UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE, LAW, AND INTERNATIONAL STUDIES

Master's Degree in
Human Rights and Multi-level Governance

The use of Digital Health Technology during the COVID-19 Pandemic and its impact in Human Rights and Data Privacy Rights

Supervisor: Prof. PAOLO DE STEFANI

Candidate: JULIANNE FREIRE DE SOUZA
matriculation No. 1167319

A:Y 2020/2021

Acknowledgments

Many many thanks to everyone who supported me during my journey and contributed to my personal and professional growth during the course of this Master's Degree.
Most sincere thanks to the Professor De Stefani, for his expertise and guidance during the writing of this thesis and for being very helpful during the hardships of the year 2020, always showing great understanding and humanity during his supervision.
Thanks to the University of Padova that welcomes foreigner students, and that also opened doors to me that I could never thought of stepping in: to the University of Zürich, to the Swiss Federal Institute of Technology and to the United Nations.
This achievement goes to my family that supported me during this time abroad, even without never had seen anything else than Brazil, but still, encouraged me to give my best, and despite the concerns, continuously believe I am following a great path.
To all my loved ones that supported me and helped me to overcome the difficulties during my staying in Italy and Switzerland. And finally, to the ones we lost for the pandemic. My dear brother, you live in our hearts.

Summary

Abstract

This Master's Thesis investigates the use of digital data health during the pandemic of the COVID-19 and its effects on privacy rights from a human rights perspective. It investigates the cases of Italy, Switzerland, and China, as examples of how countries are handling data processing and how the legal framework is designed. It is presented the risk assessment for each country, additionally with a general risk assessment and recommendation for implementing fair policies to prevent the misuse of data or the permanent implementation of intrusive technology; it is argued that based on the law and principles of proportionality, transparency, and time-bonding can lead to the effective and ethical use of the technology, preventing the increase of the digital divide, plus engaging with international cooperation is stressed as a key to building a sustainable growth of digital health without harmful intervention in the private sphere.

Keywords: Human Rights --- Big Data and Mass Surveillance --- Legal Framework --- COVID-19 --- Digital Data Health – Data Privacy Rights – contact-tracing apps - GDPR

Introduction

This Master's Thesis intends to discuss the current use of Digital Health Technology and its effects on Privacy Rights from a Human Rights perspective, using the examples of Italy, Switzerland and China and how these countries are handling the data processing and which effects it has been in privacy rights.

The advance of the technology has shown us the need for an updated legal framework that can take into consideration all the changes that are occurring in society, predicting scenarios and adapting to the current situation, to guarantee an ethical use of the health data processing and more transparency in its procedure, plus safeguard Privacy Rights as a Fundamental Human Right.

Smart Technology has changed our behavior and our lives throughout the years by the use of smartphones, laptops, smartwatches, and many other tools that help with developing our society into a more automated and time-saving social structure. Clearly we are most well adapted to the innovations, however, in some parts of the world, there are still people struggling with achieving their basic needs given to different factors, like wars, hunger, natural disasters, and political practices, for example. As society evolves together with technology, we face the challenge to indicate policies and regulations that can keep our privacy rights protected, ensuring that the Rule of Law and individual freedoms are provided and citizens can benefit from it to maintain a Democratic State.

How society will develop with the uninterrupted advance of technology has been studied by many scholars from different backgrounds, nevertheless, an intersection of subjects is somewhat needed. This dissertation will try to explain the main points in how data health has been collected during public emergencies, how the states are addressing this issue from a legal perspective, and what it could be implemented to guarantee Privacy Rights as a Human Right. As both subjects are pretty much technical fields that require very specific knowledge and finding professionals that can understand both

areas are still one of the many challenges surrounding the discussion, contribute to make the dissertation more challenging, therefore it will be more focused on the legal and human rights perspective as its is a crucial discussion at the moment.

In our daily lives, technology is already well incorporated and how it will develop during the next years should not be a reason of fear, but instead, it should be a call for discussion and protection to create a safe environment, specially given to the fact that the use of machine learning are crossing basically all spheres of studies. Artificial Intelligence, as for instance, Machine Learning, Natural Language Processing(NLP), Deep Enforcement Learning, allow programmers to develop a diverse range of software and apps that can be used for daily basic activities and more complex activities, as medical interventions, self-driven cars among other infinite possibilities. This open doors to new situations and should be regulated to prevent the misuse of personal data, no matter what the purpose of the technology is.

