC we derive that the crypto-identifiers are associated to the person.

Thus, the APP is not considered to anonymously trace positive to COVID citizens but it is at best pseudonymous. If a user is clinically diagnosed or is tested positive for COVID-19, he or she can choose to report it to the APP and to transmit his or her proximity history to the centralised server.
Each smartphone that has downloaded the APP regularly checks with this central server to see if its crypto-identifiers are among those at risk. If they are, the APP will generate an alert sent to the user, to indicate that he/she might have been exposed to the virus, and the measures to be taken.

---

[21]Inria.fr. (2021). *Accueil | Inria*. [online] Available at: https://www.inria.fr/en [Accessed 8 Feb. 2021].

[22]Gouv.fr. (2021). *TousAntiCovid*. [online] Available at: https://bonjour.tousanticovid.gouv.fr/index-en.html [Accessed 8 Feb. 2021].

The decision to use a centralised server has been the subject of much criticism. It has been abandoned in Germany, which opted for a decentralized system. France Government considers that the centralised architecture offers more guarantees and security. Proximity history data recorded by the APP on the mobile phone are kept for 15 days from the time they are recorded. When this data is shared on the central server, it is also kept for 15 days from the time it is recorded. The shared authentication key and the crypto-identifiers are retained until the user uninstalls TousAntiCovid and in any event no later than six months after the end of the state of health emergency in France (currently set to be February 16, 2021). The APP can be uninstalled at any time.

Accordingly, with the official figures on November 2020 since its launch, the APP has been downloaded by almost 9.5 million people.More than 13,000 people have been notified as having been in contact with an infected person.

Some remarks concerning privacy issues, a French researcher in cryptography[23], few weeks after the release of the first version of StopCovid explained that the APP collects more data than originally understood. His findings show that all cross-contacts are sent to the central server, contrary to the government guidance which states that only the APP users who had been in contact for 15 minutes, closer than **one meter** away from a person who tested positive for COVID-19 would be stored, meaning that the APP processes more data than necessary to trace the spread of the virus, this represent an infringement to the data minimization principle. The second version of StopCovid, launched at the end of June, remedied this problem, but the French Data Protection Authority (the "CNIL[24]") noted that this second version still contained certain shortcomings concerning user information, the subcontracting contract granted to INRIA and certain data processing aimed at securing the APP. Therefore, the CNIL gave the Health Ministry formal notice to remedy this on July 20, 2020. Following the formal notice, as the CNIL considered the processing implemented were now compliant with the EU and French legislative data protection requirements, it declared the closure of the formal notice on September 3, 2020.

- **Germany As at June 23, 2020**

On June 16, 2020 the German Federal Government launched an official APP "Corona-Warn-APP[25]" which was developed by SAP[26] and Telekom[27] on behalf of the German Federal Government. The "Corona-Warn-APP" is based on the Privacy-Preserving Contact Tracing[28] ("PEPP-IT").

---

[23]Gaëtan Leurent, researcher at Inria in the team COSMIQ, working on symmetric cryptography.

[24]Cnil.fr. (2016). *CNIL* |. [online] Available at: https://www.cnil.fr/ [Accessed 8 Feb. 2021].

[25]Coronawarn.app. (2020). *Open-Source Project Corona-Warn-App*. [online] Available at: https://www.coronawarn.app/en/ [Accessed 8 Feb. 2021].

[26]SAP. (2017). *SAP Software Solutions | Business Applications and Technology*. [online] Available at: https://www.sap.com/index.html [Accessed 8 Feb. 2021].

[27]Deutsche Telekom AG (2020). *Home*. [online] Telekom.com. Available at: https://www.telekom.com/en [Accessed 8 Feb. 2021].

[28]Klaine, P.V., Zhang, L., Zhou, B., Sun, Y., Xu, H. and Imran, M. (2020). Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic. *IEEE Internet of Things Magazine*, [online] 3(3), pp.58–63. Available at: https://ieeexplore.ieee.org/document/9241473?denied= [Accessed 8 Feb. 2021].

