MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

Subgroup report of

work 6

Report on the activities carried out by subgroup of busy work in the identification of "Technologies for emergency management" (in particular contact-tracing) by evaluating 319 technological solutions received by call for contribution from 24 to 26 March.

Coordinators:
Fidelia Cascini, Catholic University S. Heart Paolo De Rosa,
Department for digital transformation

Subgroup components:
Francesca Bria, UCL London and Carlo Alberto Carnevale Maffè
Innovation Fund, Bocconi University, Milan Ciro Cattuto, University of
Turin
Leonardo Favario, Department for digital transformation Alfonso
Fuggetta, Polytechnic of Milan Andrea Nicolini, Bruno Kessler Foundation

Alberto E. Tozzi, “Bambino Gesù” Pediatric Hospital, Rome Simone
Piunno, Bocconi University, Milan Stefano Calabrese, Department of
Civil Protection Umberto Rosini, Department of Civil Protection

Premise

The international experiences gained in recent months, starting from the onset of the COVID-19 epidemic, show that some technological solutions have been able to promptly reconstruct a precise map of contacts between individuals with infection and healthy individuals offering an important operational tool for prevention actions. The contact tracking (*contact tracing)* with adequate technologies it allows to rebuild chains of potential contagion in compliance with current legislation on the protection of personal data. The use of these technologies has already proven effective in the strategy containment of SARS-COV-2 infection in other countries. In South Korea, for example, it is been observed [1] - thanks to the use of Big Data in mapping and containment of the epidemic - a decrease over time in the effective rate of reproduction of the infection (R_0) obtained by promptly and precisely identifying the *hot spots* of potential contagion by concentrating prevention actions on them. The challenge will therefore be to isolate confirmed cases and their contacts respecting their own fundamental rights and freedoms of European democracies.

Despite the many objections initially raised against the effectiveness of *contact tracing ,* the latest scientific research on the COVID-19 epidemic [2] shows that the only one running diagnostic tests is not enough to reduce the transmission of the infections because the time required for the recognition of cases delays other preventive actions. Of in fact, the clinical manifestations of COVID-19 may be absent or employ some days to express themselves, delaying the recognition of cases with infection. To this yes adds time to receive diagnostic test results. This latency is reflected on the timeliness of the isolation measures of infected subjects. Scientific research highlights in particular that the disease is asymptomatic up to 55% of transmissions with a *generation period* very short (3-5 days). The reconstruction of the transmission chain of the virus starting from the only outcome of the diagnostic tests is therefore insufficient and late (proof is the fact that isolating the positives has no resolutive effects on the reduction of R_0 below unit).

Ferretti et al. [2], demonstrates how even at very high levels of success in the isolation of positive cases, a rapid and extensive identification and commissioning is needed quarantine at least first level contacts to be able to control the epidemic. Currently, reconstructing the contacts of a COVID-19 patient "manually" is proving to be the case slow and cumbersome activity. The Big Data Institute in Oxford therefore offers a *workflow* of [1] reference for the development of technological solutions specifically intended for *contact tracing* for COVID-19, which incorporates the main ethical and scientific elements emerging from the very latest research in this regard. The Big Data Institute model is based on best practices

[1] https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes/

studied in the international models of contrast to the COVID-19 epidemic and outlines the scheme of instant traceability of first degree contacts: a system of *alerting* on smartphone it is able to inform users, based on their contact matrix and possibly their geographical position, compared to when they can move safely, when they have to seek medical assistance when they must avoid vulnerable people. The proposed model has the potential to drastically slow the spread of the epidemic if used by a number sufficiently large of people who use it with adequate fidelity.

In line with the aforementioned publications, the indications provided by WHO at the time of the the pandemic declaration appeared clear and explicit indicating verbatim: " *Find, isolate, test and treat every case and trace every contact* ". Therefore, develop processes e technologies for the purpose of quickly tracking infections, it is essential to circumscribe and to counter the expansion of virus transmission chains, even in countries that, like Italy, apply drastic forms of generalized containment (*lockdown).*

Aligned on these same objectives, the activity carried out by the subgroup working on the examination of 'data driven' technologies for the management of the emergency in progress, is dedicated to support the decisions of political authorities so that they can be facilitated in pursuing the triple objective of: a) ensuring public health protection, b) restoring the most as soon as possible the permissive conditions of the economic and commercial activities after the *lockdown ,* c) allow the recovery of personal mobility under permanent monitoring of possible outbreaks of recovery while guaranteeing the right to privacy and privacy protection of personal data.

Towards a European model

The COVID-19 pandemic poses a serious threat to countries around the world and in especially for the countries of the European Union, currently among the most affected. In the EU, in fact, the virus has spread rapidly and knows no geographical or political boundaries. To put it under control, we must act in the same way: speed and international cooperation they are therefore essential to counteract their progress. In response to the rapidly growing number of cases and the danger of overloading health systems, many countries have imposed constraints on displacements or adopted blockages of economic and social activities to slow down the spread of the coronavirus. Because a long-term blockade is not economically and socially sustainable, some European public and private actors took action to elaborate a response

common that, through interoperable technological solutions of *contact tracing*, allow keep a society and an economy open, protecting the health of citizens without risk the collapse of the health system.

The selection of the reference technological solution at European level was proposed by Pan-European Privacy-Preserving Proximity Tracing international consortium (PEPP-PT),[2] which has over 130 members in eight European countries and includes European excellence in the field scientific and technological research, including also Italian research centers. PEPP-PT is based on a shared approach with the following fundamental characteristics:

- Tested and consolidated procedures for measuring proximity between devices (smartphones) on widely used operating systems and mobile devices.
- Cryptographic data protection, anonymization, GDPR compliance and high cybersecurity.

- International and interregional interoperability to support the tracking of local chains of infection even if one chain spans multiple countries or regions.
- Scalable back-end architectures and technologies that can be implemented with the local IT infrastructure.
- An open source code certification service to test and ensure that several implementations use the mechanisms in a safe and interoperable way.
- Reference implementation available under open source license *Mozilla License Agreement*.

The technology proposed by the European Consortium can make a decisive contribution to a efficient and much faster proximity tracking than the traditional one, in compliance with the citizens' fundamental rights and freedoms, including guarantees regarding the treatment of their personal data, in line with European values and standards.

For this reason, the process to select a technical solution that yields has been activated Proximity tracking possible via *smartphone*, so that they are not tracked natural persons and their personal data are not extracted (e.g. who they are and where they have been); it aims to trace only the short-range proximity relationships that constitute risk of exposure and correspond to potential transmission chains of the virus. The starting point natural for such processes are cell phones since most people use them regularly this type of device and even those who still lack it can be equipped quickly and economically.

The development of this technology is based on three basic principles. First of all, it is the result of an analysis of *benchmark* international and a strong spirit of European cooperation. In Secondly, the technology is studied and selected to be applicable on a level

[2] Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, https://www.pepp-pt.org

international, i.e. interoperable across national borders. Thus, the technology facilitate the resumption of regular international relations and the freedom of movement of citizens. Third, the technology identified must comply with the general regulation on data protection (GDPR).