How Human Rights are affected by the use of Digital Health is an urgent topic to be discussed. It obviously has positive and negative sides and can even create new spheres of Human Rights that will appear in a near future. Human Rights are rights inherent to every human being and through out International Conventions and Treaties, they are provided to people, and they require laws at the national and international level, in order to be enforced and implemented. For example, at the international level, the Universal Declaration of Human Rights[1] where basic human rights are stated, representing obligations for the states parties, will be cited as the core document in International Human Rights Law in this Master's Thesis, together with other international conventions, guidelines, domestic laws and treaties that cover the current framework in International Human Rights protection, regarding Data Privacy Rights and public emergencies.

It will be discussed the implementation of digital data health in Italy, Switzerland and China, discussing also their legal framework to provide a risk assessment to likely

1 Available at https://www.un.org/en/universal-declaration-human-rights/ Accessed on 01/11/2020.

gaps or data privacy violations. Also, The GDPR will be analyzed as it represents the European Union framework and is leading European countries to lawful use of data.

A complex discussion about how the States and private companies are using the data of their users and citizens, and how mass surveillance has increased in certain countries, it is a very important issue and must be fueled to enable the society to find a solution for protecting our private life and helping to build back better. The global Pandemic we are currently facing has shown us how some states are using digital health and tracing people's location to contain the spread of the virus, with minimum harm to the citizens and the economy. However, even with all the efforts and the already existent legal framework, the lack of transparency and the lack of regulation represents a blind point in our international community that needs to be discussed, and the implementation of fair policies needs to be promoted to safeguard data privacy as a fundamental human right and advance with the use of the digital health.

1. International Human Rights Law and Data Privacy

1.1 Historical Background of International Human Rights Law

Human Rights Law plays a big role in nowadays international policies and it has been developing along the years, providing guidance on good practices and protection to citizens at national and international levels. Explaining the origins of international human rights is essential to build up the discussion of this master's thesis and illustrate how the legal framework was formulated trough out the years to point solid arguments and analyze the theoretical question of this thesis.

There are diverse theories trying to explain its origins, however, the origins of human rights law are disputed. Some argue it was based on philosophical discourse, together with the "rights" speech, while some others argue, it is part of the natural law which is also linked to the Rule of Law concept[2]. In other theories, the religion was the beginning of human rights law, as there were specific conduct codes that should be followed by society, which would explain how human rights law were created and should be followed as religious rules.

Liberty-based and rights-based theories are defended by the common law system and civil law system, respectively. These theories try to explain the relationship between the individuals and the state. The libertybased theories argue that the individual must be free from the state's interference in their lives, while the rights-based theories believe that we have inherent rights that must be respected and protected by the state[3].

With the scope to protect human rights , International Human Rights Law encourages and obliges countries to provide individual rights protection. Beyond the national law sphere, international human rights law has its its own enforcement mechanisms, set forth by international treaties that are signed by states that decided to be parties and comply fully with their content[4].

In an attempt to regulate the relation between states, international Law was had established diplomatic rules, whereas international human rights law goes beyond a

2 Smith, R. (2020).*International Human Rights Law*. Oxford University Press, USA.
3 Ibid note 2.
4 Ibid note 2

layer of diplomatic concerns and creates positive rights for nationals at an international level .

1.a) The UN Charter

International Human Rights Law could be simply conceptualized as a set of obligations that States would have towards their citizens and that would be implemented by an international body with the scope to promote and respect human rights in all countries, trough the use of rules, procedures and institutions[5].

The idea of having bills to protect human rights was somehow present in early discussions of the human thinking. However, after the attempts against minorities, as for example, what happened to the Jews, showed to the nations the necessity to enforce and implement the respect to human rights as inherent to every human being, regardless religion, social status, nationality, gender or race.

After the World War I, the creation of the League of Nations resulted in the establishments of diverse treaties and covenants, that for the first time not only protected the citizens at an international sphere, as those treaties were mostly written to protect minorities , but also created to states the obligation to apply the norms to all their own nationals[6]. The creation of the League of the Nations had the scope to protect the minorities of the former colonies with some countries as State Parties, however even with a mandate system and normative bills, it did not result yet in the international human rights law.

In the early discussions about the subject, the sovereignty of countries were not questioned until the second world war, when it started to be questioned if the treatment of citizens were solely a country's internal issue, as well as, the abolitionist movement, more and more international treaties were used as a protection layer against State's abuse and wars.

5 Bilder, R. (2010). An overview of international human rights law. *GUIDE TO INTERNATIONAL HUMAN RIGHTS PRACTICE, 4th Ed., Hurst Hannum, ed*, 3-18.
6 Buergenthal, T. (2006). The evolving international human rights system. *Am. J. Int'l L., 100*, 783.