The German contact tracing APP and its backend infrastructure is entirely open source licensed under the Apache 2.0 license. The Corona-Warn-APP is being developed on basis of the Exposure Notification Framework ("ENF")[29] provided by Apple and Google, which will use Bluetooth Low Energy technology ("BLE")[30]. The Exposure Notification framework defines two user roles:
Affected user
"*When a user has a confirmed or probable diagnosis of COVID-19 (as defined by the Health Authority), the framework identifies them as affected and shares their diagnosis keys to alert other users to potential exposure."*
Potentially exposed user
"*To assign a user the potentially exposed role, use the framework to determine whether a set of temporary exposure keys indicate proximity to an affected user. If so, the app can retrieve additional information such as date and duration from the framework.*"

The Corona-Warn-APP will collect pseudonymous data from nearby mobile phones using BLE. As soon as two users approach each other within a distance of about two meters and remain at this distance for fifteen minutes or longer, their APPs will exchange data via BLE. If a user tests positive for COVID-19, the user can feed the test result into his/her Corona-Warn-APP. The Corona-Warn-APP will then anonymously inform all stored contacts. The data will be stored locally on each device preventing access and control over data by authorities or a third party.

"Corona-Warn-APP" and privacy issues; there are no major privacy concerns as the Corona-Warn-APP has been designed with a special focus on privacy from the beginning. The German Data Protection Authorities[31] generally support the Corona-Warn-APP and only expressed minor concerns, but less on the Corona-Warn-APP itself but rather on the way it may be used by IT key players.
As Apple and Google, as providers of the operating systems, have access to all data that runs over their interfaces, there are some concerns regarding the behaviour of Apple and Google.

The Corona-Warn-APP is deployed on voluntary basis but this aspect of could be undermined through social or economic pressure which could be specifically enforced by employers. As already expressed in the previous paragraph regarding anonymity issues, the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit[32]) announced that the use of the telephone-Tan-registration is not an optimal solution because the complete anonymity of the user will no longer be guaranteed.

---

[29]Apple.com. (2020). *Apple Developer Documentation*. [online] Available at: https://developer.apple.com/documentation/exposurenotification [Accessed 8 Feb. 2021].Exposure Notifications: Helping fight COVID-19 - Google. (2021). *Exposure Notifications: Helping fight COVID-19 - Google*. [online] Available at: https://www.google.com/covid19/exposurenotifications/ [Accessed 8 Feb. 2021].

[30]Bluetooth® Technology Website. (2017). *Intro to Bluetooth Low Energy | Bluetooth® Technology Website*. [online] Available at: https://www.bluetooth.com/bluetooth-resources/intro-to-bluetooth-low-energy/ [Accessed 8 Feb. 2021].

[31]Bund.de. (2020). *Internetauftritt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - Homepage*. [online] Available at: https://www.bfdi.bund.de/EN/Home/home_node.html [Accessed 8 Feb. 2021].

[32]Bund.de. (2021). *Internetauftritt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - Startseite*. [online] Available at: https://www.bfdi.bund.de/DE/Home/home_node.html [Accessed 8 Feb. 2021].

Currently there is one other APP available in Germany launched by Robert Koch Institute[33] (German federal government agency and research institute responsible for disease control and prevention, "RKI") – "Datenspende-APP[34]". This APP does not yet trace contacts, but only general movement and fitness information. The APP collects the user data using their fitness tracker and sends it to the RKI. The RKI analysis anomalies in the data, which is sorted by postcode: As pulse rate, sleep rhythm and activity level change due to an acute respiratory disease, the RKI claims that it can also indicate a Covid-19 disease having this data.

