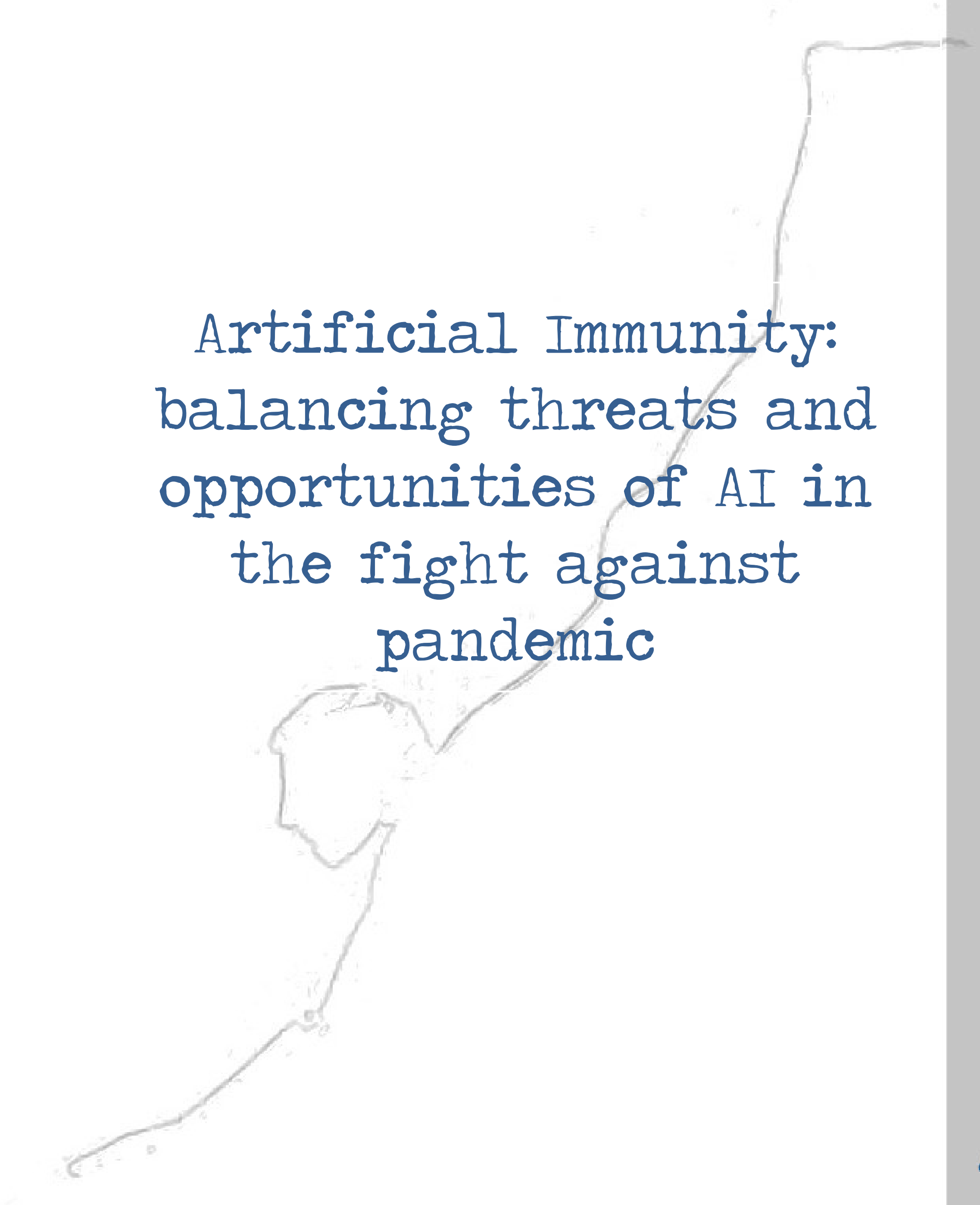
PAPER N. 43

a.a. 2019/2020



# Artificial Immunity: balancing threats and opportunities of AI in the fight against pandemic

Niccolò Iurilli, Valentina Eisendle

Trento BioLaw Selected Student Papers

Jean Monnet
EUROPEAN CENTRE
UNIVERSITY OF TRENTO

With the support of the
Erasmus+ Programme
of the European Union

UNIVERSITÀ
DI TRENTO
Facoltà di
Giurisprudenza

I paper sono stati selezionati a conclusione del corso *BioLaw: Teaching European Law and Life Sciences (BioTell)* a.a. 2019-2020, organizzato all'interno del Modulo Jean Monnet "BioLaw: Teaching European Law and Life Sciences (BioTell)", coordinato presso l'Università di Trento dai docenti Carlo Casonato e Simone Penasa.

# Artificial Immunity: balancing threats and opportunities of AI in the fight against pandemic

*Niccolò Iurilli, Valentina Eisendle **

ABSTRACT: *T*he paper aims at clarifying the relationship between artificial intelligence and the limitations of fundamental rights during the emergency caused by the Covid-19 infection outbreak. It will consider the way in which new technologies may help facing several aspects of the crisis, especially referring to the surveillance systems adopted by some Asian and European states, with emphasis on the latter. These control methods will be linked to the rights and freedoms they can restrict. The way in which this happens will be analysed by balancing the different positions at stake. The role of EU law and national law will be enlightened, with a particular focus on the application of GDPR to contact tracing apps.

KEYWORDS: Artificial intelligence; contact tracing; applications; privacy; Covid-19

## 1. The Covid-19 pandemic

Covid-19 is an infection caused by the novel coronavirus Sars-Cov-19, a highly communicable virus capable of triggering a global pandemic. The fatality rate is approximately 2% and, even more concerning, the proportion of cases requiring intensive care is about 5%, which necessitate a complex management involving the use of personal protective equipment and engage in complex decontamination procedures[1]. Hospital capacity is overwhelmed, and governments are trying to face this crisis by ordering social distancing and nationwide lockdowns. Since this condition of social stand-still cannot last forever, scientists and researchers from all over the world are proposing possible solutions in combating this virus and in making it possible to gain back a little bit of 'normality' in our everyday life. Nevertheless, it is now more important than ever to take well-balanced and rational decisions, even if circumstances are asking us to act quickly. «Whenever there is a crisis rationality exits the room and you have a policy that is driven by a panic in the pursuit of benefits that in the time are just theoretical»[2], says Edward Snowden, an American whistle-blower, trying to make us aware of this delicate situation we are facing. Emergency measures tend to be very sticky, take, for

** Students at the University of Trento, Faculty of Law.*

[1] L. FERRETTI et al., *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing,* in *Science*, 2020, 1.

[2] E. SNOWDEN, *Live debate Copenhagen International Documentary Film Festival*, 23/03/2020.

example, all the changes and restrictions involved after the terrorist attacks of 9/11 in America, which are still in force and largely operating until today. «It becomes a culture of safety at all costs, which is fundamentally in conflict with the concept of our free and open society»[3].

Important trade-offs with our government happened and still lie ahead. Perhaps this emergency is redefining the relationship between individuals and governments. Questions inevitably arise about the fair balance between fundamental rights and our relationship to personal data: how its treatment could help or hurt us.