Therefore, a milestone was the creation of the UN charter with the idea of promoting, regulating and implementing policies to protect human rights was widely discussed after the atrocities of the war. A step forward in the legal framework of international human rights, delivered to the people and to the world[7]. As described in the article 1 of the UN charter's: The Purposes of the United Nations are: To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace; To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace; To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and to be a center for harmonizing the actions of nations in the attainment of these common end[8].

Therefore, International Human Rights finally had an international bill with many countries' signatures, cooperating in promoting, enforcing and implementing Human rights. The holocaust and the Nazi ideology had compelled the world to focus on keeping the peace between nations and protecting minorities that were persecuted at the time. The bill was not only aimed at framing obligations, but also was meant to set up ways for implementing and enforcing the principles and rights enshrined in the charter.

After the UN charter, in 1948 during the General Assembly of the UN, a document was drafted with the scope to be the road map to implement the UN charter, signed by some world leaders to avoid and to not repeat the same mistakes that happened during the World War II. The Universal declaration of Human Rights opened doors to many political and legal discussions regarding the role the UN should play in

7 Ibid note 2.
8 Ibid note 1.

the enforcement of the covenants. As mentioned before Natural Law and Positive Law were in the main stage of the literature background during the drafting of the UN Charter.

The Universal Declaration of Human Rights faced different discussions mostly based on religious and political grounds. However, the Charter would describe the United Nations as an impartial organization with the scope to respond to individual complaints and alleged human rights violations. Following the Positive Law, the UN charter stated the protection to human rights as rights inherent to all human beings, as described in the Natural Law perspective, but even with the bill of rights, some nations, driven by political regimes, would not follow any of the recommendations the declaration would propose.[9]

2. The use of Digital Health Technology during the COVID-19 Pandemic

2. 1 Brief concept of the existent mobile apps for contact-tracing

The pandemic has risen many ethical questions regarding the responses given by the states to contain the virus and the long-term impacts they would have on society. The COVID-19 has shown us that is needed reliable leadership that can work together with the scientific community to find the right balance to solve the matter. Despite being a health public emergency, the consequences go beyond the social-economic layer and, if not examined carefully, could lead to the increase of the human rights crisis we are already dealing with.

In an attempt to contain the spread of the COVID-19, States, as a matter of urgence [10], engaged in using technologies to facilitate contact-tracing of people who were exposed to the virus. As the nations are emerging from strict lockdowns, and the economy needs to be back on track again, one of the many strategies used was to build

9 Kunz, J. (1949). The United Nations Declaration of Human Rights. *American Journal of International Law, 43*(2), 316-323. doi:10.2307/2193039

10 Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*.

an alliance of technologies to help with identifying infected individuals and enable health authorities to contact more rapidly those who were in close contact with them.

contact-tracing is not new, it has been used before in different pandemics, like Ebola, HIV pandemic, and consists in the process of identifying, assessing, and managing people who have been exposed to a disease, preventing the spread onward. In May 2020[11], the World Health Organization, published an interim guidance to contact-tracing during the COVID-19 pandemic, so governments were implicitly encouraged to go ahead with this strategy.

Apps are considered three days faster than conventional contact-tracing made by health authorities. This can be beneficial, as in many cases people often do not remember everyone they have met in the past days. The applications are used to deliver exposure notifications to the users. a technology was launched in April 2020 by Google and Apple. The Bluetooth technology will send a string of beacons[12] including a random Bluetooth identifier that changes every 10 or 20 minutes; when smartphones receive the beacons, they will securely store them on the device. Once a day, the system will download the beacons stored in the device, to match with the beacons of people who were tested as positive for COVID-19, and in case a match is found, the system notifies the user and give instructions on the next steps she has to take in connection with the exposure to the invection.[13]

What was mentioned above led countries to invest State's capital in the development of digital health apps. Digital Health apps help with the diagnostic; They can also be used to identify if someone is positive for the COVID-19 and how many people could have been exposed to the virus. Many types of digital health app were created around the world[14], but mostly were contact-tracing apps that can be downloaded on a voluntary basis and use the Bluetooth technology in mobile phones to

11 Available at https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19. Accessed on 02/10/2020.

12 Beacons are hardware transmitters that can identify nearby portable electronic devices. More explanations at : J. M. Bahi, A. Makhoul and A. Mostefaoui, "A Mobile Beacon Based Approach for Sensor Network Localization,"Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), White Plains, NY, 2007, pp. 44-44, doi: 10.1109/WIMOB.2007.4390838.