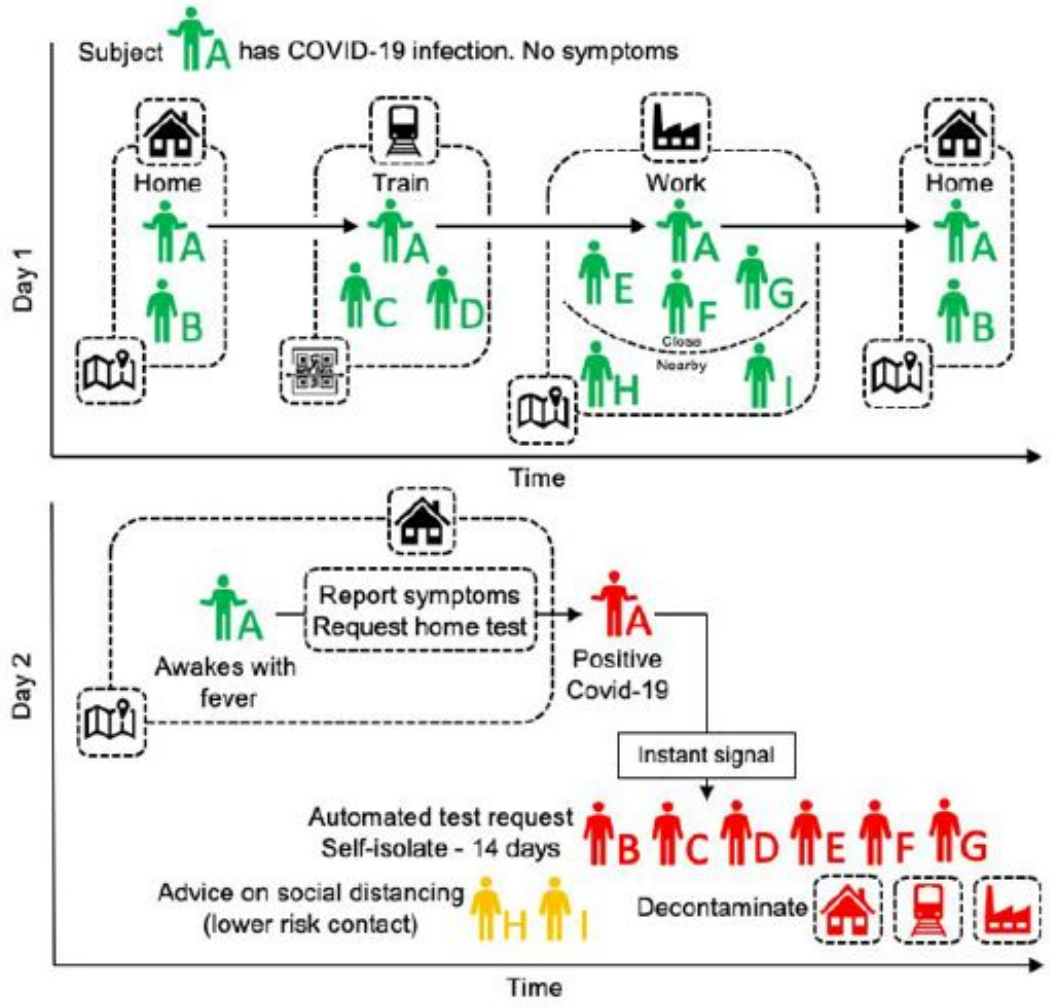
Developing such a system is a great challenge, but one that is worth taking up. How is happened years ago with the creation of the first European standards for GSM cellular telephony, grown in international adoption to become a global standard, the technology of base must provide a proximity tracking mechanism applicable so homogeneous even outside individual national borders. Based on it, each country will be able to develop your own local version of the app and provide your own secure infrastructure. This will allow each participating country to operationally apply the technological solution in coordination with local health authorities for the needs of the local population. Each country must also be able to transparently inform its citizens in this way to convince them, without using authoritarian impositions, to participate voluntarily in such system. The basic technology, developed in constant comparison with authoritative experts of different disciplines, will have to provide an important contribution to allow the tracking of the proximity, also in cross-border mode, respecting privacy, according to a model scalable and open, which can be used from any country.

The selection of solutions was therefore oriented towards full compliance with laws and principles European privacy and data protection. Mechanisms and technical standards are therefore sought to protect privacy, transparency and security in management data, exploiting the possibilities of digital technology to maximize speed and real-time response to the pandemic. These mechanisms include technologies of proven proximity tracking, secure and encrypted data anonymization, reliable mechanisms to allow contact between the user and health officials in a data protection compliant environment, digital data exchange interfaces (API) in can provide anonymized contact chains and risk assessment to other applications (for example for the management of healthcare resources, the management of private risk or the systems of response to the pandemic).

The reference implementation must be based on open source code, with backend services secure and scalable capable of managing hundreds of millions of registered devices, services support for cross-border interoperability, disclosure and adoption by one critical mass of citizens.

Digital contact tracing

By way of illustration, the general operation of a solution is described below the *contact tracing* digital, capable of assessing the risk of virus transmission through monitoring of the number, duration and type of contacts, through a normal one
smartphone . The diagram below proposes a reference operating process for the technological solutions intended for *contact tracing* for COVID-19. The model, derived from the research of the Big Data Institute of Oxford University, is based on the best practices studied in the international models of contrast to the COVID-19 epidemic and outlines the scheme of instant traceability of first degree contacts based on an app to be installed on your own
smartphone and a management infrastructure (*backend)* under the control of the authorities health.

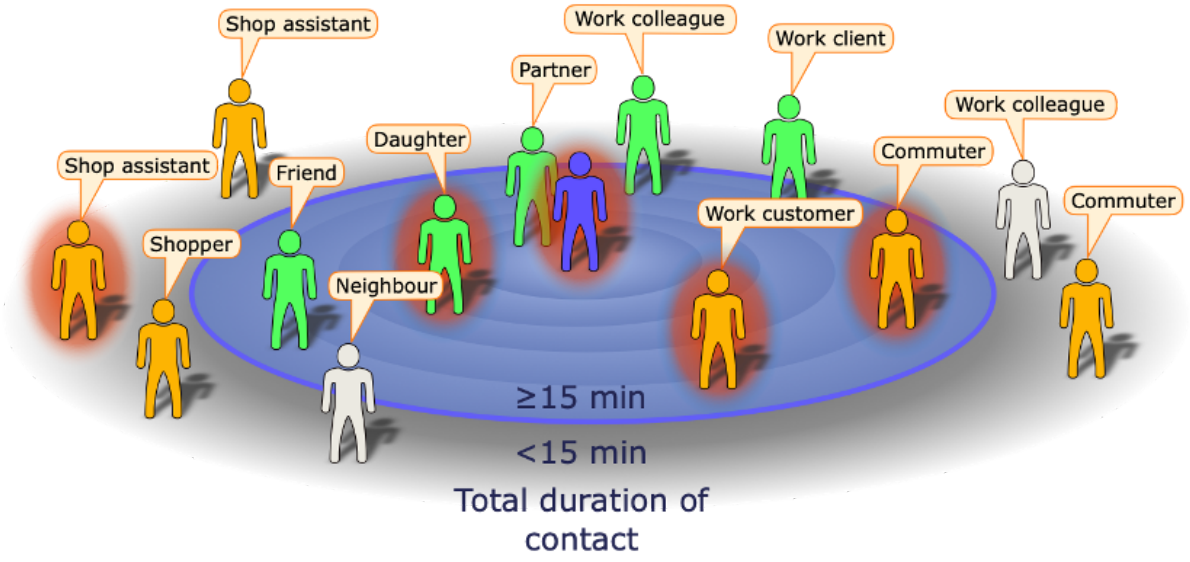


In the top panel the figure illustrates the possible contacts between individuals during daily activities such as for example in means of transport or in the workplace. The bottom panel shows the

series of interventions of isolation and social distance that can be implemented immediately after the SARS-COV2 positive subject is reported as positive to his / her daily contacts previous through the application on smartphones. Source: Sustainable containment of COVID-19 using smartphones in China: Scientific and ethical underpinnings for implementation of similar approaches in other settings, David Bonsall, Michael Parker, Christophe Fraser, Big Data Institute, 16 February 2020.

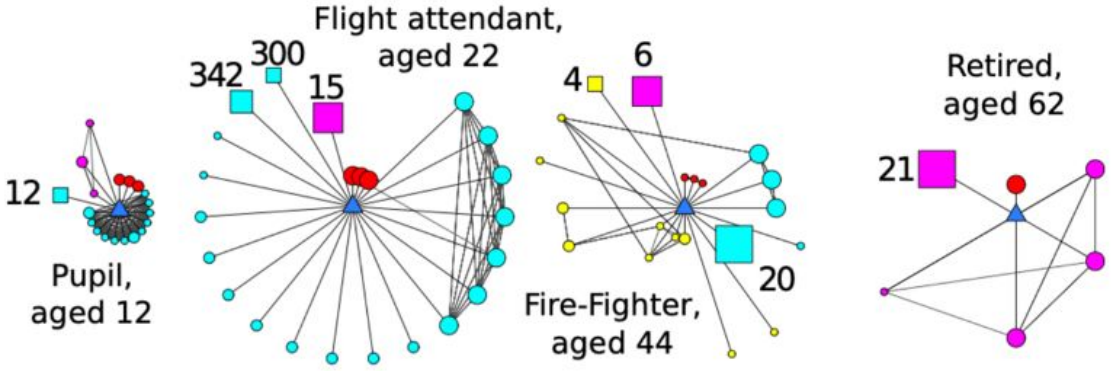
The solution proposed in the European model, indicated above, does not collect data on an ordinary basis personal data, or other data that allow identification of the device owner mobile. The contact tracing solution normally tracks only the number, duration and type of close contacts with other devices in which the same solution is active. However there is a risk that data will be collected during the operation of the solution could compromise the anonymous nature of data processed on an ordinary basis. The user is not necessarily geolocated (although this may be technically made possible, provided that behind a specific and conscious choice of opt-in by the user), neither is made recognizable, unless you explicitly accept these options, where applicable and available. In case of contagion, the information is shared with the health authorities only. Using SAN (Small Area Network) oriented data transmission methods such as ad example ANT, BT-LE, BT, AUDIO and WiFiP2P according to the sensors available on the device and crossing (where possible and always with the explicit authorization of the user) i position data from GPS and Network Position (cell-based triangulation phone numbers), the phone acquires a unique and encrypted ID of all smartphones in proximity (about 1-2 m., but in some cases even beyond) and preserves the duration and distance estimated of such close contact. Scanning occurs at programmable periods of some seconds, even with the app in *background* . The technologies selected must be able to track i contacts near the potentially infected subject with very high precision, in the order of a few tens of centimeters.

