• Fabio Saragoni
• Marco Tordelli

Data Privacy and Personal Freedom:
How are they influenced by technology in the Pandemic situation?

Abstract

Among the topics that most shook the public debate in the last months of pandemic, the control of movements of people and collection of private data related to our daily activities are today the most controversial and unclear for many of us. If different considerations have been done to evaluate impacts caused by national legal frameworks in facing the initial phase of SarS-CoV2 pandemic [1], there is a lot to explore on the long term technology measures adopted to gather everyone's personal data for safeguarding Public Health at the expense of data privacy and personal freedom.
In this paper we will browse the main track and tracing technologies adopted to limit the spread of SarS-CoV2 in the world, we will attempt to define a data privacy sensibility index to classify the mobile apps in use of three different countries (USA, Italy and China) and analyze, through the opinion of an expert in the field, the Italian case of the app Immuni in the legal framework of European GDPR.

Introduction

Among the digital health technologies implemented in these months to tackle COVID-19 pandemic, the ones used for contact tracing and tracking have been subject of intense debate mostly for privacy concerns.
In fact, on one side all these technologies aim to rapidly identify potentially newly infected persons who may have come into contact with existing cases, to limit further transmission [2], on the other there are differences regarding their sensibility to data privacy.

There are 3 technological approaches on which most of the track and tracing mobile apps rely on, and these are based on:

- Network operators' ability to locate communication devices on cellular networks (capability that is implicit in mobile radio technology) even without the full awareness of users, thus being able to make assumptions about any proximity situations between mobile terminals;

- Smartphone's ability to autonomously determine their position (receivers of the signals emitted by global localization systems) and to communicate it to a service centre capable of collecting positioning data and processing them in order to identify any situations of proximity between the devices;

- Proximity tracing using smartphones capacity to autonomously detect the presence of other devices nearby by receiving identification signals (radio beacons) spread with Bluetooth Low Energy (BLE) technology.

Following the guidelines issued by the European Commission [3] and WHO [4], we first identified five common principles for creating a solid application from the point of view of data privacy. Subsequently, compliance with these principles was used to classify the data privacy sensibility of three applications build in three different countries (USA, Italy and China) according to the following:

Principles	Description
Voluntariness	The download and use of the application is not mandatory.
Data utilization	Data used for a predefined scope strictly related to Public Health safeguard. Sale or reuse of those data shall be strictly prohibited.
Data retention	Data retention shall be limited to the period of the pandemic response, except for the purposes of research or epidemic planning. Timelines should be based on medical relevance. Proximity data should be stored on user's device, deleted after one month or in case of negative test results, and uploaded on the server only by choice.
Data minimization	Data processing shall be limited to the minimum necessary amount of data needed to achieve the public health objective and must be limited in scope. The data must in any case be processed anonymously and in aggregated form.
Transparency	Data collection and processing shall be transparent, and individuals shall be provided with concise and reader-friendly information in clear and unambiguous language regarding the purpose of collection. There should be full transparency about how the applications operate even in case where automated decision-making models are adopted and error margins.

Table 1: Common principles for creating a contact tracing mobile application in COVID-19 pandemic

One single point was assigned for each principle met by the mobile applications and then classified as per the following tables:

DPS (Data Privacy Sensibility)	Conditions
HIGH	≥ 4 points – the application fully complies to all or most of the five principles
MEDIUM	2-3 points – the application partially complies to some of the five principles
LOW	≤ 1 points - the application support minimally or none of the five principles

Table 2: Data Privacy Sensibility Index

Country	App Name	Technology	Data Privacy Sensibility	Notes
Italy	Immuni	BLE	4	Minor technical risks were evaluated in the data anonymization process
USA (Utah)	Healthy Together	BLE, GPS	3	Geolocation was considered as an excess to the data minimization principle. Data retention period does not mention data erasing in negative test cases.
China	Chinese Health Code System	GPS, Data Mining	1	Mandatory nature of the system makes the principle of voluntariness fall. Geolocation, Data mining and other data processing (e.g. medical records and travel history registered on the assigned QR code) were considered as an excess to the data minimization and transparency principles. [5]; [6]