At the beginning of April 2020, RKI launched the official Corona Data Donation App. Since then, 529.281 German inhabitants have decided to donate their data. Some of you may be asking yourselves questions about the purpose of this project and the expected scientific results. On this site, RKI would like to give the donor, a glimpse into the scientific process by sharing findings as RKI uncover them. To achieve this transparency, RKI regularly posts updates detailing the methodological approaches and interim results of analyses creating a Fever Map for Germany using vital signals collected by wearable health and fitness tracking devices and donated by sponsors.
The aim of this map is to detect regions in which the number of residents exhibiting fever symptoms is higher than average. By updating the map on a daily and municipality-level basis, RKI aims to identify so-called "hot spots" of COVID-19 as they emerge.

There are several concerns indicated by Chaos Computer Club[35], a cyber security NGO, in particular:

- ❖ RKI can directly retrieve the fitness data from the provider of the fitness tracker as the smart bracelet and wrist watch or Google Fit and only then the data will be pseudonymized (except Apple Health). As the RKI also stores access data to the fitness tracker, it can be used to access complete history and names of the users.
- ❖ Easy reversal of the pseudonymisation and the insecure handling of the confidential pseudonym as the APP does not use a standard browser but an embedded web view which is insecure due to man-in-the-middle attacks.
- ❖ The RKI server exposes additional functionality such as a management and admin interface as well as a SOAP API via the Internet. This increases its vulnerability."

- **What about China[36] ?**

Over 20 million people in three Chinese cities were under lockdown as of Friday 24 January 2020 morning, as authorities battled an outbreak of a novel coronavirus first discovered at the beginning of January in Wuhan, China, in the central province of Hubei. The strong Chinese measures came

[33]Www.rki.de. (2020). *RKI - Homepage*. [online] Available at: https://www.rki.de/EN/Home/homepage_node.html [Accessed 8 Feb. 2021].

[34]Www.rki.de. (2021). *RKI - Coronavirus SARS-CoV-2 - Corona-Datenspende-App*. [online] Available at: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende-allgemein.html [Accessed 8 Feb. 2021].Koch-Institut, R. (2020). *Corona Datenspende*. [online] Science Blog. Available at: https://corona-datenspende.de/science/ [Accessed 8 Feb. 2021].

[35]Www.ccc.de. (2020). *CCC | Home*. [online] Available at: https://www.ccc.de/en/ [Accessed 8 Feb. 2021].

[36]Updated 24 January, 2020

after the World Health Organization[37] decided not to declare the outbreak a "public health emergency of international concern" (PHEIC)."[38]

On January2020 China declared the Health Emergency in the city of Wuhan and Hubei Province; this paragraph offers a quick overview on the different strategies adopted by Chinese Government after the health emergency this before setting the focus on contact tracing applications as key tool to detect cases and manage them. China embraced two main strategies, "Containment" and "Suppression". As outlined by Chinese researchers[39] "*Strategy decisions were based on factors including feasibility of interrupting virus transmission, estimates of disease severity, projected social and economic effects of strategy and disease, public acceptance and willingness, and last but not the least, government willpower and capacity.*" In addition to these two main strategies there was a third one "mitigation", which has not been implemented in China, include similar or overlapping measures. Comparison of the three basic strategies shows that all use non-pharmaceutical interventions as outlined in the following lines.

"Containment" strategy applies to an early-stage epidemic in a geographically limited area, taking measures that prevent person-to-person transmission of SARS-CoV-2[40] and importation and exportation of infection. The core measures of a containment strategy are proactive finding and managing cases, tracing and quarantining close contacts, and strict restriction or control of population movement when feasible and appropriate.

Maximum timeliness was requested from hospitals, laboratories and prevention departments to test, treat and isolate each suspected case and trace and isolate contacts in the shortest possible time (the time elapsed from the onset of symptoms to diagnosis went from 12 days in January to just 3 days in early February): statistical models have shown that it was above all this that reduced the number of infected and dead, compared to travel and contact restrictions. Without these measures, the number of infections would have been about 67 times greater, as some experts stated.