With reference to *contact tracing* traditional, see the following graphic representation of encounters made during the day by an infectious patient (blue) with contacts positioned according to the total duration of the contact. In the diagram below, the definition of "Contact" refers to someone with whom the infectious person met for 15 minutes or more. Some contacts will be traceable (green), while others will not be traceable (Orange). A definition of contact that is too restrictive and inappropriate for infection with COVID-19 would imply that some meetings may fail to satisfy the definition, but could still be at risk of infection; in turn, these excluded contacts may be traceable (light gray) or non-traceable (orange).



Source: Matt J Keeling et al., *The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi:* https://doi.org/10.1101/2020.02.14.20023036

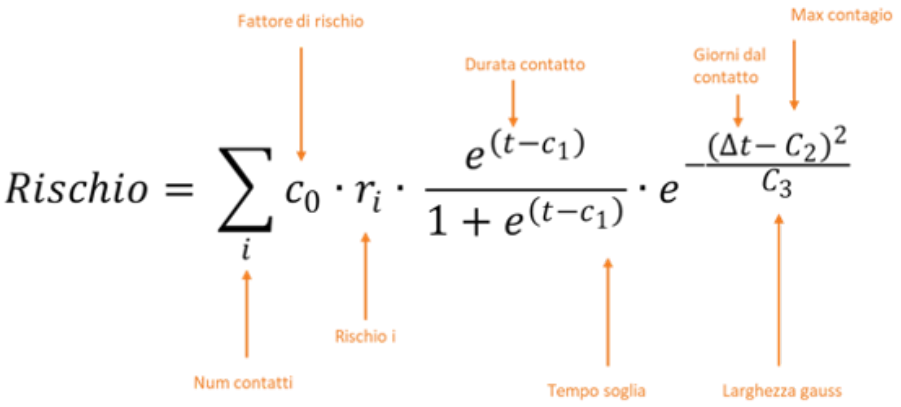
It is appropriate that the technological solution, also through data post-processing algorithms anonymous and encrypted, can reconstruct the "social graph" of the with adequate precision interactions relevant to epidemiological purposes. By way of example, in the graph below, the infected subject (ego) is the central blue triangle; the circles represent the individual contacts, i squares represent the groups of contacts (the size of each group is indicated). THE colors represent the social categories of the meetings (red = home, cyan = work / school, yellow = travel, pink = other). The larger dimensions of the symbols represent a duration of contacts longer, while greater closeness to the individual indicates that contact is more frequently.



Source: Matt J Keeling et al., *The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi:* https://doi.org/10.1101/2020.02.14.20023036

It should be noted that, based on the current technological constraints on some types of devices, in especially those based on the iOS operating system, the only proximity tracing via Bluetooth is likely not to maximize the probability of identifying all contacts, as it does it may not be able to intercept the signals from devices where the functionality Bluetooth do not operate consistently with the purposes of the application. It is therefore believed It is advisable not to exclude a priori the possibility that, under the condition of informed opt-in e aware, the technological solution to be implemented can deal with some punctual and limited geolocated information, not oriented to reconstruct the routes but limited to specific places of potential contagion, especially if with high density and frequency of contacts, in as not all possible contacts could have devices (due to a minor one penetration of smartphones, especially among the elderly population) or installed apps (minor adoption / compliance by the population). In the event that it was deemed to be used the geolocation features of the devices even if in limited hypotheses it would be necessary, obviously, reviewing the considerations on the anonymous nature of the data processed is not shown as much as possible to rely on actual anonymity.

Furthermore, cases of environmental contagion could have occurred and therefore it could be sanitization of places / premises required. It could therefore be judged in addition to the list of proximity contacts, the solution should also retain a *timestamp* and a limited chronology of geo-locations for the previous 14-21 days, but the collection of such data, even after the user's opt-in, must be carefully evaluated on the basis the risks of re-identification that it entails, as the use of the position nullifies - de facto - any form of authentically privacy-preserving approach e *can make more the public communication and user acquisition strategy is less complex and less effective who voluntarily use the aforementioned app .* It is noted in this regard that the German Parliament has recently denied the possibility of using GPS information for contact applications tracing, by approving a bill to this effect on March 27, 2020. The probability of contagion is normally calculated on the basis of a model that holds account of the duration of the contact, the days that have passed since the contact and the number of these contacts. THE numerical parameters (in the diagram below, indicated with c0 ... c3) are initially estimated starting from the data in the scientific literature and come later updated as the system allows you to learn the details of the mechanism spreading. Below is proposed, by way of example, a general and synthetic form of the contagion risk calculation method:



In the solution proposed by the European consortium, data are normally kept only on the user's device. Depending on the objectives of the service, some aggregated data e encrypted they can eventually be periodically saved on a protected database, for limit the risks of loss or damage to the device and related contact data. Limited to verified cases of contagion, such data may be shared with the health authorities for the necessary containment and prevention measures.

The acquired data and the calculated risk can be made anonymously accessible to health authorities, which can read risk data and update a person's status (negative or positive on the test). The risk calculated for the individual user is a function of data of other users. If one person tests positive, the risk of each other person with whom this has come into contact is updated according to a precise alerting procedure. For example, if a person you have had contact with 5 days before it proves positive, the risk of infection is updated on his mobile phone. Each receives information about their own risk status, not that of others. The citizens they can be informed in real time and they can spontaneously take measures precautionary measures (voluntary isolation) towards the closest people. The authorities local health can thus have an important tool to focus tests on people who have actually had contacts at risk of contagion.

More in detail, in order to be able to converge with the model of *digital contact tracing* proposed by the European PEPP-PT consortium, the desired functioning of the *contact tracing* can be summarized as follows:

1) Sending an anonymous identification code.

Each enabled device transmits a temporarily valid, authenticated and identifier (ID) anonymous that is not connected to a user or a phone number. The proximity between phones of other users of the system is estimated by measuring the radio signals emitted by the device (Bluetooth, etc.) using tested and calibrated algorithms.

2) Recording of the proximity history.

When device "A" is in epidemiologically relevant proximity to device "B" for an epidemiologically sufficient period of time, as determined by the empirical measurements and from medical heuristics, the anonymous ID of phone B is recorded in the encrypted proximity history stored locally on phone A (e the other way around). In the model proposed by PEPP-PT, no geo-localization, none personal information, no phone numbers or other data are recorded, so as not to allow user identification in any way. This contact history of Anonymous proximity cannot be viewed by anyone, not even by the phone user "TO". Older events in the proximity history are progressively deleted when they become epidemiologically unimportant (e.g. after 21 days)

3) Use of proximity history: two operating modes.

Mode 1

If a user has not been tested or tested negative, the anonymous proximity history remains encrypted on the user's phone and cannot be viewed or transmitted by nobody, not even from the health authorities. At any time, only the history of proximity that could be relevant for virus transmission and previous history is continuously deleted.

Mode 2

In the model proposed by PEPP-PT, if it has been confirmed that the user of phone A is SARS-CoV-2 positive, the health authorities will contact user A and provide the user a special encrypted key, to ensure that no potential malware can enter incorrect information about the infection into the system. The user uses this special key to voluntarily provide information to the national health service which allows the notification of apps registered in the proximity history and therefore potentially infected. Since this history contains anonymous identifiers, neither person can be aware of the other's identity.

4) Health service operation dependent on the country and / or region.

Anonymous IDs contain cryptographic mechanisms to identify the country and / or region of every app that uses the system. Using this information, anonymous IDs are managed country-specific.