Table 3: Classification and Comparison of some examples of apps based on different technologies

The Expert's perspective

The expert is Alessandro Di Fazio, graduated in Computer Sciences at the University of Pisa, class '61. In his free time, he loves getting his hands dirty with grease from vintage cars and motorcycles. He grew up as a consultant of integrative solutions in the field of Telecommunications at Hewlett-Packard (HP), Director of information systems at AIFA (Italian Medicines Agency), project manager and promoter of GDPR Compliance, Data Privacy and Cybersecurity services at DOTS until February 2019. Now he works as Data Protection Officer at Tinexta SpA.

What is Tinexta?

Tinexta S.p.A. listed on the STAR segment of the Italian Stock Exchange is a holding. Leader in Italy in its three main operational areas (Digital Trust, Credit Information and Management, Innovation and Marketing Services) Tinexta Group counts about 1300 employees.

Interview

Data Privacy, GDPR and Personal Freedom.

Marco:
There have been numerous measures regarding the protection of personal data necessary to remedy the situation generated by the spread of Sars-Cov-2.

1. **In which areas the existing regulatory framework had most to do to readjust?**

Alessandro:
The question is complex and with strong legal value. In general, rather than readjusting, it has been necessary to reinterpret. In Europe, the regulatory framework within which we must move is the GDPR. All the actors involved have interpreted the laws already defined within this regulatory context under the authority guidelines. Different regulatory entities have disseminated the communications and FAQs which affected many operational areas. First of all was **the health sector**, for which a series of emergency measures went to define the limits and purposes of the involved personal data processing. Another area was the one of local authorities (Regions, Municipalities and Police). The intervention in the field of labor law was decidedly more substantial. In particular, the definition of the new active role of the employer in the management of the so-called "contagion event" for which it is required to know some information about the pathology. Moreover, other areas were interested by the definition of the "new" behavior of teachers and operators at testing centers, such as school, clinical trials. Finally the technology sector with the intervention on "contact tracing".

Marco:

2. **Therefore, is it correct to say that there has not been any kind of relaxation of the existing regulatory constraints occurs?**

Alessandro:
Interpretations have been given rather than relaxation of constraints. There are generally two approaches in the area of treatment safety: "Is everything that is not forbidden lawful or only what is explicitly defined as lawful is lawful"? To define these clarifications and interpretations we can say that this second approach has been privileged.

Marco:

3. **It is clear that the principle is to safeguard the public interest, however, many fear the restrictions of their personal freedom. What are the principles that should guide the processing of our data in these times?**

Alessandro:

There are two principles. **The first,** in the processing of personal data, is the one of **relevance and not excess.** This means that it is necessary to minimize the data processing to what is necessary for the achievement of predefined purpose. In particular, the principle of non-excess also moves along the time axis. Thus, when we hear that certain data will be used for pandemic purposes for the duration of the health emergency, this is in fact a risk. **The second principle** concerns the **security of data processing** which is based on three axes: **integrity** which means that the data must be correct throughout its life cycle, **availability** which means that the data must not be lost and finally **confidentiality** which means that the data is made available only to authorized persons and not to third parties. This means that when we think about state of emergency the Data Processor must be able to comply even in the management of what in fact is a sort of metadata on the personal data that is the *treatment expiry date*. That may not be an easy requirement to implement. It is not by chance that it is one of the points of greatest attention.

Marco:

4. **What are the technological and organizational requirements that governments and private companies can put in place to maintain operational flexibility and, at the same time, ensure compliance with the various legal requirements?**

Alessandro:

The **Data Integrity** that already applies in the pharmaceutical field is a unique reference model in terms of data management at a technological and organizational level. It typically refers to metadata or to the attribution of responsibility for data management. Applying Data Integrity in the world of privacy clearly determines a strong push towards the digitization and therefore dematerialization of data. This is a first fundamental technological requirement. Another aspect that is common to Data Integrity and the GDPR is the **Accountability.** This aspect require that I must be able to understand who has processed a certain data. Thus, that there are data processing personnel who are identifiable, traceable and who have training suited to their role. Do we want to call it “segregation of duty”?