Core measures are summarised in:
Aim: Stop virus transmission and spread.
Scenario: Early stage of epidemic in well-defined areas.
Case detection and management: Active case detection; managed isolation and care; quarantine of close contacts.
Lockdown and intercity travel prohibition: Lockdown of endemic areas; restrict travel from those areas to other low epidemic areas.
Other physical distancing: Strict stay-at-home orders; school closure; cancellation of mass gatherings.
Personal protection: Hand hygiene; respiratory etiquette; face mask use.
Duration: Short term, followed by maintenance of elimination of transmission.

---

[37]Who.int. (2018). *Home*. [online] Available at: https://www.who.int/ [Accessed 8 Feb. 2021].

[38]https://www.facebook.com/HealthPolicyWatch (2020). *WHO Refrains From Declaring Public Health Emergency Now Over Coronavirus Virus Outbreak; But 3 Chinese Cities On Lockdown - Health Policy Watch*. [online] Health Policy Watch. Available at: https://healthpolicy-watch.news/wuhan-china-goes-on-lockdown-who-postpones-decision-on-public-health-emergency-over-virus-outbreak/ [Accessed 8 Feb. 2021].

[39]Zhongjie Li, Qiulan Chen, Luzhao Feng et al. Active case finding with case management: the key to tackling the COVID-19 pandemic. The Lancet https://doi.org/10.1016/S0140-6736(20)31278-2 (published on line June 4, 2020)

[40] Alias COVID -19 in news

Endpoint: Vaccine response to immunise the population to achieve community protection.
Pros: Early, proactive, and strict implementation can be effective, largely preventing infection and death.
Cons: Major short-term effect on daily life and social and economic costs; continued moderate socioeconomic effects during elimination period.

The second strategy applied was that of "Suppression", after the containment strategy has been successful and only sporadic cases and small outbreaks remain. "Suppression" strategy is useful when an epidemic is in multiple areas with varying degrees of outbreak and community spread, when it is not possible or feasible to stop spreading by confining transmission to an isolatable geographical area.

In this case, the goal is to keep the infection reproduction index (R0) low (below 1) and prevent the importation of cases. In this phase, the lockdown measures are gradually loosened (reopening of schools, restaurants and shops, etc.) even if maximum control is exercised on individual cases and small outbreaks with the restoration, if necessary, of containment measures. People who move between areas at different risk report it online or via a telephone application, which also supports in China public health operators in tracking contacts. Naturally, physical distancing and personal hygiene measures, the obligation to wear masks indoors and the ban on gatherings remain in force.

Core measures are similar to those for containment and are summarised in:
Aim: Decrease or stop community transmission.
Scenario: Ongoing community transmission in which containment is not feasible.
Case detection and management: Case detection; managed isolation and care; testing of close contacts.
Lockdown and intercity travel prohibition: Few, based on risk-
Other physical distancing: Stay-at-home orders; school closure; cancellation of mass gatherings; adjustable to conditions.
Personal protection: Hand hygiene; respiratory etiquette; mask use.
Duration: Long term, adjusting suppression measures based on epidemic situation (relax or strengthen periodically).
Endpoint: Vaccine response to protect the vulnerable, stop community transmission, and achieve community protection.
Pros: Early, proactive, and strict implementation can be effective, largely preventing infection and death.
Cons: Major short-term effect on daily life and social and economic costs; premature relaxing of interventions can lead to rebound of the epidemic.

"Suppression" logically follows successful "Containment" to prevent spread from imported cases and re-establishment of community transmission. Suppression measures can keep transmission and prevalence low, decreasing the effective reproduction number (Re). Once Re is below 1 in a community, spread in that community should eventually stop. However, maintenance of strict suppression measures, particularly lockdowns and physical distancing, brings a large socioeconomic burden.

The third strategy not implemented in China, is "Mitigation", the key aspects of Mitigation are:
Aim: Lower and delay the epidemic surge to reduce health-care demand.
Scenario: Extensive community transmission, impossible to suppress.
Case detection and management: Detection of severe cases; managed isolation and care; limited contact tracing.