Mode 1

If both the anonymous IDs of phone A and B come from the same country, the anonymous ID of the potentially infected part can be marked, so that when the app this part asks for information on its status, the app will be informed of the possible exposure.

Mode 2

If an anonymous ID of phone B is identified as associated with another different country from phone A, information associated with the anonymous ID of phone B is transmitted to national health service of the other country. This transmission is completely encrypted and digitally signed. Further processing is performed by the service national or local health of the country / region that issued the app.

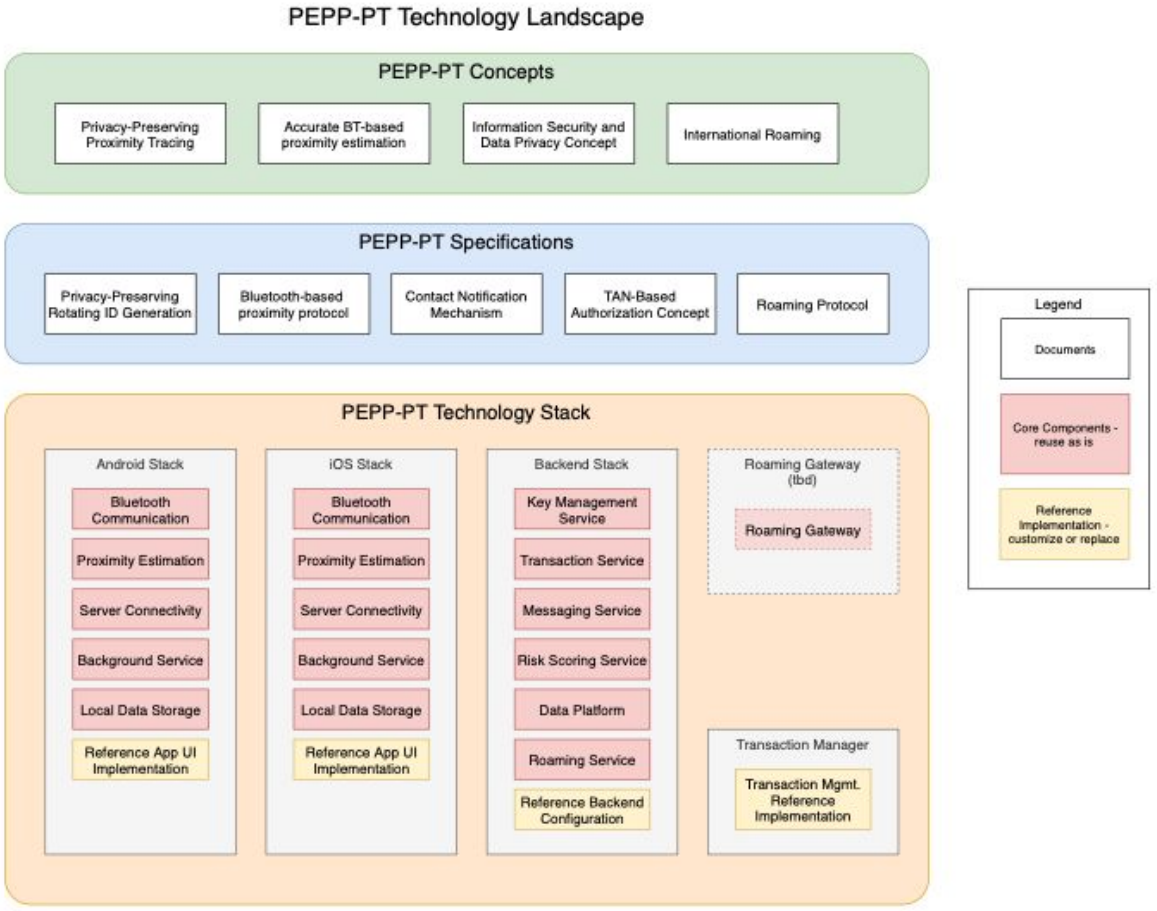
5) Health processing

The process on how to inform and manage exposed contacts can be defined country by country, in such a way as to guarantee interoperability of the processes between the different authorities local health.

6) Information and infrastructure

All procedures, mechanisms, standards and system codes go constantly monitored by the security team. In parallel, the national security agencies IT and national data protection agencies regularly monitor all lines of code and validate them from the point of view of cybersecurity. All that comes released to the public is controlled to prevent unwanted effects in procedures or in the code.

The scheme of the technological architecture proposed by the PEPP-PT project is reported in the following figure, which incorporates the concepts, the high-level specifications and the structure of the stacks technologically described above.



The evaluation process

The activities of the data-driven Working Group for the COVID-19 emergency have been introduced by one *fast call for contribution* lasting three days (from 24 to 26 March), as part of an interministerial initiative called Innova for Italy, promoted by Ministry of Economic Development, from the Ministry of University and Research, from Ministry for Technological Innovation and Digitization, from the Ministry of Health.

The 'Technologies for the emergency' subgroup has dedicated itself to the identification of technologies for identification of cases of potential contagion (*contact-tracing)* immediately usable to manage the epidemic emergency and possibly improvable with quick and easy modifications. [3]

[3] The assessments were carried out by a team made up of the following people: Carlo Alberto Carnevale Maffè, Ciro Cattuto, Leonardo Favario, Andrea Nicolini, Alberto E. Tozzi.

At the end of the *call for contribution ,* the general process aimed at identifying of the proposals was divided into five steps. In particular:

1. creation of a reference grid containing the minimum requirements necessary for select the technological solutions;
2. use of this grid for the selection of proposals to be submitted for characterization technique by expert members of the subgroup;
3. verification of technological solutions with reference to current legislation in particularly regarding privacy;
4. elaboration of a summary document containing the description of the characteristics technically better proposals that respond to the immediate objective of responding to the epidemic emergency;
5. validation of the document of technical experts by the assessors indicated in Ministerial Decree for Technological Innovation and Digitization of March 31st 2020

For the attention of members of the subgroup 'Technologies for emergency management' 319 proposals were received. The examination, aimed at the selection of proposals technically more responsive to the need to contribute promptly to the government of the emergency, was divided into three successive phases. In particular:

1. General screening , which allowed the identification of 15 solutions corresponding to essential minimum technical requirements;
2. Analytical characterization, which led to the selection of one *short list* of 5 target technological solutions, technically ready for use *contact tracing;*
3. Technical interview conducted on the *short list* of the 5 target solutions, for the definition of those among these 5 that offered that they respected in the best possible way the greater number of defined criteria.

The general screening phase 1 was carried out by 5 examiners, based on a fact sheet analysis specially studied and prepared by the technicians of the subgroup before the examination of the proposals. The criteria taken as a reference are shown in table 1 and are each was considered according to a value of sufficiency (1) or insufficiency (0). All the proposals that, during the examination, obtained an overall score of all the criteria less than 5, they did not pass to phase 2 of analytical characterization.

Ta beautiful 1.

	Screening criteria	**Value**
TO	The application plays **the digital contact tracing function ?**	1 = yes

	B The proposer is a Public Administration, a public company or private, public or private research body or center, association (which can interact with associates able to respond to these needs), cooperative, consortium, foundation or institute?	1 = yes
	C The proposed solution turns out **concrete, already built or available** for the implementation in a short time and compatible with the emergency?	1 = yes
	D The technical approach of detecting proximity Physics takes place a means of direct communication between the devices (e.g. via Bluetooth radio technology) and is independent of information otherwise obtained on the position of users in space (geo-location, GPS, WiFi SSID, cell of the mobile network, etc.)?	1 = yes
	IS Availability of the technological solution and times for the activation of the deployment services (*assess the speed with which technology can have impact; assign the value 1 if it is estimated that the services can be active within 15 days, 0 otherwise. To consider also application adaptation developed for other purposes).*	1 = yes
	F Technical aspects of proximity detection (*evaluates the goodness of the solution in terms of accuracy in the detection of parameters with an epidemiological value (e.g. resolution of the distance, starting time and duration of contacts) assign the value 1 if the proposed solution allows proximity measures short-range passive device-to-device and calibration of the strategy proximity detection, 0 otherwise).*	1 = yes
	G Technological / performance and scalability aspects *(1 if the solution is based on FLOSS code, scalable architecture and appropriate data encryption solutions, privacy protection e data minimization).*	1 = yes

The analytical characterization phase 2 was carried out by 5 examiners with the use of the following indicators and criteria, divided into three categories:

Technology

- FLOSS solution: all the source code of the solution is covered by licenses FLOSS compatible with each other and is available within a public repository complete with documentation.