Marco:

5. **In many cases, companies have found themselves playing a new role in managing the health data of their staff. As Tinexta's DPO, what were the applied countermeasures?**

Alessandro:

As Tinexta is a holding, what we did was to provide the control and compliance guidelines to all subsidiaries. As DPO of many of Tinexta's companies, I created a specialized Task Force that puts together the standards for all the companies in the group:

- First of all, we defined a DPIA model (Data Protection Impact Assessment). It is a process that is implemented in advance of the processing of personal data, in case of high risk treatment. This was applied to all Tinexta's employees.
- Another area of intervention was the common definition of parameterizable organizational measures. In practice, it was a question of creating common work instructions for the processors taking into account the diversity between the various companies in the group, thus taking into account local legislative peculiarities. That was complex.

- Finally, I was involved in the creation of a technological solution, through a company of the group, called DizMe based on Blockchain. The solution guarantees the secure management of company data precisely because it is based on a strong pseudonymisation mechanism.

Marco:

6. **In the USA, Google and other digital giants are promoting the definition of a new legal framework for the management of personal data and the European GDPR has been taken as a model. Is the GDPR actually a solid model that is guaranteeing, even in the current situation, greater protection? What are the critical points?**

Alessandro:

The GDPR is certainly an excellent regulation and as such tries to find the balance between the freedom of the data subject and the circulation of personal data as the lifeblood of organizations and markets. A clear example is the right to the Data Portability defined by GDPR. Let's pretend that I want a better energy offer that is more suited to my consumption profiles, I request this profile from the supplier company and submit it to another company to obtain one that is more advantageous for me. This example clarifies the concept: the privacy risk is a risk on the personal freedom of the interested parties, in the absence of such, a series of conditions for coexistence fall apart. A critical point of the GDPR is integration in an international context. The European Court of Justice recently canceled the Privacy Shield. This is an agreement made between the European Commission and the American government which recognized the privacy guarantee systems between the two states as comparable, equivalent. In practice, it was lawful to process the data of European citizens in the United States. This has now been canceled with a disruptive impact in all areas of the pharmaceutical sector but also that of the digital and consumer sectors, for example in the outsourcing of large data center providers.

Marco:

7. **Among the measures taken to contain the spread of the virus, those relating to the monitoring and tracing of individuals have aroused greater interest. What are the ways that we have at our disposal to monitor the return to normal or rather, to the "New Normal" in the long term?**

Alessandro:

Speaking of ways to monitor the return to normal, we are basically talking about indicators. The indicators are healthcare, social and economic ones and are managed at the institutional level. Regarding tracking, this is a processing of personal data. Geolocation, social footprints are metadata that have been around for a long time. What emerges today from this pandemic situation is perhaps a greater awareness of the importance and risk associated with the tracking and use of personal data. In particular, to the secondary use of these tracking data. If for a tracking app, such as Immuni, the tracking itself has a clear purpose, that is the containment of the virus, in other instances where the security principle is weak, the data management could become illegal or even dangerous for personal freedom. Thinking of a "New Normal" scenario in which the tracking will certainly continue, I see greater awareness and consequently also on the part of all the Privacy actors a need for greater transparency and security of treatments. In a future context, I expect more awareness in the best use of informed consent by those who ask for it. Another aspect of the New Normal scenario will be the implementation of the data retention policy and therefore a technological capacity to be able to manage consent and data retention in an appropriate manner. Awareness and consent management will have to be revised, in this sense the harmonization of international laws is important.

Technologies, use and storage of data

Fabio:
Digital tracking and tracing technologies have been identified as a powerful tool to support the traditional way of contact tracing to limit the spread of COVID-19. However, these technologies raise several privacy concerns. The approaches to tracking can be different, varying from more invasive methods (i.e. GPS) to less invasive and more widely used approaches (Bluetooth) technology, such as in Italy for the Immuni App.