## 2. Contact tracing or tracking as solution for a possible relaxation of restrictions

Several measures were taken by governments to slow the spread of the virus, and now arises the question which is the best and safest way to go back to 'normality'. Since Covid-19 is not likely to stop being a medical emergency anytime soon, authorities are evaluating different approaches to have a better control of the medical risk going back to conventional social interaction. One of those approaches is the use of a contact-tracing mobile app. Contact tracing is a method of identifying and alerting people who have come into contact with an infectious person (contact).

The WHO defines a *contact* as a person who experienced any one of the following exposures during the 2 days before and the 14 days after the onset of symptoms of a probable or confirmed case:

1. face-to-face contact with a probable or confirmed case within 1 meter and for more than 15 minutes;
2. direct physical contact with a probable or confirmed case;
3. direct care for a patient with probable or confirmed Covid-19 disease without using proper personal protective equipment;
4. other situations as indicated by local risk assessments[4].

In the initial stages of the outbreak this was carried out manually, but it soon became clear the viral spread is too fast to be contained by manual contact tracing. Therefore a contact tracing app which builds a memory of proximity contacts and immediately notifies contacts of positive cases can provide more efficient and accurate tracing. However we need to differentiate between contact tracing and contact tracking. Tracing apps aim to gain insight in retrospect (where was the person in the past?), whereas tracking apps aim to gain insights in real time (where is the person right now?), i.e. determine a person's current location using geodata (GPS or radio cell location)[5]. This second type of monitoring system may entail the risk in creating detailed

[3] *ibid.*

[4] WHO, *Global surveillance for COVID-19 caused by human infection with COVID-19 virus: interim guidance,* in *Surveillance Guidance*, 2020

[5] *Corona App: What's the difference between tracking and tracing?*, in *Cliqz*, 29/04/2020.

movement profiles of its users. Nevertheless, even contact tracing apps pose the risk of an insufficient protection of discreet personal data and an abuse of power can easily happen[6].

### 3. Global developments

At least 30 governments around the world have instituted temporary or indefinite efforts to detect infectious individuals or maintain quarantine in the attempt to contain and control the spread of Covid-19. Many of these efforts compromise civil liberties and involve different dangers threatening personal privacy[7]. The Tech and Science Medium *OneZero* compiled press reports from more than 25 countries where potential privacy issues are occurring, updating the list on a weekly basis[8]. The most common form of surveillance implemented to battle the pandemic is the use of smartphone location data, which can track the movement of single individuals, register their person-to-person contacts, and eventually enforce individual quarantines. However, many of this surveillance technologies, such as the *Alipay Health Code App* applied in China[9] and the data tracking system implemented in South Korea[10], are not limited to track necessary data to stop the spreading of the virus, but are used by governments to track and store location data of millions of people, and register even their credit card movements[11].

### 3.1 South Korea: a role model in managing the coronavirus-crisis?

South Korea is for sure an outstanding case in this corona crisis. From late January, when first people were tested positive in South Korea, to late February the numbers of cases exploded from a few dozens to several thousands. At the peak medical workers identified 909 cases in a single day, on February 29[12]. But in the same way the numbers had risen, they dropped remarkably fast. Within a weak the cases halved and on March 15 the confirmed cases fall off to just 76[13]. The South Korean Government launched a massive testing-system, setting up numerous drive-through testing centres. The country tested a total of nearly 300.000 people, so far, more people per capita than any country in the world[14].

In addition an extensive contact tracing-system was set up to spot infected people and then retrace the persons recent movements to find, test and, if necessary, isolate anyone the person may have had contact with. To monitor people under quarantine health authorities in South Korea developed a global positioning system (GPS) which triggers an alarm if those infectious people leave the designated isolation zone. The

[6] *Lawmakers warn coronavirus contact-tracing is ripe for abusive surveillance*, in *Los Angeles Times*, 26/04/2020

[7] www.onezero.medium.com (last accessed 10/05/2020).

[8] *ibid*.

[9] *In Coronavirus Fight, China Gives Citizens a Color code, With Red Flag*, in *New York Times*, 01/03/2020.

[10] *Tech Tent: Can we learn about coronavirus-tracing from South Korea?,* in *BBC*, 15/05/2020.

[11] M. Zastrow, *South Korea is reporting intimate details of COVID-19 cases: has it helped?*, in *Nature Research*, 2020.

[12] Korea Centres of Disease Control, *The Updates of Covid-19 in Republic of Korea*, 15/03/2020.

[13] *ibid*.

[14] M. Zastrow, *op. cit.*

investigators from the Korea Centres of Disease Control and Prevention check mobile phone GPS data, closed-circuit television camera footage and credit card records to release details about the patients' travel history via text messages on mobile phone and state-managed websites, so the public can avoid places where the virus was once active[15].

There are also some private sector initiatives. The *Coronamap*, for instance, allows users to see on a map the hospital and date the cases were confirmed and the places that the patients visited before testing positive[16]. As Business Insider reports on March 2, this was the second-most-downloaded app in Korea[17].

The *Corona 100m* app collects data from public government info, including Korea Centres for Disease Control, and alerts users of any diagnosed Covid-19 patient within 100-meter radius along with the patient's diagnosis date, nationality, age, gender, and prior location[18].

Although the control over the spreading of the infection was very successful in South Korea, it is now becoming clear the publication of such information brings the risk of exposing people to the social stigma that might come if their community knows they are infected, which could even dissuade some infected people from coming forward to get tested[19].

### 3.2 China: a data driven pandemic response

China is repurposing its vast existing system of digital surveillance for Covid-19 tracking, but this technology is not limited to contact tracing. For instance, Chinese high-tech firms, *SenseTime* and *Megvii*, both known for their facial recognition technology, have developed and deployed AI-based contactless temperature detection software. *SenseTime* has also developed the *Smart AI Epidemic Prevention Solution* to provide a system for screening and detection of suspected carriers of the Coronavirus in public spaces. By using AI algorithms with infrared thermal technology it is able to detect fever within an accuracy of 0.3°C and identifies individuals not wearing a face mask with over 99% success rate[20].

Chinas government has long recognized that the key to data-driven pandemic response are giant firms such as *Alibaba* and *Tencent*, that harvest colossal amounts of users' data in real-time. The app *WeChat*, developed by tech-giant *Tencent*, has not just over a billion active users, who spend on this app double the average time spent on Instagram, but it integrates within its own platform social media, instant messaging, payment, food delivery, ride hailing, health care and thousands of other apps. Hence the Chinese government introduced

[15] *ibid.*
[16] coronamap.site (last accessed 02/05/2020).
[17] *Take a look at these Korean apps helping people avoid areas infected by the coronavirus*, in *Business Insider*, 02/03/2020.
[18] *ibid.*
[19] *'More scary than coronavirus': South Korea's health alerts expose private lives*, in *The Guardian*, 06/03/2020.
[20] www.sensetime.com (last accessed 05/05/2020).

the *Alipay Health Code* rolled out by Alibaba's sister company *Ant Financial* and has since been adopted nationwide[21]. The app was not obligatory, but its use was compulsory for people to move between certain areas, such as into subways, malls and other public spaces[22]. This app assigns users into three categories based on their Covid-19 risk factors calculated using self-reported and collected data. Three colour codes indicate their health status: green for unrestricted travel, yellow for seven-day quarantine, and red for a two-week quarantine. Neither the company nor Chinese officials have explained in detail how the system classifies people. Some users report they have no idea why the app is quarantining them[23].