- The solution has no proprietary (software and / or architectural) dependencies that may constitute lock-ins.
- The technical solution allows passive short-circuit device-to-device proximity measurements radius.

- Calibration of the short range proximity detection strategy (to take into account hardware differences between different smartphones).
- Maximum distributed approach: minimization of contact data recorded in centralized way to the data strictly necessary for contact tracing measures, testing and containment.

- Possibility of international deployment, with privacy-preserving interoperability of national servers (roaming features).
- Ease of connection of the technical solution with the epidemiological and clinical process of contact tracing.

- Temporal sampling of proximity relationships at sufficient frequency high, passively activated.

- Power saving strategies that reduce battery use and resulting user churn.
- Information on the context of the contacts (eg, contact "indoors" or "outdoors").
- Elastically scalable and multi-tenant architecture (limited number of interactions with the backend, non-monolithic backend architecture).
- Privacy-preserving technology, with options through informed consent: absence of private entities with access to individual data.
- Use of cryptography *state of the art*.
- Possibility of deleting your local / remote data.
- Low technical debt (complexity of maintenance, deployment, management)

PM & deployment

- App already released in stores, number of downloads and feedback collected.
- Testing level reached (codebase maturity).
- Ease of use and incentives for adoption.
- Existing user base and / or possibility of refactoring the solution already adopted.
- International approach. Allows exchange of best practices, testing distributed on larger population, reduction of costs and risks.
- Technical approach that leverages the experience of research groups internationally recognized in contact tracing with digital means. Integration with health systems local and general practitioners.

Data analytics

- Ability of the solution to detect parameters of recognized epidemiological value for an airborne pathogen: resolving short-range proximity interactions radius, temporal resolution of individual contacts.
- Use of robust ID for interoperability with other databases in case of decryption.
- Integration with other information from an integrated contextual questionnaire.
- State-driven, data-enhancing data analysis strategy of the art of scientific literature relevant to contact tracing, outbreak investigation, high-resolution contact networks.
- Individual risk scoring mechanism that leverages graph analytics.
- Machine learning techniques in support of contact tracing and scoring of risk.

- Availability of a mature / already tested / integrated data analysis platform with the application back end.

User Experience / User Interface

- End-user-centered design approach to the project (user search, interaction design, visual design, information / content architecture).
- Design focused on usability and accessibility.

Phase 3 of technical interview with applicants who have returned to *short list* allowed to deepen some aspects including:

- solution maturity / internship;
- security / reliability;
- technology of *contact tracing* used;
- development approach *software ;*
- architecture and approaches to *deployment ;*
- potential analysis *lock-in (software ,* infrastructural);
- presence of critical components that cannot be released with FLOSS licenses;
- composition of the team, partnerships and roles;
- roadmap analysis.

Interview 1 - ProteggInsieme

From the interview with Whatif srl, the group proposing the "ProteggInsieme" solution, it is clear that the offer was entirely built starting from the solution proposed by the Government Singapore Digital Services team is protocol-based *Bluetrace.*[4] In this sense, the state of ProteggTieme together today is very preliminary (*concept)* that is, there is no version functional and testable of this product and this is attributable to the fact that the source code

[4] BlueTrace: https://bluetrace.io/

of the *software* developed by the Singapore team has not yet been made available to third parties. Furthermore, as *Bluetrace* is a protocol based on Bluetooth technology, it is believed It should be noted that the ProteggInsieme team does not have a track record of experiences past with regard to this specific technology but could rely on own network of partners to remedy this. Finally, the interview made it clear that the proposal ProteggInsieme needs further development on several fronts to be ready to respond fully to the challenge of digital contact tracing.

Interview 2 - TrackMyWay

The "TrackMyWay" solution, proposed by Antares Vision spa, is based on know-how solid of the proposer in the world of tracking consumer goods (such as, for example, tracking of drug shipments). In this sense, the solution is strongly focused on the technologies of backend owned by Antares Vision useful for the reconstruction of the contact graph for each node. In detail, the proposal plans to collect a variety of information through a mobile application (such as, for example, GPS coordinates and any contact with others device detected via Bluetooth) which must subsequently be sent to backend consisting of the aforementioned technologies. Anyway, from the interview I'm not the choices regarding the measures useful to minimize the amount of information were clear to be withdrawn and subsequently transferred to the backend, the strategies to be adopted for management the different responses between the various Bluetooth devices and the possible ways to detect them iOS-to-iOS events. Furthermore, although the team has proven experience in the field of

tracking digital moving objects via GPS technology there is no track record significant in the field of *digital contact tracing.* Finally, the proposed architecture appears to have a centralized nature which represents a possible problem in view of commissioning national exercise.

Interview 3 - CovidApp

The solution called "CovidApp" was proposed by a team of developers independent. The interview with the team shows that the problem has been analyzed in a way in-depth analysis and many of the possible scenarios that could also occur on a national scale have been examined in detail. CovidApp is therefore an application-based solution mobile for the management of the *contact tracing* through technology *Bluetooth Low Energy .* In Primis, the application collects data relating to registered contacts that are registered inside the device. Subsequently, the application sends the collected data to the backend-every 4 ore- which processes them to build the contact graph. In this perspective, it is noteworthy the approach used for the detection of contacts between devices with the iOS operating system which plans to take advantage of triangulation with other devices running Android and

subsequent reconstruction of the proximity graph. A possible disadvantage of this solution is that a lot of information needs to be sent to the backend several times a day which it not only increases the requirements in terms of computational and storage resources, but it could be a scalability problem for the whole architecture. Note also that the representation of the proximity graph centrally at the backend, where each node and interaction are represented

regardless of being identified

respectively as cases or as risk interactions (i.e. regardless of the process of *contact tracing)* involves higher data protection and privacy risks than distributed approaches which are equally effective for strategies *digital contact tracing.*

Subsequently, the interview allowed to detail the alerting process envisaged by this solution. This offers to health authorities, following the detection of a case positive, the ability to automatically and immediately activate the alert. Moreover, the latter is guaranteed to be completely anonymous as it is not necessary to have the your mobile phone number or your personal identification number. Notice like this feature differs significantly from the PEPP-PT model, which instead requires mandatory - to activate the alerting process on the contact log - consent and active collaboration on the part of the user recognized as positive and who must proceed in order to proceed enter a TAN code on your device.

Finally, during the interview it was possible to attend a real-time demonstration of the product that is currently under private testing among team members.

Interview 4 - Immune

The proposal called "Immuni" was formulated by a pool consisting of Bending Spoons, Jakala, GeoUniq and Santagostino Medical Center. Each of these actors has participated in the realization of the presented prototype.

The interview allowed to know the genesis of the project and understand some choices architectural. In detail, the concept behind Immuni comes very close to that proposed in the BlueTrace protocol presented by the Singapore team. In fact, Immuni takes advantage of the Bluetooth Low Energy (BLE) technology to recognize the interactions between two devices. Of consequently, each of these events is saved in the device memory in mode encrypted. Note that this information never leaves the device unless the owner is diagnosed positive to the virus. In this case, the information relating to all Contact events previously recorded by the device are sent to the backend afterwards explicit owner authorization. Only at this point will it be possible to rebuild a backlinks the chain of contacts and, where necessary, the platform may send a notification to all devices affected by contact events.

As for mobile device coverage, the team says they can track correctly 94% of Android-Android and iOS-Android contacts. Instead, however long concerns the detection of contact events between two devices with the iOS operating system, the

team proposed two possible alternatives: the first consists of a software device while the second is to use the GPS signal. This second strategy turns out to be particularly accurate thanks to a software library developed by GeoUniq. Note, however, that using this proprietary library would lead to a software lock-in. As for the back-end, the solution consists of FLOSS and components currently the test architecture is functioning within the infrastructure of Google Cloud but, since no proprietary components have been used, the lock-in risk.

Finally, the interview made it possible to get to know the team which seemed solid, with experience both in the roll-out of large-scale mobile applications and in project management complex software also in FLOSS mode. Even the epidemiological aspects of the application have been developed thanks to the partnership with the Medical Center Santagostino.

Finally, note that the team has already joined and actively collaborates with the Consortium European PEPP-PT. The latter is a positive factor regarding the ability to work on a pan-European level and with a view to implementing a solution in a short time European Union.