13 Available at https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf. Accessed on 18/01/2021.

14 Ibid note 16.

send anonymous identification codes with other devices that also have enabled the same app.

One of the main discussions about contact-tracing apps is that the technology is provided by private companies, Google and Apple[15]. Companies are responsible for developing the technological environment (the operating systems), but are not responsible for developing the apps. An ethical and practical question would be the reason why States are investing public capitals to be eventually used in technological infrastructues owned by private companies, and whether trusting Google and Apple that they would not monetize our personal health data is a wise choice.

Many aspects of the use of mobile apps to contact-tracing ought to be discussed and analyzed , as the use of these applications entails more surveillance from the government and more control over people's movement. Another interesting aspect would be the inclusiveness of using this tool, as there are many people without access to internet (not to consider access to even more basic rights like clean water or education). Creating a mechanism to fight the virus that requires a mobile phone and based on the necessary cooperation of only two private companies is not the best way of promoting inclusiveness[16].

Various concerns surrounding the apps are raising more awareness to the technological privacy issue and how governments should handle the situation and take into consideration the whole society without leaving certain categories of the society behind.

Obviously the use of Bluetooth in contact-tracing can be time saving tand really be helpful in strengthening the strategies to fight the virus. Problems arise however, on how these technologies are being delivered to the society and how the personal data are stored. Both should be in the center of the concerns the leaders.

Going back to presenting the apps that are current available for download, each country that decided to use this mechanism has developed apps from different sources.

15 Available at https://covid19.apple.com/contacttracing. Accessed on 18/01/2021.

16 Available at https://www.who.int/southeastasia/news/opinion-editorials/detail/together-forward-in-the-fight-against-covid-19. Accessed on 18/01/2021.

Most of them are using the services provided by Apple and Google as mentioned before. The use of new technologies for good, is not a harmful move, however the lack of appropriate data protection could represent a threat to the society in a long term.

Digital contact-tracing can be really helpful. It is more accurate than any manual methods of tracing individuals' contacts and mvements; it doe not require memory or contact lists; alerts can be instantaneous and the follow ups can be organised fast by the Government. [17]Several countries already started using contact-tracing apps, for example, Belgium, Brazil, Italy, Japan, Switzerland, Ireland, United Kingdom, and some states in the USA. [18]

The Bluetooth signal is used to verify if any other device with the app installed and enabled has been in proximity and for how long the contact has lasted. The main idea is to be able to identify only the individual that has been in contact with the person who was positive and inform the health authorities. This information is claimed to be held anonymously and voluntarily by the service providers.

For enabling a non-corrupted use of the apps, the legal framework needs to be updated to the current needs created by the pandemic, to protect Democracy and the Rule of Law in the states. However, the need to ensure basic services during a lockdown or while the pandemic lasts, should be taken as an opportunity to adapt the regulations for data privacy rights to the present problem and long term solutions.

2.3 Digital Data Health in Italy

Italy is one of the countries with highest numbers of Covid-19 infected people in Europe and with the highest mortality[19], especially in the region of Lombardy, in the north part of the country, where the cases during the first wave (February-April 2020) had exponential growth, leading the region to face a serious crisis in hospital facilities

17 https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf?m=1586179217

18 https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

19 https://www.bbc.com/news/world-europe-52594570 Accessed on 30/09/2020.

and other sectors – namely structures for the elderlies. As per 4 February 2021, Italy had 2.570, 608 cases in total, and 89.344 deceased.[20]

The lockdown measures in the country were very strict given to the very high number of infections, in an attempt to protect the population and to solve the crises. The number of deaths were increasing so fast that there was no place anymore to bury the corpses, reason why some of them were lined up waiting for coffins to be buried.[21]

With freedom of movement restricted, the contact-tracing apps are a very strong ally to control and possibly limit the spread of a disease. Countries have to find a balance between safety and keeping as close as possible to normality the social context, while the whole world wait for a vaccine that can be effective against the virus.

In June 2020, that is at the end of the "first wave" of the pandemic, Italy released the mobile app called "*Immuni*", with the slogan: "Living a normal life once again is possible. *Immuni* helps us reach this goal faster and without compromising our privacy."[22] A whole website was built to inform how the app works with specifications, open code source and data privacy content.