## 4. European developments

Also European countries are searching for possible contact tracing solutions to face the current emergency. The European Data Protection Supervisor has also called for a pan-European model *Covid-19 mobile application*, coordinated at EU level and, ideally, with the WHO[24]. Nevertheless copying the Asian approach would violate Europe's law under several aspects. Therefore Europe urges to put privacy in front and centre and assure a high level data protection. Bluetooth Low Energy (BLE) chatter between devices is seen as a better way than GPS location data to measure person-to-person contact. The majority of Member States agree that apps should be voluntary, however, researchers from Oxford University's Big Data Institute say, the apps would need to be downloaded by at least 60% of the population to be effective and to achieve a so-called "digital herd immunity"[25].

The first contact tracing app to go live in Europe was Austria's Red Cross *Stopp Corona* app on March 25. By explicit user recognition the app exchanges data with other smartphones in nearby surroundings. This data is stored as contacts. In case of infection the user must report it to the responsible of the app, the Red Cross, which then informs all the contacts of the last three days of the infected person via app. This notification triggers the storage of the mobile phone number of infected people[26]. Within a month this app was downloaded 400.000 times[27].

Very soon researchers came together in a European wide consortium, the Pan European Privacy Protecting Proximity Tracing to provide a complete framework and reference implementation with technical standards, trustworthy mechanisms, and services creating interoperability to local implementations[28]. «The idea is to make the technology available to as many countries, managers of infectious disease responses, and developers as quickly and as easily as possible. The technical mechanisms and standards provided by PEPP-

[21] Y. HUANG et al., *How Digital Contact Tracing Slowed Covid-19 in East Asia*, in *Harvard Business Review*, 2020.

[22] *In Coronavirus Fight, China Gives Citizens a Color code, With Red Flag*, in *New York Times*, 01/03/2020.

[23] Y. HUANG et al., *op. cit.*

[24] W. WIEWIOROOWSKI, *EU Digital Solidarity: a call for a pan-European approach against the pandemic*, 2020, 3.

[25] *Rift opens over European coronavirus contact tracing apps*, in *Reuters*, 20/04/2020.

[26] www.roteskreuz.at (last accessed 06/05/2020).

[27] *France, Germany in standoff with Silicon Valley on contact tracing*, in *Reuters*, 24/04/2020.

[28] PEPP-PT Manifesto, 2020, 1.

PT fully protect privacy and leverage the possibilities and features of digital technology to maximize speed and real-time capability of any national pandemic response»[29]. PEPP-PT does not want to offer a concrete app, but rather a specification for a suitable data processing system. We find basically two different models within the framework: the centralised system architecture, which allows a central entity to process the users' data, and the decentralised system architecture, where contact history is processed by individual clients in the network (*infra* 4.1). Furthermore, it offers a certification service for local initiatives so national authorities can release apps with a high level of trust, built both their credibility and their certainty that European standards in data protection, privacy and security are enforced at all time and that cross-border interoperability is supported [30].

However in mid-April some high-level members (*Helmholtz Centre for Information Security CISPA, Istituto per l'Interscambio Scientifico ISI, Catholic University of Leuven*) of the PEPP-PT Consortium dissociated from the project claiming a lack of transparency and citing concerns over centralisation and privacy[31]. This withdrawal was probably caused by the cancellation of one possible system architecture, the DP-3T protocol (Decentralised Privacy-Preserving Proximity Tracing), from the official Website of PEPP-PT without any further discussion with the members of the Consortium. This gives rise to concerns whether PEPP-PT still wants to provide different implementations within the framework or the only centralised model. The main supporter of the project Hans-Christian Boos (AI company Arago) assures that PEPP-PT is going to still support both of the two main approaches[32]. Nevertheless by know the PEPP-PT seems to be the main European representative of the centralised system architecture, whereas the DP-3T[33] stands now for the main decentralised approach launched by researchers from EPFL and ETH Zurich, and is now being developed in collaboration with a number of other leading European institutions.

### 4.1. Understanding possible system architectures

As mentioned before, we can roughly differentiate between at least two system architectures of a possible contact-tracing app, the centralised and the decentralised processing. Both are based on voluntariness, they do not use any GPS data, but determine the contact by using BLE.

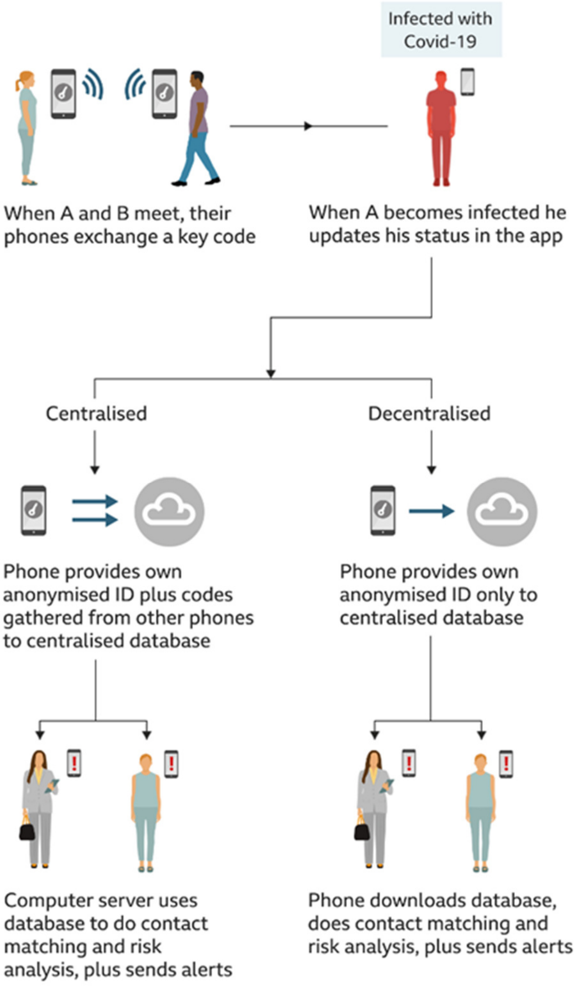
a) The centralised architecture.

In the centralised architecture, contact history is processed by a central health authority. That means, when a patient tests positive for Covid-19 a centralised system requires him to upload his contact history log to a

[29] *ibid.*
[30] *ibid.*
[31] *Joint Statement on Contact Tracing*, 19/04/2020.
[32] *Auch alle Zufallskontakte in der U-Bahn können gewarnt werden*, in *Der Tagesspiegel*, 17/04/2020.
[33] www.github.com/DP-3T (last accessed 03/05/2020).

central server, where the health authority by using artificial intelligence would match the identifiers with users records and contact people who came in close contact with the patient. Therefore the anonymity of the user and confidentiality of contact events is only provided regarding outside entities, i.e. other users or third parties. The involved authorities and operators can identify and connect all the users to recorded contact history[34].