Interview 5 - SafeTogether

The SafeTogether proposal, put forward by Microsoft srl, aims to create one versatile data collection platform for the ongoing pandemic. From the interview with the The proposing team shows that the SafeTogether solution is in a very phase preliminary construction (*concept).* In fact, to date there is no real solution usable but there are only possible use scenarios and the roadmap of project estimates about 4/5 weeks for the construction of a preliminary object to be tested on the field. Specifically, the SafeTogether proposal contains several infrastructure components and backend with the aim of facilitating the collection and analysis of data, but not it has an application frontend which makes it difficult to imagine a real use case. For regarding the direct experience with the pandemic currently underway, the team of SafeTogether pointed out that the model they theorized follows what was implemented from the Singapore GDS team (TraceTogether).

Extra interview - COMBAT

In order to deepen also some proposals that have not explicitly declared of use the technologies of *digital contact tracing* more common, the evaluation team has deemed appropriate to proceed with the technical interview with Telecom Italia Spa as proposer of the "COMBAT" solution.

The interview made it possible to clarify that the "COMBAT" framework consists of two complementary solutions to each other. The first is purely aimed at the exploitation of data of telephone cells already available to the proposing group while the second is based on a mobile application.

As far as the first solution is concerned, the proposal provides for the exploitation of the information regarding the telephone cells and extracting the information useful for the *tracing.*
This type of approach is completely transparent towards the end user to whom, however, the possibility would not be explicitly offered for a possible opt-out. Moreover, currently the accuracy of this approach for the purpose of *tracing* is not comparable to that offered by other technologies.

The second approach, however, involves exploiting a mobile application to be created *former novo* . This application could fill the gap left by the presented solution previously as it would allow to obtain a higher intra-cell resolution e provide this data to the backend for an ex post tracing graph reconstruction. Note, however, that currently the second solution is in the very preliminary phase of realization (*concept)* is therefore it was not possible to evaluate their maturity. Finally, the roadmap declared for mass the second solution was estimated in 4 weeks.

Technical characteristics of the solutions

At the end of the three phases of the process *selection, characterization and evaluation of proposals* a synoptic table of the solutions considered the most has been created reliable, to illustrate the main technical characteristics, strengths and possible critical issues.

Solution name	**immune**	**CovidApp**
Technology	Native app, iOS (Swift) e Android (Kotlin).	Native, iOS and Android app.
Program Management	Team with experience in roll-out of mobile applications towards millions of users. Team includes skills vertical in mobile app development, date analytics, wait epidemiological, geolocation.	Distributed team created ad hoc. Prototype of the realized application and currently undergoing private testing intra development team.

	Prototype of the application created and currently under private testing within the development team.	
Strengths	Integrates the "PEPP-PT" solution. Strongly decentralized architecture. Wide spectrum of possibilities for privacy levels and opt-ins. The information remains encrypted on the edge and are removed progressively each 14/21 days. High backend scalability.	IOS-to-iOS contact detection by elaborated proximity graph in the backend as triangulation between Android contacts.
Critical issues	Detection of the contact iOS-to-iOS not managed	Centralized architecture: centralized representation of the proximity graph for all users, regardless of diagnosis, with temporal continuity. Stronger scalability constraints e backend performance. The centralized representation of the proximity graph in the backend implies greater risks than date protection and privacy.

Realization and experimentation

To accompany the exit from *lockdown* country, it is vital to foresee a trial particularly careful though quick to validate and commission the solution chosen to guarantee the achievement of the objectives.

In light of these considerations, the implementation process must be redundant and must be based on at least 2 solutions, in order to be sure of having at least available a solution to be put in place if, in the concrete experimentation phase, one of the chosen options proved to be for any reason unable to offer functionality and / or required performance levels. For this reason, it is proposed to articulate the process of implementation of the solution *contact tracing* long **parallel paths** according to following model:

to. Make a thorough *assessment* security on the whole source code, the architecture and system of the solutions identified, including risk assessment and threat modeling (by the *intelligence).* It would also be appropriate share the source code with the cyber scientific community with a view to having reviews from the largest number of specialists in the sector possible.

b. Carry out a phase of *test* in the field for each solution pre-selected in different limited areas of the territory (for example, some urban territories). Such a test will be conducted on a sample of subjects (for example, law enforcement and civil protection operators) who, moving on the territory despite the measures restrictive of the movements still in progress, they can already verify the correct how each solution works.

For this to happen, you must first complete a few steps:

the. establish the necessary protocols for using the application (by staff medical-health, public security forces and citizens / testers);

ii. improve the functioning of the application on the basis of needs encountered, integrating any features to better respond to requests that emerged during the test phase;

iii. define the necessary coordination between territorial bodies, ISS and Protection Civil for the use of the application.

This parallel testing phase of the candidate solutions should start immediately after the phase of validation and choice of technological solutions by the Government Authorities e last approximately 10 days, so as to make available the application that presents the

better performance for large scale use from the beginning of the exit process
lockdown.

In addition, it is necessary that, in parallel with the commissioning of the technological solution (test phase), the following objectives are pursued:

1. outline strategic-organizational processes in the health sector, useful for to govern the contagion control system as a whole and to follow up on it operationally to the indications that will emerge from the availability of the traces (such as the management of infected potentials and their isolation and care), including the program that will be put in place for communication and training towards healthcare personnel;

2. define the legal and technical aspects relating to the subject of privacy, ethics and security b *y design ,* including the data flow map, the subjects who have access to the data, and the access conditions;

3. define a process *governance* which will oversee the exercise, the evolution and evaluation of the tracking system in its operational phase;

4. evaluate the integration with the existing technological infrastructures for the management of the centralized databases.

For the operational management of the solution of *contact tracing* six are needed key components:

1. A public authority that plays the role of *Driver* of the execution of the whole project, taking care to take care of the implementation of all necessary activities e coessentials for the *contact tracing* is usefully employed on a national scale (training of doctors, technical support to users, etc.). It is strongly recommended that a figure of *Program manager* with mandate executive, in particular for the initial phase of the project.

2. An interdisciplinary development team that brings together technological and development skills public health with strong leadership and digital skills needed for guide the development and maintenance of the solution, also collaborating with the European stakeholders (these characteristics should be sought in a private entity or in a consortium of private entities that support the development of the code of application components of the identified solution).

3. A governmental entity that can manage, through a service provider publicly controlled technology, the technological infrastructure of the contact service tracing, ensuring maximum security and high reliability of the service.

4. One *governance* clear and transparent information entrusted to the health authority national and civil protection.

5. A widespread and widespread campaign of *nudging ,* communication and information of the citizenship, in order to encourage active and conscious, guided participation by the Prime Minister for maximum authority.

6. Supervision of the entire process by public security and the sector of *intelligence* .

The following table summarizes purely a hypothesis of subdivision of the skills among the actors involved in the implementation and management of the *contact tracing* .

	Program Manager	Team of development	Service manager technological	Health authority	GPDP	PCM	DPC
Definition Roadmap	TO	R	R	C	THE	C	THE
Development and maintenance of the technological solution	R	TO	C	C			THE
System management contact tracing	R	C	TO	THE			C
Ensure anonymity of the data transmitted	R	R	TO				
Clinical health management and activate the contact tracing	C			RA			
Security supervision	R	R	R			TO	THE
Privacy supervision	R	R	R		TO		
Campaign of communication	R			C		TO	THE

Legend:

- **Responsible (R)** : it is the person who performs and assigns the activity
- **Accountable (A)** : it is the person who is responsible for the result of the activity.
- **Consulted (C)** : is a person who helps and collaborates with the Responsible for the execution of the activity.
- **Informed (I)** : it is a subject that must be informed when the activity is carried out.

Great importance in this regard assumes one *Road map* of agile development that includes one series of releases spread over time of the use of the technology, whose profitable use in the containment of the epidemic and in the prevention of new infections requires time and resources dedicated.

For the preliminary estimate of the times and costs of development, testing and national roll-out, you can divide the overall program into three phases:

1. **Alpha (** prototype for the first functional tests) **+ Beta (** perfecting and testing phase in the field in defined contexts / areas). This phase can take about 3 weeks of work with costs deriving mainly from the technical team involved on the two prototypes that will be chosen to limit the risks.

2. **National Roll-Out** . Progressive extension of adoption throughout Italy.
   This phase can take about 3-4 weeks with the most significant costs due to communication program and setup costs and progressive expansion of the infrastructure, in this case relating to the only solution that will be chosen for normal use

3. **Fully operational software management** . This is a phase of indefinite duration, during the
   which the system is armed and progressively expanded and improved using the information acquired in the field to refine precision and effectiveness, add additional features of which - after the launch has already taken place - discover the usefulness, as well as ensure continuous integration with analogues programs carried out by the other European countries with which it will be understood collaborate.