The app and the code were developed by the public company Sogei S.p.A. However, the exposure notification functionality is provided by Apple and Google Technology. The main function of the app is to notify people who were in close proximity with positive tested individuals.No geolocation is necessary, as the app use Bluetooth technology. One of the key features of this kind of software is that a person who is tested positive for COVID-19 can upload her keys (I.e.random numbers associated to the app) only with the validation of health care provider, which proved to be an effective way of avoiding frauds and false notifications. [23]

The principles on which the app was based are, according to the Sogei website, the following:

> **Utility:** The app needs to be useful in fulfilling the project's vision and goals, as outlined above. The key here is to be able to notify as high a percentage of the people who are substantially at risk as possible, and to do so as early as is practical. This is the

20 https://covid19.who.int/region/euro/country/it Accessed on 04/02/2021.
21 https://www.theguardian.com/world/2020/mar/19/generation-has-died-italian-province-struggles-bury-coronavirus-dead Accessed on 30/09/2020.
22 https://www.immuni.italia.it/ Accessed on 30/09/2020.
23 Complete information can be found: https://github.com/immuni-app/immuni-documentation.

> most important principle. **Accessibility:** For fairness and to facilitate the widest adoption, Immuni should be accessible to the maximum possible number of people who may want to use it. This principle impacts decision-making across the board, including in user experience, design, localisation, and technology. **Accuracy:** Immuni aims to notify only those users who have a substantial risk of having contracted the virus. This is important because of the psychological toll that goes with being notified about a potential transmission of the disease, and because too high a rate of false positives would result in users losing trust in the app—and stopping their use of it. Also, the more accurate the app is, the more efficiently the National Healthcare Service (Servizio Sanitario Nazionale) will be able to take care of users, making sure to attend to higher-risk ones first. **Privacy:** Immuni must protect user privacy while remaining effective. Earning and maintaining user trust is critical—failing to do so reduces the likelihood of widespread adoption. **Scalability:** Immuni needs to be widely adopted throughout the country. This requires the system to scale well technologically and the operational burden it places on the National Healthcare Service to be manageable. **Transparency:** Everyone should be provided with access to documentation describing Immuni in all its parts and the rationale behind the most important design decisions. Also, the app will be open source. This allows the users to verify that the app works as documented and the expert community to help improve it. (https://github.com/immuni-app/immuni-documentation#principles)

Reading and explaining the principles, we can notice the concerns expressed about inclusiveness and transparency, which should be the most important principles of the app. Continuing with the analysis of the information contained in the website, one really important point is that the app is supposed to save operational and epidemiological information as part of its analytics. The operational information saved regards the following:

> "Whether the device runs iOS or Android; Whether permission to leverage the Apple and Google Exposure Notification framework is granted; Whether the device's Bluetooth is enabled; Whether permission to send local notifications is granted; Whether the user was notified of a risky exposure after the last exposure detection (i.e., after the app has downloaded new temporary exposure keys from the server and detected if the user has been exposed to SARS-CoV-2-positive users); The date on which the last risky exposure took place, if any."[24]

According to the providers, this information is important to know the number of apps actually functioning correctly, the localities with more positive tests, to prevent possible breaking outs of the virus. Another feature of the collected data is the estimation of when people with Covid-19 symptoms are most likely to appear in certain locality. This could be very effective in preventing chaotic situations in hospital facilities. Effectiveness however depends on the number of users of the app, as the

24 https://github.com/immuni-app/immuni-documentation Accessed on 01/10/2020.

highest the number, the more will be the system effective in providing a faster response to the National Healthcare, and the more hospitals will be prepared to the upcoming local needs.

Moving forward and addressing now Data Privacy concerns, which is the big highlight of the use of digital health app, the SOGEI's website ensures that all the data collected are anonymous and encrypted, and will be deleted no later than 31/12/2021. The Health Minister is the responsible for the data collected; data will be only used for research purposes or for the purpose of containing the COVID-19 pandemic.

The Italian app was downloaded by 5 million people, as of August 2020,[25] It is still enough to really profit from the tool. Crucial factors that condition the successful implementation of such tool are still lacking. In particular, the level of technological literacy of people is still low in most of the cases, and the government needs to inform the population on how the data will be used, to build confidence and make the users' number to surge.