An advantage of this system would be the possibility for epidemiologists to use the stored data of the central server as a basis for projecting the number of coronavirus-infected people and its development and thus understand the spreading of the infection. The central entity, however, would know who people met, when they met and for how long they were together. This creates a significant risk of pervasive tracking of individuals' associations and a great degree of trust in handling this data by the government would be necessary.


Infected with Covid-19
When A and B meet, their phones exchange a key code
When A becomes infected he updates his status in the app
Centralised
Decentralised
Phone provides own anonymised ID plus codes gathered from other phones to centralised database
Phone provides own anonymised ID only to centralised database
Computer server uses database to do contact matching and risk analysis, plus sends alerts
Phone downloads database, does contact matching and risk analysis, plus sends alerts

Centralised and decentralised contact tracing
Source: BBC

b) The decentralised architecture.

In the decentralised architecture, contact history is processed by individual clients in the network. Users upload to a central server a token that has no intrinsic information about the user's identity and contact history but can then be used by client devices to derive and match contact history identifiers. Users remain anonymous towards third parties and other users, in addition contact events would remain secret. Operators and authorities can de-anonymise just positively tested users but not their contact history[35].

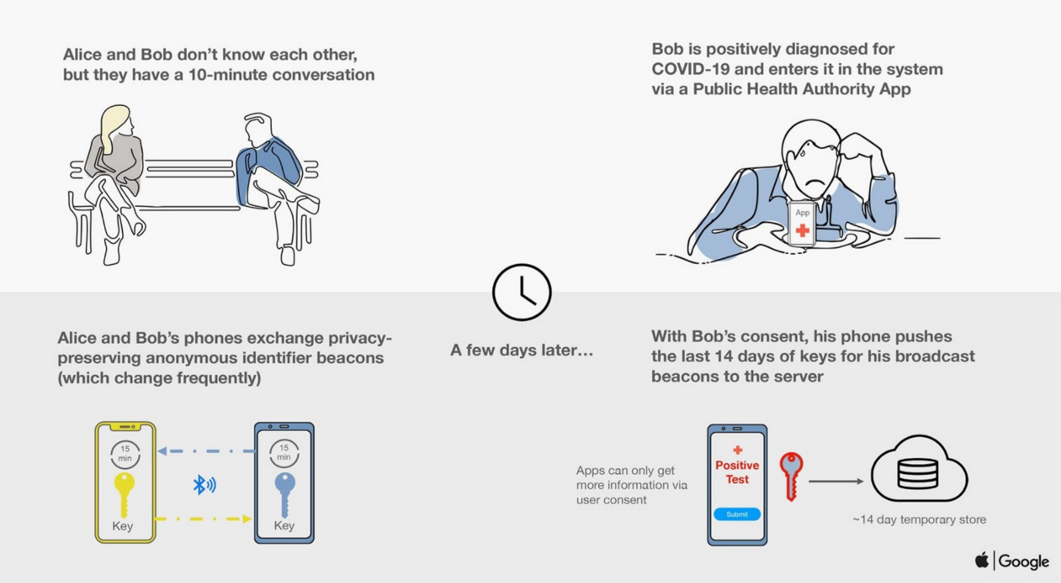
A downside of this system architecture is that data would not be usable for epidemiological research. The system could provide a solution by offering a data donation function, which will allow users to share their contact histories for epidemiological research. If done so, positively tested users' contact events would become visible to operators and authorities and an analysis of the spreading of the infection would be possible.

[34] K. Bock et al., *Datenschutz-Folgenabschätzung für die Corona-App,* in *Forum Informatiker Innen für Frieden und gesellschaftliche Verantwortung, 2020,* 6.

[35] *ibid*.

### 4.2. Apple and Google's joint effort to release APIs

Apple and Google announced on April 10 a joint effort to release an APIs (app programming interface) that enable interoperability between Android and iOS devices using apps from public health authorities. In addition both companies work to enable a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platform[36]. The technology stores most sensitive data in a decentralised way and does not use any GPS location data. Some countries, however, would prefer the firms to be less prescriptive and allow a centralised storage. Dave Burke, vice president for engineering at Google called the DP-3T protocol developed by a Swiss-led team of researchers «the best privacy preserving solution»[37]. The two tech-giants argue that it is preferable to support a single standard to ensure that national contact tracing apps can talk to each other across borders. On May 20 Apple and Google launched their Exposure Notification API to support public health agencies, thus allowing the interested countries to incorporate the API in their own apps[38].


Alice and Bob don't know each other, but they have a 10-minute conversation
Bob is positively diagnosed for COVID-19 and enters it in the system via a Public Health Authority App
App
Alice and Bob's phones exchange privacy-preserving anonymous identifier beacons (which change frequently)
15 min
Key
15 min
Key
A few days later...
With Bob's consent, his phone pushes the last 14 days of keys for his broadcast beacons to the server
Apps can only get more information via user consent
Positive Test
Submit
~14 day temporary store
Google

This graphic shows how the Apple/Google solution is intended to work.
Source: Google, 2020

### 4.3. European nations towards the gradual implementation of contact tracing apps

On April 17 European parliament demanded not obligatory contact-tracing apps with a decentralised storage of data and full transparency given on (non-EU) commercial interests of developers and functioning of the

[36] www.apple.com/newsroom (last accessed 20/05/2020).
[37] *France, Germany in standoff with Silicon Valley on contact tracing*, in *Reuters*, 24/04/2020.
[38] www.blog.google/inside-google/company-announcements, 20/05/2020.

apps[39]. Equally a coalition of nations, led by Switzerland, also including Italy, insists on the decentralised system architecture, to avoid governments spy on their citizens. Germany, who initially insisted in the centralised approach on data storage, changed course backing a decentralised approach too[40]. Crucially for the coalition is the support by Apple and Google, whose iOS and Android operating system run 99% of the world's smartphones. Britain and France, however, argue people should trust their health authorities to hold such information on a central computer server.

Latvia, as one of the first countries in the world, launched a smartphone app based on the APIs from Google and Apple, the *Apturi Covid* (Stop Covid) app[41]. From 25 May the download of a contact tracing app for both Apple and Android smartphones is available in Switzerland too, but including a pilot phase lasting presumable until the end of June[42]. Also the developers of the Austrian Red Cross *Stopp Corona* app intend to provide an update to integrate Apple and Google's APIs, but so far available for only iPhone-users[43].

The Italian contact tracing app developers Bending Spoons made the backend app configuration available on GitHub on May 29, providing all information about its functionalities[44]. Also this approach is based on the Apple-Google APIs and as already announced earlier this month, the Italian app will follow the decentralised system architecture, specifying that all data, whether stored on the device or on the server, are deleted when no longer needed, and in any case no later than December 31, 2020[45]. Like the Swiss approach, Italy projected a pilot phase making the download initially available only in some specific Regions (Abruzzo, Liguria, Marche, Puglia) [46] and from June 15 the app is in use in the whole country[47].

However, contact tracing apps struggle to make an impact. Reports show that not enough people download and use these applications. In Singapore, for instance, the app was downloaded by merely 25 per cent of the population of 5.7 million[48]. In Iceland, where 40 per cent of the whole population downloaded the *Rakning C-19* app, an official in charge of contact tracing clarifies that the app was «useful», but no «game-changer»[49].