Lockdown and intercity travel prohibition: None.
Other physical distancing: Cancellation of mass gatherings; school closure when and where necessary; ask vulnerable population to stay at home.
Personal protection: Hand hygiene; respiratory etiquette; face mask use.
Duration: Long term.
Endpoint: Vaccine response to protect the vulnerable, stop endemic transmission, and immunise the population to achieve community protection.
Pros: Less short-term socioeconomic effect; necessary medical care able to be provided.
Cons: Medical system capacity can still be exceeded; substantial risk of high morbidity, mortality, and economic damage.

To enforce case detection and management the Ministry of Information Industry Technology after the COVID-19 crisis outbreak decided to take advantage from an ad-hoc information technology platform. The Chinese Government encouraged the introduction of APPs for the dynamic certification of health status in a notice released by the State Council[41] Joint Defence or Control Mechanism in February 2020.

Based on this platform, telecom carriers (China Mobile, China Unicom and China Telecom[42]) may provide a tracking record of the cell phone users' location in the past 15 days or up to 30 days.

On the citizens side, various APPs with similar functions were introduced in different regions of China to achieve a dynamic certification of health status of the local residents. Different status (red, yellow or green) will impose a different level of restrictions or regulations. The name of such applications is "Health Code" or similar name which can be a separate APP or integrated into Alipay and WeChat. The download and activation of the APP is voluntary, whilst not technically compulsory, a clean result (i.e. green status) of the APP, the "health code", is required to be presented for access to certain public buildings or areas.

The purpose of the "health code" system is to control and monitor movements around China based on the risk profile of a user. Individuals are allocated a QR "health code" which is either green (low risk and free to move around), amber (which means at risk and must quarantine for seven days in some regions) or red (which means high risk and must quarantine for 14 days in some regions).

QR codes must be scanned before entering public places such as subway stations and shopping malls, and in some cities, before leaving apartment complexes and access will be denied and the authorities alerted if the individual should be in quarantine in accordance with their QR health code. The clean result of the APP is compulsory when the user goes to hospital or tourist sites and certain other locations; employers and owners of office buildings may require clean results of location tracking records before the resumption of work. Furthermore, some public workplaces may require visitors to provide dynamic certification of health status before granting access.

[41]Www.gov.cn. (2021). *The State Council of the People's Republic of China*. [online] Available at: http://english.www.gov.cn/ [Accessed 8 Feb. 2021].

[42]Founded in September 2000, China Telecom is a large state-owned communication backbone enterprise. China Telecom owns the technology-leading mobile communication network. It provides global customers with comprehensive information services and customer service channel system covering all regions and services. As one of the most critical technology revolution, the development and application of Artificial Intelligence technology have risen to the level of national strategy.

Some newspaper said that in practice, not all the operators of public workplaces, e.g. office buildings or restaurants, are strictly implementing the restriction of access based on the results of the APP.

With reference to privacy issues, following the Chinese laws and regulations when the personal data is collected and used for public security purposes, no consent from individuals providing it is required. This is the principle established by the Personal Data Security Specifications. The notice issued by the Cybersecurity Administration of China supporting mechanisms to control COVID-19 (Notice) provides that entities authorized by National Health Committee are entitled to collect this data without consent.In practice, both the Government or authorized private sector organizations may have access to personal data, but the mechanism for the processing, use and storage of the personal data lacks transparency, with the potential for abuse of personal data in the future.

Some additional remarks from Chinese citizens, they consider that information collected is excessive. To use the APP citizens must provide: Name, ID card number and facial scan. The exact data varies with the APPs. Users are required to complete a detailed questionnaire setting out medical and travel history, national identity number, possible symptoms they may have etc.

The technology rationale of these APPs is not publicly available, but it is based on the records of the individuals' location (GPS, triangulation?). No official information about the use of centralised servers, the identity and basic information of the infected user must be reported to the Disease Control and Prevention Centre(China CDC)[43]within a designated timeline. Based on the investigation and management guidelines of "contiguous", the contiguous must fill out the relevant forms and report to the local Disease Control and Prevention Centre. Both the contiguous' and the infected user's identity is required to be filled out by the "contiguous".