1. **Can you explain us which are the differences between the available mobile track and tracing technologies and what led to prefer the use of Bluetooth technology over the others?**

Alessandro:
The macro difference is that with a Bluetooth technology we have the tracking of the contact that took place but we don't know where this happened. Where it happened allows us to better qualify the contact (i.e in a public place). It is clear that the two technologies based on cellular networks or on geo-localized geographical positioning are certainly those that give the greatest wealth of information.
The choice of BLE technology is common to many countries, certainly all of the European Union countries. As assessed by the Italian Data Protection Authority, while in some regions far from the European Union and its personal data protection standards (GDPR, Ed.) the other categories have been taken into consideration, we have chosen the BLE for the implementation of these mobile tracing platforms. The reason is essentially that it somewhat respects the GDPR principle of minimizing the data collected in order to identify possible contacts with infected people. From a data minimization point of view, it was considered more important to trace the contact than the place where this occurred. This was the fundamental reason for choosing BLE technology.

Fabio:

2. **Could it be a disadvantage to only trace occurred contacts without being able to locate them?**

Alessandro:
The effectiveness of these digital tracing systems is essentially based on the number of people who use them. The real factor of effectiveness is their diffusion. It is clear that rich information from a geolocation point of view allows advantages, but the real effectiveness is given by its diffusion. Currently the Immuni app has not reached a very wide diffusion yet, but it is not only the Italian case. I would link the effectiveness of the tracing system app to its widespread utilisation, rather than to the technological choice.

Fabio:

3. **Could you explain better how the Immuni app works?**

Alessandro:
In a nutshell, the Immuni system is composed of a Client part which is the one related to the mobile App and a Server component which has different functions, especially the part focused on managing information related to security and transactions on infections. The purpose of this system is to provide users with an alerting tool related to exposure to the contagion. It is a system that can be used in a participatory way and it ensures that the interconnected devices are able to mutually detect each other and allowing users to qualify as Covid-19 positive through a voluntary procedure assisted by a health worker. The app itself can then present a message on users' devices that warns of the detected proximity to a device belonging to a person who has declared being positive to Sars-Cov-2, thus making the person receiving the message assume a qualification of "close contact" of a positive subject, informing him of the necessary measures to be taken. This is how the system works in principle, so it is an alerting system based on an absolutely voluntary participatory model.

There is an additional part related to secondary data treatment regarding the backend (server) component. These data can be used for public health purposes (scientific research, statistics) to improve risk assessment models and also to improve the accuracy of algorithms.

Our temporary and random codes (RPI, Rolling Proximity Identifiers) and those we have exchanged with people we have been in contact with remain on our smartphone for 14 days and are then deleted. Only when an individual who tested positive for Sars-Cov-2 decides to give consent to the use of the data collected by the app, this data is shared with the system's central server.

Fabio:

4. **Have you possibly found any weakness in terms of data processing after sharing them?**

Alessandro:
In general, the security problems of this management are mainly in the client part, even before they reach the server side and depend on the technology used, because Bluetooth technology can be violated. An example is the so-called "paparazzi attack". The “paparazzi attack” evokes the figure of the “paparazzo”, therefore a cyber-criminal who lurks near some known public points (e.g. airports, entrances to some areas where some public people are known to pass, just like a paparazzo does). Once the interesting individual passes by from a data theft standpoint, this cyber-criminal intercepts such information. Speaking of the Immuni app, we know that there is a continuous dialogue between the app and the service centre, in which the cyber-criminal can intercept a pseudonymous code and therefore, from that moment on, he knows that the pseudonym can be associated with that individual. This technique exploits the vulnerability of Bluetooth technology, precisely because the technology broadcasts to all devices and, in the specific case of the “sniffer”, to the cyber-criminal device.
The Italian Data Protection Authority identified all these risks, for example in its "Data Privacy Impact Assessment" document. On the client side there is, for example, another vulnerability of the smartphone itself that could be infected by apps that are actually malware able to capture certain information. All these threats were assessed by the Italian Data Protection Authority who approved the Immuni app in June, providing prescriptions that take into account the risks, but also any excesses of unauthorized processing on the System’s Server side. It has expressly provided for, requested and imposed on service providers, for example, some countermeasures concerning the data retention time, the guarantee on their effective deletion with automatic mechanisms as per data retention policy, and provided that the roles of system administrators are particularly monitored and requested the minimization of some administrative information collected because must be noted that, for example, the IP addresses that are still part of this treatment (or could be part of it) are still attractive for other forms of cybercrime. So there is not only the health data we are talking about, there is the so-called "trawling”.