The *Ada Lovelace Institute*, an independent research institute and deliberative body, states in an evidence review regarding the UK Government's contact tracing proposals, that «there is currently insufficient evidence to support the use of digital contact tracing as an effective technology to support the pandemic response. The technical limitations, barriers to effective deployment and social impacts demand more consideration before digital contact tracing is deployed»[50].

[39] European Parliament, *EU coordinated action to combat the COVID-19 pandemic and its consequences*, 2020, § 52.

[40] *Germany flips to Apple-Google approach on smartphone contact tracing*, in *Reuters*, 26/04/2020-

[41] *Latvia to launch Google-Apple friendly coronavirus contact tracing app*, in *Reuters*, 25/05/2020.

[42] ethz.ch/services/en/news-and-events (last accessed 29/05/2020).

[43] *Apple and Google release marks 'watershed moment' for contact-tracing apps*, in *BBC*, 20/05/2020.

[44] github.com/immuni-app (last accessed 29/05/2020).

[45] github.com/immuni-app/immuni-documentation (last accessed 29/05/2020).

[46] *Tutto quello che c'è da sapere su Immuni, l'app di contact tracing italiana*, in *La Stampa*, 02/06/2020.

[47] *Immuni, da oggi l'app per il rischio contagio attiva in tutta Italia: oltre 2 milioni di download,* in *La Repubblica,* 15/06/2020.

[48] *Coronavirus contact-tracing apps struggle to make an impact*, in *Financial Times*, 18/05/2020.

[49] *ibid*.

[50] M. Ryder et al., *COVID-19 & Tech response: Legal opinion*, in *COVID-19 Rapid Evidence Review Ada Lovelace Institute*, 11, 2020.

## 5. Balancing health, rights and freedoms

Contact tracing is an effective solution to contain a pandemic in a democratic context. The discussion focuses on the relation between apps and fundamental rights, as balancing rights is crucial in fighting the pandemic. Our aim is to recap and discuss the features of the European approach to make fundamental rights coexist. Even if we analyse the current situation, the impact of the pandemic will be part of our legal future. Therefore, we discuss the matter through the lens of basic rights to privacy, freedom, public and individual health. The approach is not a Law 1.0 one, but rather a Law 2.0 or 3.0 one, since there is a strict connection between talking about technology and thinking about law[51]. The regulatory environment should be re-imagined so as to face the challenges of 'surveillance capitalism', where the process of personal data commodification combines with a mass monitoring system[52].

### 5.1. EU law and its impact on the Italian situation: GDPR during the emergency

The first concern about artificial intelligence *sub specie* of contact tracing technologies is that they could not offer the necessary guarantees of respecting the individual's rights to privacy and freedom of movement. As explained *supra*, countries belonging to different legal traditions chose to use a variety of means to enable contact tracing in order to face the problem of identifying infected people and containing the spread of the coronavirus. This solution worked for some states, but it may not work alike with different societal rules. For instance, in the US, a lot of people tend to be reluctant and wary of sharing personal data with tech companies or the government[53]. In Europe, a different authority-freedom relationship shapes the legal framework where technologies are to operate. There, rights do not operate as trumps, but they express *principles to balance* as to obtain the best composition of the interests at stake, trying to safeguard them all by sacrificing some of their aspects. This mechanism should be applied especially during emergencies, a crucial test for the validity of constitutionalism and the rule of law. Moreover, fundamental rights work both in a vertical and horizontal direction, so the individual's position has to be protected not only from the government, but also from the interference of tech corporations. The best regulatory composition of interests in a multi-level context requires a dialogic confrontation between national and supra-national laws[54].

[51] The «field of legal interest is constituted by three conversations (and mind-sets): the traditional coherentism of Law 1.0; the regulatory-instrumentalism of Law 2.0; and the technocratic approach of Law 3.0», they interact in governing complexity, R. Brownsword, *Law, Technology, and Society: In a State of Delicate Tension*, in *Notizie di Politeia*, 137, 2020, 26.

[52] S. Zuboff, *The Age of Surveillance Capitalism*, New York City, 2018.

[53] H. Cho et al., *Contact tracing mobile apps for COVID-19: privacy considerations and related trade-off*, in *arXiv*, 2020, 2.

[54] M. Farina, *La* data protection *ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, in *BioLaw Journal*, 1S, 2020, 685.

The safeguard of the fundamental right to privacy is enshrined in Article 16(1) of the Treaty on the Functioning of the European Union, which states that «everyone has the right to the protection of personal data concerning them». Besides, Article 8 of the EU Charter of Fundamental Rights prescribes that «everyone has the right to the protection of personal data concerning him or her», that «such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law», that «everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified», and that «compliance with these rules shall be subject to control by an independent authority». On these bases, the GDPR (Regulation 2016/679) recognises the protection of natural persons in relation to the processing of personal data as a fundamental right contributing to «the well-being of natural persons» (recital 2). Yet, recital 4 explains that even if the processing should be designed to serve mankind, the right to the protection of personal data is not absolute, but it must be considered in relation to its function in society and be balanced against other fundamental rights, according to the principle of proportionality. The same rationale characterises the Italian approach: all rights are situated in a relationship of reciprocal integration, a single one cannot prevail. The unlimited expansion of a right would make it unacceptably «tyrannical»[55].

In democracies, the reason for restricting rights to privacy and freedom of movement – which is actually prodromal to the exercise of other liberties, e.g. the right to vote[56], association, protest, organisation in trade unions or parties... – during a sanitary emergency is the need for national healthcare services not to be overwhelmed by the overflow of patients, which would otherwise lead to their collapse[57]. This is coherent with lawful limitations of basic right grounded on «public safety», «emergency» or «the protection of health» (Articles 8-11, 15 ECHR). Recital 46 of GDPR contemplates the hypothesis of a situation like the Sars-Cov-2 spreading. In fact, the processing of personal data should be regarded as lawful whenever it is *necessary* to protect an essential interest for the life of the data subject or another natural person. Processing personal data based on his/her vital interest should in principle take place only where there are not different legal bases to proceed. «Some types of processing may serve both important grounds of public interest and the vital interests of the data subject […] including for monitoring epidemics and their spread or in situations of humanitarian emergencies». This necessity is reflected into Article 6 of GDPR, which contemplates as possible bases for the lawfulness of the processing the fact that «(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person» or that «(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the

[55] See the constitutional judgment 85/2013 (ILVA) on the protection of the «fundamental» right to health. There, Article 32 of the Constitution was balanced with environmental safety, freedom of enterprise and the right to work.

[56] A further aspect of tension between democracy and health, G. Maestri, *Urne rinviate per virus: la soluzione di (inattesi) conflitti tra diritto al voto e diritto alla salute*, in *BioLaw Journal*, 1S, 2020, 293.