In general, in compliance with Chinese laws and regulations no consent is requested to upload and share information, e.g. the APP used in Beijing does not require consent to share or upload the data;outside of Beijing there are regional differences in the APP.

More in detail the APP used in Beijing only generally indicates that data collection is compliant with the law and only for the purpose related to COVID-19, without incorporating "privacy by design" or indicating if a privacy risk assessment has been completed, and does not make any reference to the data retention term. There are regional differences in the APPs.

Concerning data security, the data controller is responsible for the data security and must take strict management and technical measures to prevent data leakage, only the organizations authorized by the National Health Commission[44] according to the law can collect the data for the COVID-19 related purpose without consent from data subjects. Other unauthorized organizations must secure consent from data subjects before data collection.

[43]Chinacdc.cn. (2016). *Chinese Center for Disease Control and Prevention*. [online] Available at: http://www.chinacdc.cn/en/ [Accessed 8 Feb. 2021].

[44]Nhc.gov.cn. (2018). *National Health Commission of the PRC*. [online] Available at: http://en.nhc.gov.cn/ [Accessed 8 Feb. 2021].

- **Closing remarks**

We explored some of the key issues and concerns related to the use of contract tracing applications. The use of such applications has been planned in conjunction with a set of measures that all use non-pharmaceutical interventions. Different countries all around the world issued specific norms and regulations concerning the guidelines to develop contact tracing APPs. The European Institutions published clear regulations and recommendations concerning the design and development of the APPs. Key aspects to be carefully considered were privacy issues starting from the personal information requested to download and activate the APP, the anonymisation, sometimes pseudo-anonymisation, of data to be exchanged to validate potential risky contacts, the request of consent to store contact info and related upload on local, semi-centralized or centralised servers. How long personal data will be stored on servers, who is in charge as data controller, and who is entitled to access or share such data.

An additional relevant aspect concerns the voluntary or compulsory use of the APP not only related to the activations but much more related to the need to have a positive/green feedback from the APP in order to perform an activity or enter a specific place.

- **Bibliography**

1) Clusit, Rapporto Clusit 2020 sulla sicurezza ICT in Italia, Clusit - Astrea
2) Council of Europe, Joint Statement on Digital Contact Tracing, Strasbourg April 2020
3) European Data Protection Board (edpb), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.
4) A, Hendy SC, Plank MJ, Steyn N. Suppression and mitigation strategies for control of COVID-19 in New Zealand. medRxiv 2020; published online March 30. DOI:10.1101/2020.03.26.20044677 (preprint).
5) Syed Rafiul Hussain, et. Al., Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information, Internet Society, ISBN 1-891562-55-X
6) Lai S, Ruktanonchai NW, Zhou L, et al. Effect of non-pharmaceutical interventions to contain COVID-19 in China. Nature 2020; published online May 4. https://doi.org/10.1038/s41586-020-2293-x.
7) Zhongjie Li, Qiulan Chen, Luzhao Feng et al. Active case finding with case management: the key to tackling the COVID-19 pandemic. The Lancet https://doi.org/10.1016/S0140-6736(20)31278-2 (published on line June 4, 2020)
8) PresidenzaConsigliodeiMinistri, DPCM 03/12/2029
9) Ronchi, Alfredo M., (2019).*e-Citizens: Toward a New Model of (Inter)active Citizenry* , ISBN 978-3- 030-00746-1, Springer (D)
10) Ronchi, Alfredo M., (2019). *e-Services: Toward a New Model of (Inter)active Community*, ISBN 978- 3-030-01842-9, Springer (D)
11) Ronchi, Alfredo M., (2010). The Patient's Perspective - empowerment or bewilderment eHealth: Background, Today's Implementation and Future Trends. Alan R. Shark, SylvianeToporkoff in eHealth - A global perspective. (pp. 181- 198), ISBN 978-1451540291, CreateSpace Independent Publishing Platform
12) Lei Zhang, Bingpeng Zhou, et al. (2020) Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic, DOI: 10.1109/IOTM.0001.2000078, IEEE