Fabio:

5. **Could you give us examples of potential fraudulent use of this data, of these IP addresses for other purposes than to have access to health data?**

Alessandro:
In general, they refer to all personal data information that can be associated, for example, to the same smartphone. We know that the smartphone is the access point to a plethora of services. On the smartphone there are digital signature functions, access to banking systems, flight booking systems, not to mention the sensors provided inside the smartphone. It is a bit like entering with a Trojan horse: you enter into the smartphone and from there you can see anything. Of course, in my experience as a DPO, so far I have been able to verify that these attacks by cyber-criminals do not always have a utilitarian purpose, they often are part of demonstrative actions (for example the publication of the confidential phone numbers of parliamentarians). Clearly this is a serious breach of personal data, but it is not immediately for profit or

attributable to a utilitarian action, it has a demonstrative purpose. These could be some of the side effects of a possible intrusion through this system.

Fabio:

6. **Summarizing, then, do you see major privacy related weaknesses of the technology at the app (client) level than at the server level?**

Alessandro:
Yes, most of the risks are concentrated at the client level because, for example, considering malware that can be present on a personal smartphone, these are very difficult to detect centrally. There is no control as instead happens on corporate smartphones where there is greater control (e.g. you cannot install some kind of apps, etc...).

Conclusions

The world is facing a serious health crisis that requires strong responses, the impact of which will manifest itself beyond the end of this emergency. It is clear that positioning of technology may play a key role in a pandemic scenario but great attention must be paid by governments in adopting surveillance means that can became detrimental in terms of data privacy. In fact, if on one side the usage of technology can greatly support the fight against COVID-19 spared with extreme efficacy, on the other hand, it can jeopardize rights such as data privacy and personal freedom.

In this terms, the promotion of common guidelines and robust regulatory frameworks is paramount to define, at an international level, a use of technology which is commensurate to the real risks and that take into account the balance between two fundamental rights such as health and personal freedom.

In conclusion, extraordinary measures taken to combat the spread of SarS-CoV2 may be justified by interests in safeguarding the Public Health only where the usage of personal data is time limited, minimized and continuously monitored.

Key Notes:

- Data Protection Officer (https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en)
- Data Minimisation (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504)
- GDPR (https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati)

Bibliography:

[1] Pucci T., Hodovsky J. What did WHO, EC and each country have in terms of a legal framework already in place to combat the virus?. (3 August 2020); https://www.pqegroup.com/blog/2020/08/what-did-who-ec-and-each-country-have-in-terms-of-a-legal-framework-already-in-place-to-combat-the-virus/

[2] Ferretti L., Wymant C., Kendall M., Zhao L., Nurtay A., Abeler-Dörner L., Parker M., Bonsall D., Fraser C.; Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. SCIENCE, 08 MAY 2020

[3] European Commission – Communication from the Commission “Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection” Brussels, 16.4.2020 C(2020) 2523 final https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf

[4] World Health Organization (WHO) – Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance, 28 May 2020 https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf?sequence=1&isAllowed=y

[5] Mozur, P., Zhong, R. & Krolik, A. In coronavirus fight, China gives citizens a color code, with red flags. *The New York Times* (1 March 2020); https://go.nature.com/2yfrKLI

[6] Yang, Y., Liu, N., Wong, S.-L. & Liu, Q. China, coronavirus and surveillance: the messy reality of personal data. Financial Times (2 April 2020); https://go.nature.com/3cfvvzG