[57] M. Fasan, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del coronavirus,* in *BioLaw Journal*, 1S, 2020, 677.

controller». Article 9(1) imposes a general prohibition to process data related to biometric information for the purpose of uniquely identifying a natural person or data concerning health, without further specifications. Yet, in §2, there are some exceptions. Dealing with that kind of data is considered lawful if «(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be *proportionate* to the aim pursued, *respect the essence* of the right to data protection and provide for suitable and specific measures to *safeguard the fundamental rights* and the interests of the data subject». It is also lawful for «(h) […] the management of health or social care systems and services», and overall if «(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health», provided that the law introduces suitable and specific measures to safeguard the data subject's rights. This is why, according to recital 54, the processing of special categories of personal data may be deemed inevitable for reasons of public interest in the areas of public health *even without* the involved person's consent.

In Italy, Article 14 of decree 14/2020 sets out dispositions on data processing during pandemic. It allows various actors concerned with the fight against coronavirus to process data *ex* Articles 9 and 10 of GDPR (special categories, also related to criminal offences). If strictly necessary to face the emergency, these data can be communicated to other subjects, and related data may be diffused as well (§2). Finally, the norm calls for measures to reconduct proceedings to ordinary rules and competences once the extraordinary situation has ended. The proceeding must hence be informed to the pivotal principle of minimisation. It follows that, applying the general canon of proportionality, at the conditions hitherto explained, only essential data can be legally used, exclusively for the purpose they are collected for. At the end of the pandemic, they could lawfully be preserved and employed after their anonymisation, to make the person they are related to impossible to find[58]. Far from establishing exceptions to GDPR, a higher source of law, the Italian legislation integrally applies it, balancing new needs and defining provisional roles and functions for the precise and circumscribed purpose of health safeguard[59]. Article 32 of the Constitution legitimises it, to the extent that it considers health to be both «a fundamental right of the individual and a collective interest».

### 5.2. The role of regulation: the Commission

In this context, soft law instruments were implemented. On April 8, the European Commission adopted a Recommendation (Article 292 TFEU) on a common Union toolbox for the use of technology and data to combat and exit from the Covid-19 crisis, in particular concerning mobile applications and the use of

[58] F.P. MICOZZI, *Le tecnologie, la protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal*, 1S, 2020, 623.
[59] *ibid.*

anonymised mobility data[60]. It recognised that digital technologies and data have a valuable role to play in combating the pandemic, since many people in Europe are connected to the internet via mobile devices. They offer an important tool for informing the public and helping authorities to contain the spread of the virus or allowing healthcare organisations to exchange health information. However, a fragmented and uncoordinated approach hampers the effectiveness of anti-Covid measures, whereas causing serious harm to the single market and to fundamental rights and freedoms. Economic and financial needs related to the functioning of the common market enter the balancing, expressing the «genomic imprinting»[61] of the EU legal system, which is indeed highly committed to free market regulation. The Recommendation has two purposes. First, to lay down a pan-European approach for the use of applications, coordinated at the EU level, «for empowering citizens to take effective and more targeted social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the Covid-19 disease». This involves a methodology that allows to monitor and share assessments of apps' effectiveness, interoperability and cross-border implications, as well as their respect for security and data protection. The second objective is to create a common scheme for using anonymised and aggregated data on mobility «(i) to model and predict the evolution of the disease, (ii) to monitor the effectiveness of decision-making by Member States' authorities on measures such as social distancing and confinement, and (iii) to inform a coordinated strategy for exiting from the Covid-19 crisis».

This common strategy, referred to as the Toolbox, has to be developed by Member States through their representatives in the eHealth Network[62], who have to meet «immediately and frequently», with representatives of the Commission and the European Centre for Disease Control too. The Toolbox indicates the best way to use data from various sources with a high level of trust and security, within the framework of EU and national law. The European Data Protection Board ensures it integrates data protection and the principles of privacy by design – a concept including all the strategies to achieve from the beginning a substantial level of protection, not merely a formal one. To do so, both at the time of determining the means for processing and of the processing itself, the controller has to implement appropriate technical and organisational measures, like pseudonymisation, designed to implement data-protection principles, such as minimisation, in an effective manner and to integrate the necessary safeguards into the processing (Article 25 GDPR).

Then, the Recommendation states some operational steps and adds some principles to observe during the app development. In fact, fundamental rights must be respected, especially not to allow discrimination and stigmatisation. There is a preference for the least intrusive yet effective measures, including the use of

[60] C(2020) 2296 final

[61] R. Bin, *Critica della teoria dei diritti*, Milano, 2018, 70.

[62] The network established by Article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare.

proximity data and the avoidance of processing data on location or movements of individuals, and the use of anonymised and aggregated data if possible. There are also technical requirements concerning appropriate technologies, such as BLE[63], to establish device proximity, encryption, data security, data storage on the mobile device, and possible access by health authorities. In case of a confirmed infection, the uploading of proximity data must be permitted. Appropriate methods of warning people who have been in close contact with a positive person shall make sure that the latter remains anonymous. Eventually, a sunset rule needs the measures to cease and personal data obtained through these measures to be deleted as soon as the pandemic is declared to be under control at the latest – in principle, before 90 days from the collection. Accidentally processed data, capable of identifying individuals and notifying it to providers and competent authorities, must be immediately and irreversibly deleted.

Following the Recommendation, the Commission published a Communication[64] on April 17, serving as a guidance on apps supporting the fight against Covid-19 in relation to data protection, developing many aspects only stated in principle by the former. First, it recognises that the apps' functionalities can have a different impact on a wide range of rights protected by the Charter, such as human dignity, respect for private and family life, protection of personal data, non-discrimination, freedom of movement, freedom to conduct a business, freedom of assembly and of association. In particular, the interference with privacy and the connected right to protection of personal data is significant, given that some functionalities follow a data-intensive model. The Communication elucidates how Member States can limit the intrusiveness of contact tracing devices, in compliance with EU legislation, above all the GDPR and the ePrivacy directive (2002/58).

The first condition is to qualify the data controller as a public institution. National health authorities or entities carrying out activities in the public interest in this field should hence be accountable. This contributes to higher trust among the population and acceptance of the tracing, ensuring it fulfils the purpose of protecting collective and individual health. The second condition is to let individuals in control of their data – a matter of trust as well. To ensure it, the installation of the app on one's device should be voluntary and without any negative consequences for who decides not to download or use it. Also, apps' diverse functionalities – e.g. information, symptom checker, warnings – should not be bundled, so that one can provide his/her consent specifically for each purpose. Furthermore, proximity data should be stored on the device. Their sharing with authorities can happen exclusively after the confirmation that the person is infected and on the condition that he/she chooses so. The entire data processing must be compatible with

[63] Also known as Bluetooth Smart or Bluetooth 4.0, it was developed to fit novel applications in healthcare, fitness, beacons, proximity marketing, security and home entertaining. Compared to classic Bluetooth, it can maintain a wide communication range and provide a heavily reduced power consumption.

[64] 2020/C 124 I/01.

the GDPR, providing for the exercise of the rights to access, rectification and deletion. In the end, those apps should be deactivated – i.e. the data processing must terminate, this is why deactivation should not depend on the sole de-installation by the user – at the latest when the pandemic is over. Further technicalities to protect users (or patients?[65]) are discussed *infra*. Anyway, the Union guidance «does not cover apps aimed at enforcing quarantine requirements (including those which are mandatory)» – a serious *vulnus* without explanation.