For any new version with significant additional features, to be developed in "agile" mode, it is possible to prudently estimate a total number of hours of work equal to development of the basic version.

For immediate operation on **secure cloud infrastructures** and with very high reliability, the cost prediction can depend on many factors, mainly represented by the number of people who will install the application, by how often the application will contact the system *backend* by updating the data, by the amount of people who will have to be alerted because you come in contact with positives, from the data size of tracking on average produced by each person. Comparing with similar projects, it is possible to imagine that the overall cost of the project could be, prudentially, at the most in the order of a few million euros a year.

The basic software features provided here include Bluetooth LE, the clinical diary, the user interface and the safe software integration with the cloud infrastructure, in addition to the functionality necessary to operate the system end-to-end. Other features such as the are not included in the estimates of costs and initial times georeferencing of some data or the development of the territorial data analytics system e integration with regional and national health databases. These extensions are from deemed necessary but will have to be evaluated and estimated at a later stage after the start of the project. In case the authorities decide to follow the recommendations of the Work, or proceed with two solutions in parallel for the alpha + beta test phases, at general estimate of operating costs an amount due to the experimentation will be added with the "plan B" application, which will in any case be marginal compared to the total cost operation.

Other costs that must be taken into consideration will be, by way of example and not comprehensive, communication and advertising costs, integration costs with any solutions international, the costs for cross-border contact tracing roaming services e of alerting, the costs of developing specialized dashboards for specific institutional purposes or medical and health care.

Considerations on security of information

An application solution with such a wide diffusion in the population lends itself with high probability of becoming the subject of numerous attempts at fraud and / or cyber attacks. Any compromise activities could, for example, be based on techniques of phishing, such as creating apps or "owl" sites with fake logos or names that could be mistaken for the service itself by end users.

It is therefore vital to pay close attention to the safety aspects of the information of the entire system *contact tracing ,* in order to guarantee the necessary resilience and the operational continuity of the services, also as a contrast to external attempts by systems compromise. It has not been possible to date, given the limited time a provision, carry out a thorough security audit of the source code of the two applications candidate to the testing phase. Therefore it is strongly recommended to carry out this audit as soon as possible, as well as a thorough *assessment* on the proposing subjects and the third-party technological components used. A risk assessment is also recommended (*risk assessment)* wide-ranging of the whole system of *contact tracing* and all those involved, with particular reference to the different implementation hypotheses that can be identified.

For this reason, the involvement of the safety authorities is necessary national with specific skills in the field of *cybersecurity .*
Finally, to ensure greater security and transparency, after the verification performed by the above authorities, it may be appropriate to publicly release the source code of applications, so that the whole community of experts in the field of *cybersecurity* to national level has the opportunity to scrutinize the system and report any problems not yet detected.

This choice would, however, contribute to raising the level of trust in the project by the citizens.

The following table shows, for purely indicative purposes, a preliminary and non-exhaustive risk analysis (type and level of risk associated with the solution, together with possible mitigations), developed on the basis of the methodology *STRIDE (see legend)*.

Type	**Risk**	**Level**	**Possible mitigation**
Information disclosure / Spoofing	Phishing by counterfeiting and spreading fake news	Tall	Distribution of the app exclusively through app stores and information campaigns
Spoofing	Pollution of contact lists High in the	CovidAp case p	Certificate-based client authentication system (certificate pinning)
Denial of Service	DoS / DDoS attacks on backend endpoints	Tall	Distributed architecture, DNS and anti-DDoS countermeasures
Denial of Service	Boycott of the solution using disinformation campaigns	Middle	Nudging and information campaign, surveillance by AGCOM
Information Disclosure	Exploit of the code or injection of trojans in the application in order to collect information on the GPS, MOBILE, WiFi SSID position etc.	Middle	FLOSS is community based, responsible disclosure policy, bug bounty
Elevation of Privilege	Exploit of the backend in order to report possible false infections by sowing panic	Tall	Hardening backend, frequent audits and logging analysis, SOC
Tampering / Data integrity	Alteration of information saved on the device and / or sent to the backend. They would make construction of the proximity graph impossible	Middle	Audit and monitoring of cryptography systems and data structure
Non repudiation	Declaration of not having accomplished a certain action (not having had contacts)	Tall	Nudging / communication and informed consent
tampering	Switch off the BLE device to not record contacts	Bass	Audit of the ex-post device logs

Legend:

STRIDE is[5] a methodological process that helps identify security threats in a complex system,

- Spoofing (identity forgery): the claim to be something else or someone else who is not.
- Tampering (alteration of data): the alteration of something that is assumed to be unchanged.
- Repudiation: it means declaring that you have not done something (regardless of whether it has been done or not).
- Information Disclosure: concerns the exposure of information to people not authorized to view it.
- Denial of Service: Denials of service are designed to interrupt the service.
- Elevation of Privilege: occurs when a program or user is technically enabled to do things that are assumed not to do.

Privacy

For considerations on the protection of personal data and privacy refer to report produced by the subgroup "Legal profiles of connected data management emergency ".

Conclusions

The *contact tracing* o contact tracking is one of the public health actions used for the prevention of the spread of some infectious diseases and represents an element important within a sustainable post-emergency strategy. Its effectiveness has been well documented during the 2009 influenza pandemic containment phase [3]. In years more recently, this method was a valuable tool: in 2014, later on the import of Ebola virus disease into the United Kingdom [4] and in 2018 in the case of monkeypox [5]. The main advantages of *contact tracing* are that it can identify individuals potentially infected before symptoms emerge [1] and, if conducted in a manner fast enough, can prevent subsequent transmission from secondary cases.

Based on recent estimates for the COVID-19 transmission, empirical research [6] shows that in order to trace at least 80% of the contacts of the detected infections, it is necessary to predict a very high logistical burden, with an average of 36.1 individuals (95 percentiles: 0-182) traces for each case of contagion. If the definition of contact is made wider, it is possible reduce this burden, but with a corresponding increase in the risk of untraced cases; the researchers estimate that, for any definition of close contact one wants to adopt, one procedure

contact tracing manual that takes more than 4 hours of research is probably intended to generate an uncontrolled spread of the infection. The standards of *contact tracing* manual provided by the European Center for Disease Prevention and Control (ECDC) in

5 Guidelines for modeling threats and identifying mitigation actions compliant with the principles of secure / privacy by design:
https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

March 2020 relative to the COVID-19 epidemic indicate however in 12 hours - with the use of 3 resources of specialized personnel - the average time for each operation of *contact tracing ,* with a success rate, however, insufficient to identify all contacts or however to reduce the number of infected secondary contacts not identified and isolated below unity (and therefore to stop epidemic reproduction).

The use of technology in the field of *contact tracing* looks promising and able to give a relevant contribution for a much more efficient and rapid proximity tracking than that traditional. Technology for the *contact tracing* however, it must be approached in a way very responsible and in line with the fundamental rights and freedoms of citizens. A process of selection towards a technical solution that makes possible the *contact tracing* through *smartphone* but without tracking people and / or accessing sensitive data and information personal (for example who they are and where they have been), was recently launched at European level by a consortium involving excellence in scientific and technological research in Europe in order to trace only the short-range proximity relationships that make up a risk of exposure and which correspond to potential transmission chains of the virus.

The pan-European solution is based on three basic principles, in particular: 1) it is the result of a well documented analysis of international benchmarks and a strong spirit of cooperation European; 2) the technology is studied and selected to be applicable on a level international, i.e. interoperable across national borders; 3) the technology is privacy-preserving and therefore compliant with the general data protection regulation (GDPR). So the technology behind the European solution is a contribution important to allow tracking of proximity, even in cross-border mode, respecting privacy, according to a scalable and open model that can be used by any country.

Aligning with these principles, this subgroup of work dedicated to the study of technologies for emergency management in Italy, it carried out a methodological process with rigorous methodology selection and evaluation of technological proposals, detected with a three-day fast-call from 24 to 26 March us The examination of the solutions has been articulated on three consecutive levels which, starting from a general screening of all the proposals, it allowed - after characterization analytical and technical and organizational interviews - to identify two suns technological solutions, considered theoretically valid to be tested for the purpose of implementation in the current emergency situation. These are in particular Immuni e CovidApp.