### 5.3. Regulatory agencies

The president of the Italian *Autorità garante per la protezione dei dati personali* stated: «the potential juxtaposition between privacy and public health is the effect of the general tension between individual freedoms and collective interests, which can be balanced, if not synergistically combined, only by democracy. Today's challenge is to guarantee that individual rights are limited (only) in the necessary way to safeguard as many human lives as possible. Data protection legislation already contemplates the necessary limitations to guarantee solidarity demands like those expressed by public health exigencies, according to the criteria of proportionality, precaution, and temporariness»[66]. In a parliamentary hearing the *Garante* specified that the actual purpose of contact tracing devices «is to be received most favourably because it is not focused on repression – contrary to what is the case with the surveillance of quarantined individuals based on their geolocation – but on solidarity»[67]. The pursued objective lies within the scope of the same solidarity element inherent to the right to health as a societal interest, which was highlighted by the *Corte Costituzionale* in decisions on mandatory vaccination. Indeed, Article 2 and 32(1) of the Constitution are the ultimate criteria of validity. Likewise, on May 11 the French *Conseil Constitutionnel* argued that surely *traçage* systems jeopardise the right to privacy, nonetheless the legislator must preserve the constitutional value of health[68]. Indeed, from today's constitutional perspective, collective life is based not only on individual rights, but also on the related duties[69].

National regulation authorities' different standpoints converged within the European Data Protection Board. On April 21, it adopted the *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak*[70]. This soft regulation states the principles of flexibility of data protection legislation, empowerment and not stigmatisation or repression of individuals, voluntariness, transparency,

[65] «Any natural person who seeks to receive or receives healthcare in a Member State» is a patient (Directive 2011/24). It might be argued that as soon as someone is found infected thanks to contact tracing, he/she can be considered as a patient. This implies the application of the rules on patients' mobility: a set of diverse rights, compressed to the extent that freedom of movement is.

[66] *«Le app di spostamenti solo su base volontaria». Intervista ad Antonello Soro*, in *Il Mattino,* 17/04/2020.

[67] *Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus*, Commissione IX, Camera dei deputati, 08/04/2020

[68] *Décision 2020-800 DC.*

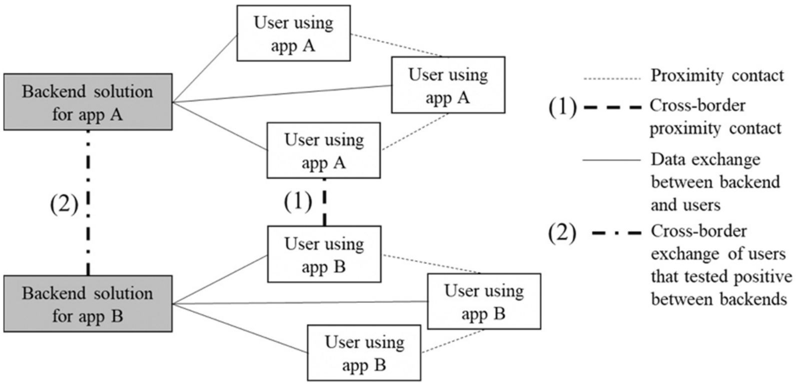
[69] G. Zagrebelsky, *Il diritto mite*, Torino, 1992, 126.

[70] www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en (last accessed 27/05/2020).

effectiveness, necessity and proportionality of the measures. The guidelines apply to geolocation and contact tracing. Location data can be collected through electronic communication service providers, during the service provision, or via specific applications. Preference is given to the processing of anonymised data rather than pseudonymised or personal ones. In fact, anonymous data can be used without restrictions, falling outside the scope of the GDPR, whereas pseudonymised and personal data fall within it. Anonymisation refers to a set of techniques to remove the ability to link data with an identified or identifiable person against any reasonable effort. The robustness of anonymisation is assessable using three criteria: (i) singling-out, i.e. isolating an individual in a larger group based on the data; (ii) linkability, that is connecting two records concerning the same individual; (iii) inference, meaning deducting unknown information about an individual with significant probability. Many reports showed location data thought to be anonymised may in fact not be. Indeed, individuals' mobility traces are inherently highly correlated and unique. Hence, they can be seriously vulnerable to re-identification attempts under certain circumstances. For this reason, contact tracing is preferable. Moreover, technologically it works via Bluetooth, while geolocation needs a GPS. This technical situation has a correspondence on the voluntariness of the practice, as Bluetooth allows the individual to avoid the possibility of position and time tracking, while the GPS does not. Clearly, the goal is not to follow the movements of individuals or to enforce prescriptions, but to permit that people know whether they have been in proximity with an infected person and perhaps when, specifying the day instead of the minute. Yet voluntariness is not equal to consent: «the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest». This is consistent with the provisos of Article 6 of GDPR (*supra* 5.1, *infra* 6) and Article 32(2) of our Constitution: no one can be obliged to undergo a health treatment *except* under the provisions of law[71].

Another important point is the right not to be subject to an automated decision: apps cannot replace, but only support, manual contact tracing performed by qualified health personnel. A corollary is that algorithms must be auditable and should be regularly reviewed by independent experts, and the application's source code should be made publicly available for the widest possible scrutiny. Also, implementation of contact tracing can lawfully follow a centralised or decentralised approach, the latter being preferable, according to the principle of data minimisation. In compliance with anonymisation requirements, under the first approach, the arbitrary temporary identifiers are stored on a backend server held by the health authority; through

[71] This entails considering contact tracing as a health treatment (see footnote 65).


User using app A
Backend solution for app A
User using app A
User using app A
(2)
(1)
User using app B
Backend solution for app B
User using app B
User using app B
Proximity contact
(1) Cross-border proximity contact
Data exchange between backend and users
(2) Cross-border exchange of users that tested positive between backends

them, users in close contact with a positively tested user, receive an alert on their device (backend server solution)[72]. On the contrary, under the decentralised processing an alert is automatically delivered from the app to the close contacts when a user notifies the app his/her positiveness, with the approval or confirmation by the health authority, via a QR or TAN code. The balancing operated by the Commission and the Board is aware that one should not choose between an efficient response to Covid-19 and the protection of fundamental rights. Both can be achieved, as the combination of artificial intelligence and data protection principles plays a crucial role in containing the pandemic. Yet, the object of regulation is profoundly and continuously changing, so an effective and shared regulation must establish a connection, a correspondence between law and the object itself. This can be done only if the law is open to other dimensions (mostly the scientific one), constantly updated, and careful in considering the specific case[73]. European data protection law currently allows for a responsible use of personal data for health management purposes, ensuring that individual rights are not significantly eroded in the process.

### 6. Some challenges: towards a (provisional) conclusion

The voluntariness of the download and use of contact tracing apps is recommended. Its assurance is not just normative, but also technical: the preference for BLE rather than GPS removes external control on personal life. Also, if there was an obligation to undergo it, people would probably not accept it. Hence, the effectiveness of the measure can be better assured by voluntariness. Exploring the potential of a nudge-based approach in this field would be useful. Libertarian paternalism is an effective means for institutions to affect behaviour without sacrificing freedom of choice[74]. The new architecture of the decision can entail a different use of the slow way of thinking that allows people to determine the appropriateness of a particular

[72] The white blocks represent users and their devices. They record proximity contacts with other users and exchange limited non-personal information with the corresponding backend solution. The grey blocks represent the backend solution which sends and receives information from the apps and with other backend solutions too. Sent and received data depend on the architecture of the system.

[73] C. CASONATO, *Le 3 A di un diritto sostenibile ed efficace*, in V. BARSOTTI (a cura di), *Biotecnologie e diritto*, 2016, 29.

[74] Nudge theory proposes reinforcement and indirect suggestion to influence behaviour and decision-making. It is a libertarian theory since it ensures freedom to opt out of arrangements if people want to. This model was adopted in the USA and UK for organ donations, thus the monitoring aspect of the fight against the coronavirus can be built upon nudging. R. THALER, C. SUNSTEIN, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, New Haven, 2008.

behaviour in the social setting they live in[75]: «effective responses to the emergency are based on governments' ability to exercise control over the national territory, including by persuading individuals to change their lifestyles and daily habits»[76].

Though, EU regulation clearly distinguishes between voluntariness and consent. They can coexist or be separated. In fact, the legal basis for the processing might be found in national legislation which, complying with GDPR, contemplates the necessity of protecting collective health, that can prevail over consent, even if it does not have to constitute an obligation. Yet, consent is the appropriate ground for these activities, provided it is freely given, specific, explicit, and informed. Tacit forms of consent are deemed invalid, and the possibility to revoke consent should be allowed. Individuals remain free to install the app and share data with health authorities, no adverse consequences for them should occur when it is uninstalled.

Member States are advised not to collect location data. The task is to obtain proximity data to assess the contact, therefore only the accuracy of the information (not of the position) is sufficient to detect crucial facts such as the epidemiological distance and the duration of the contact. This minimises the risk of having false positives, which could frequently happen if two users of the app were in contact on a bus or in the same building. Yet discrimination is a threat to consider: all the collected data should be anonymised and encrypted using ultimate up-to-date cryptographic techniques. Nevertheless, it is a fact that, for example, although the Italian app *Immuni* works via BLE, it contemporarily needs the GPS to be activated, even if – it says – not recording location data. This is a matter of possible distrust among people, insofar as they are not given the possibility to opt out[77].

*Immuni*, developed by Bending Spoons, poses other important challenges COPASIR analysed, focusing on the composition of that corporation and discussing the following critical points[78]. The collected data, especially their backup, should be stored in internal servers, not into a cloud. Also, the control over data should compete to public institutions, to reduce interferences from hackers, criminal organisations, or foreign intelligence. Other risks could be caused by negligence or bribery between individuals. BLE technologies are not the most reliable, as they can be easily accessed by hackers to fake or delete data. Moreover, while PEPP-PT recommends the cryptographic key being generated from an external server, *Immuni* follows the Apple-Google model, a decentralised system, where the key is formulated by each personal device and exchanged

[75] The reference is to the behavioural dichotomy of thinking fast and slow. The first system is characterised by automatic, emotional and unconscious decision-making; the second one recognises complexity and interaction between things. Nudging improves the latter and contributes to awareness in data sharing. D. Kahneman, *Thinking, Fast and Slow*, New York, 2011.

[76] M.V. Cagnoli, *Contact tracing technologies and data protection: a European perspective*, www.medialaws.eu/contact-tracing-technologies-and-data-protection-a-european-perspective/ (last accessed 27/05/2020).

[77] This fact is not considered in the privacy information people are requested to approve *before* concretely using the app, https://get.immuni.gov.it/docs/app-pn-it.html (last accessed 09/06/2020).

[78] *Relazione sui profili di sicurezza del sistema di allerta Covid-19 previsto dall'articolo 6 del decreto-legge n. 28 del 30 aprile 2020*, COPASIR, 14/05/2020.

with proximity smartphones. This permits a diffuse control on information and higher standards of quality in data protection and security[79], as well as an open source code allows anybody to activate remedies. In the Netherlands, a major defect causing the leak of users' data was so discovered. These problems are a consequence of technologically unprepared governments, also because AI and contact tracing are residual options to manage a pandemic a causal factor of which was the heavy outsourcing of healthcare[80]. A single EU app or 'simply' cross-border data sharing may be a step forward to gain «technological sovereignty»[81]: indeed, a huge risk of an unregulated environment is that tech corporations could exploit the crisis to entrench their power, embedding themselves in a key infrastructure – needless to say, the issue of public funding to research is more actual than ever.

To address some concerns, the eHealth Network released further guidelines[82] to stress the importance of accessibility and inclusiveness not just from a right-based perspective, but especially for effectiveness. The success of contact tracing depends on the number of people using the app. Despite we live in a tech society, many people (children, elders, vulnerable groups) might not possess a device, and healthcare workers usually avoid carrying their mobile on them. What is more, apps need an updated version of iOS or Android, thus excluding who does not have a new generation smartphone or even an 'old' operating system[83]. A satisfying result (60-75% of the population traced) needs manual tracing support. Non-users will benefit from the widespread use the app too. Some citizens, like persons with disabilities, may need additional functionalities, e.g. a complementary location-based approach, with strong guarantees to respect. In point of fact, then, apps like *Immuni* send notifications to contacts (i.e. accomplish their task) only *when* someone is tested positive. The crucial element is not the *quando* but actually the *an* of the testing: it integrally depends on health authorities *if* individuals get tested – and ultimately the number of tests carried out is a matter of political choice on allocation of resources.

In conclusion, States should adopt *ad hoc* legislation to compose all potential conflicts in a *political* context[84], being *aware* of all the known *scientific* implications: «such laws and regulations should not only lay down general principles and guidelines, but also set forth specific and detailed rules on the collection, management, and storage of personal data during a global health crisis»[85]. It must be clear, though, that in this field any conclusion cannot be but *a new starting point*.

[79] *L'app Immuni cambia. Seguirà il modello decentralizzato di Apple e Google*, in *Il Sole 24 Ore,* 22/04/2020.

[80] M. Mazzucato, G. Quaggiotto, *The Big Failure of Small Government*, in *Project Syndicate,* 19/05/2020.

[81] *App contact tracing, l'appello dei ministri Ue: «I dati dei tracciati valgano anche oltre i confini»,* in *Corriere della Sera, 25/05/2020*

[82] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf (last accessed 27/05/2020).

[83] In Germany, the app runs only on devices from Android version 6 or iOS version 13.5 (very recently released) and needs a software which is lacked by Huawei smartphones, among others. *German COVID-19 warning app wins on user privacy*, in *Deutsche Welle*, 15/06/2020.

[84] In Italy, an actual parliamentary debate over *Immuni* lacked, and the app was finally legitimised only by Article 6 of decree 28/2020 (*'Sistema di allerta Covid-19'*), and by the GDPR (which of course is always in force as an EU Regulation). On the contrary, France knew a complete and strongly felt discussion in representative assemblies. *Coronavirus: après l'Assemblée, le Sénat valide l'application StopCovid*, in *Le Monde*, 28/05/2020.

[85] M.V. Cagnoli, *op. cit.*