The mechanisms and technical standards declared were found to be consistent with the objectives of exploit the possibilities and characteristics of digital technology to maximize the speed and real-time response to the pandemic. In addition, they are results

adhering to the European model and oriented towards full compliance with European laws and principles privacy and personal data protection. In particular, these two solutions technology considered, based on the analysis carried out by the work group, best to be able to advance to a field test phase to be carried out in parallel on both, they seem to be reliable and adequate technologies for proximity tracking, for a safe one data anonymization, to create a contact between the user of the technology and the figures reference healthcare, to interact with digital data exchange interfaces (API).

It should be noted that for both Immuni and CovidApp solutions it will be necessary to carry out customization and adaptation activities to make them compatible with the scenarios which will be defined. The Immuni solution uses the technology developed by the European Project Consortium PEPP-PT, thus promising greater guarantees of interoperability and anonymization of personal data. This solution also appears to be ad a more advanced stage of development of the CovidApp solution.

In order to be able to adopt the most effective technological solution for the *contact tracing* which important component of the set of measures that must be put in place for the emergency and post-emergency situation management, a particular importance is a careful though fast process of validation and commissioning of the solution chosen technology, which guarantees the achievement of the objectives set. For this reason, the implementation process should include testing the two in parallel technological solutions identified: Immune, as a solution that appears at the outcome of this first more appropriate evaluation and CovidApp, as a good alternative solution and / or of reserve.

This prudential approach serves in fact to have the guarantee of being able to dispose of at least a solution to be implemented, even when it occurs, in an experiment concrete, the failure for any reason of functionality and / or performance levels other alternative option required. The testing phase obviously includes both the verification of the security on the entire source code (by the *intelligence)* is the verification of field operation to be carried out in several limited areas of the territory. It will be in in any case, regardless of the technological solution that also to the verification tests should to be preferred and more reliable, than a dynamic process in evolution that improves a first technological version will pass to more advanced and performing versions from the point of view technical and practical use. Therefore, great importance assumes to this about agile development planning that involves a series of releases staggered in time of using technology.

The proposition of the technological solution for the *contact-tracing* that will come out on test, before being implemented in the field, it should finally be brought into a picture

strategic-organizational framework for the political decision maker, who, to control the transmission of infections, should take into account not only other measures of prevention (for example social distancing for particular population groups fragile) in addition to those based on technological solutions for the *contact tracing* but also general action strategies. This strategy allows an efficient application preventive actions also towards some segments of the Italian high risk population like the elderly and healthcare workers. In the scenarios studied, it is evident that the use of contact tracing technology has the greatest effectiveness before the end of the period lockdown, when the isolation measures allowed the rate to be reduced as much as possible of basic reproduction of the infection.

Decisions requested from public authorities

Decisions requested from public authorities

To put the system into operation *contact tracing ,* the public decision maker should:

TO. **Appoint a Program Manager** with full decision-making power over the project of public authority, to the end of guarantee protection e timeliness in the implementation and governance of technological processes.

B. **Choose from the main technical-organizational options** that impact on issues key to public health and privacy protection. A decision is therefore requested immediate and explicit on each of the following points:

1. *Policy for contact tracing technologies.* The systems of *tracing* and the proposals selected can make use of contact detection tools that have different levels of expected impact on the effectiveness of health interventions publishes and on the processing of personal data. The proposed options are:

   to) **Only technologies of proximity without geolocation (Bluetooth-LE)** as per European model proposed by PEPP-PT (Pan-European Privacy Preserving Proximity Tracing). Advantages : better data protection thanks to unique identification codes which mark the installations of applications, returns sufficiently anonymous, in adherence to the PEPP-PT model. Disadvantages : less coverage of situations with low presence of enabled devices, failure to indicate places of possible environmental contamination to sanitize.

   b) **Bluetooth-LE + GPS and / or other technologies that allow the geolocation (** only of the single points of potential contagion, not personal paths, with data encryption and behind *opt-in* informed). Advantages : greater coverage than the base of

smartphones popular in Italy and Europe, greater potential for the identification of places to sanitize. Disadvantages : use of information related to personal data (position of the *device).*

2. *Policy to be applied for alert following contagion .* In the event that a citizen with an app tested positive, you can activate two different alert procedures:

to. **Manual and voluntary procedure:** (as per model PEPP-PT) this option requires explicit authorization and technical action by the citizen (photo of a QR code or entry of a code released by the health authority in case of a positive virus test) so that your history of anonymized contacts is transmitted to server and then allow the process to start warning. Advantages : contact data only reside on *device* of the subject.

Disadvantages : greater risk of malfunctions in the sending procedure, as well as spontaneous non-fulfillment and / or temporal delay in the fulfillment by the citizen, with the effect of reducing the effectiveness of *contact tracing .*

b. **Automatic pre-authorized procedure:** the second option is that the list of anonymized contacts is available to the authority health, with pre-authorization granted by the citizen at the moment the installation of the app; Advantages : maximum timeliness and effectiveness of the contact alert process. Disadvantages : the data of the contacts they reside on public authority servers, with risks characteristic of the centralization of a database, mitigated with appropriate technological solutions.

3. *Policy to be applied to ensure enforcement of character actions consequent healthcare .* Following the detection of a positive case e of the alert of the subjects with which it came into contact, they must follow sanitary actions (e.g. quarantine and / or self-isolation for the subjects who came into contact with the positive case), which may be undertaken based on the following options:

to. **Voluntary procedure** : this option requires contacts exposed to risk of contagion remain unidentified (therefore unknown) to the health authorities) and that they therefore subject themselves spontaneously to the containment measures indicated in warning message sent to them *device .*

Advantages : greatest protection of personal data, even after a possible alert on the risk of contagion. Disadvantages : greater risks of non-adhesion and / or of time delay in adherence to containment measures by

of alerted contact, with the effect of reducing the effectiveness of the *contact tracing* .

b. **Proactive procedure** : this option provides (as per current practice *contact tracing* manual on WHO / ECDC guidelines) that the health authority requests and obtains nominal identification from part of the recipients of the alert messages following contact with positive patients occurred, providing for appropriate penalties for any defaults.

Advantages : maximum timeliness and effectiveness of actions to contain contacts exposed to potential transmission of the infection, better *compliance* waiting. Disadvantages : app data collection, a priori and regardless of the process *contact tracing* , necessity of appropriate communication e citizen involvement.

Bibliography

1. Abbott S, Hellewell J, Munday J et al., *Temporal variation in transmission during the COVID-19 outbreak* . Center for Mathematical Modeling of Infectious Disease, 2020, https://cmmid.github.io/topics/covid19/current-patterns-transmission/global-time-vary ing-transmission.html

2. Ferretti L, Wymant C, Kendall M et al, *Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing,* 2020, doi: https://doi.org/10.1101/2020.03.08.20032946 , available at: https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes /

3. McLean E, Pebody RG, Campbell C, Chamberland M, Hawkins C, Nguyen-Van-Tam JS, Oliver I, Smith GE, Ihekweazu C, Bracebridge S, Maguire H, Harris R, Kafatos G, White PJ, Wynne- Evans E, Green J, Myers R, Underwood A, Dallman T, Wreghitt T, Zambon M, Ellis J, Phin N, Smyth B, McMenamin J, Watson JM. *Pandemic (H1N1) 2009 influenza in the UK: clinical and epidemiological findings from the first few hundred (FF100) cases* . Epidemiol Infect. 2010; 138: 1531-41

4. Crook P, Smith-Palmer A, Maguire H, McCarthy N, Kirkbride H, Court B, Kanagarajah S, Turbitt D, Ahmed S, Cosford P, Oliver I. *Lack of Secondary Transmission of Ebola Virus from Healthcare Worker to 238 Contacts ,* United Kingdom, December 2014. Emerg Infect Dis. 2017; 23: 2081-2084

5. Vaughan A, Aarons E, Astbury J, Balasegaram S, Beadsworth M, Beck CR, Chand M, O'Connor C, Dunning J, Ghebrehewet S, Harper N, Howlett-Shipley R, Ihekweazu C, Jacobs M, Kaindama L, Katwa P, Khoo S, Lamb L, Mawdsley S, Morgan D, Palmer R, Phin N, Russell K, Said B, Simpson A, Vivancos R, Wade M, Walsh A, Wilburn J. *Two cases of monkeypox imported to the United Kingdom ,* september 2018. Euro Surveill. 2018; 23

6. Matt J Keeling et al., *The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19) ,* medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036