2.3.1 Italian Legal Framework and Risk Assessment

Italy, as part of the European Union, operates the measures against COVID-19 in compliance with the EU Law[26], National Laws and the State Emergency Decrees. Initially, The Italian State declared 6 months of State Emergency, that on 7th of October was extended until 31st of January 2021, by the Council of Minister n°66[27]. Art. 5 of the Decision also stressed the collection and treatment of personal data by the Civil Protection[28]

25 https://www.repubblica.it/tecnologia/2020/08/25/news coronavirus_l_app_immuni_a_5_milioni_di_download_ma_e_solo_il_13_-265432164/ Accessed on 01/10/2020.
26 The EU Law regarding Data Privacy will discussed in the next chapters of this thesis.
27 Available at http://www.governo.it/node/15350, Accessed on 16/11/2020.
28 Available at https://fra.europa.eu/sites/default/files/fra_uploads/italy-report-covid-19-april-2020_en.pdf, Accessed on 16/11/2020.

Regarding the Use of the *"Immuni app"*, the public authorities released the "*Decreto legge*[29] *30 aprile 2020, n. 28*[30]*"*, based on article 6 of the initial *decreto legge* and also on the Health Minister Impact Evaluation of Data Protection regarding the use of the *Immuni App"*[31], the State is operating the use of personal data in the country to contain the spread of the virus through the exposure notification technology.

Article 6th of the initial Decree[32] set forth the use of the application for the only purpose of notifying individuals that were in contact with people confirmed as positive, to protect the health of users. The app's download must be voluntary and cannot discriminate the ones that have not downloaded the app, for the principle of equality. Together with the legal basis mentioned in the first paragraph, also the public interest needs to be demonstrated in order to be considered lawful in the use of data health. Accordingly with the GDPR[33], EU countries need to have their own definition of what is considered public interest[34], to regulate specific provisions regarding data privacy adapted for the country needs.

Through the Decreto Legge 110/2018 some modifications regarding the use of data privacy are provided, following the premises of the recital 46 of the GDPR[35]:

> The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person.
> Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis.
>
> Some types of processing may serve both important grounds of public interest

29 It is a tool used by the government in state of emergency and has the same effect as any other law but must be converted in law in the next 60 days after its promulgation. Morisi, M., & Cazzola, F. (1981). LA DECISIONE URGENTE. USI E FUNZIONI DEL DECRETO LEGGE NEL SISTEMA POLITICO ITALIANO.*Italian Political Science Review/Rivista Italiana Di Scienza Politica*,*11*(3), 447-481. doi:10.1017/S0048840200011977.

30 Available at https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg, Accessed on 17/11/2020.

31 In Original *Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni"*, Available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9357972, Accessed on 16/11/2020.

32 Available at https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg Accessed on 18/11/2020.

33 Article6(1)(e) and Recital 45, GDPR.

34 Available at https://www.agendadigitale.eu/sicurezza/privacy/covid-19-il-difficile-equilibrio-tra-diritto-alla-salute-e-tutela-della-privacy/ Accessed onaccessed on 19/11/2020.

35 Available at https://www.privacy-regulation.eu/en/recital-46-GDPR.htm, Accessed on 19/11/2020.

> and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

Accordingly to the content above, the grounds for monitoring epidemics should be enough to retain personal data, certainly respecting other principles and a maximum length of data storage, as will be discussed further more in the chapter destined to the European Legal Framework.

The GDPR is clear in relation of the prerogatives the countries have in applying the restrictions to the fundamental rights, grounded in the public interest and in respect of the independence principle[36]. However it is necessary to assess Italian National Laws to underline the framework that has been used during the COVID-19 pandemic.

As the pandemic introduced new scenarios, the regulations surrounding Data Privacy Issues are still in a test phase. In other words, most of the outcomes of the use of contact-tracing app will be under close scrutiny and also the aftermath of this phase will be addressed, as all the important aspects of the use of this technology are still new to the legal system.

In this regard, it can be observed that the legal basis to achieve a significant protection of data privacy as a fundamental right is still a bit ahead of the current legal framework it is necessary to develop a bridge between technical and legal definitions.

The Italian Law is not innovative regarding the process of personal data, however it enshrines basic rules to be followed based on principles that can guarantee the legitimate use and process of health data during the pandemic.

Having the Health Minister as the controller of the data certainly uphold more confidence to the citizens. As of the start of the pandemic, in a survey made on June

36 Article 52, GDPR.

2020[37], 65 percent of the Italians interviewees approved the measures taken by the government in response to the pandemic and the acceptance of the Prime Minister Giuseppe Conte increased during the month of April, 2020.[38]

Some instructions have been made by the European Data board regarding the use of geolocation in case goverments decide to use GPS technology to control people in quarantine and monitoring social distance measures, assuming they would carry their phones in case they leave the house[39]. However, according to the Italian Law, the authorities have no access to the user's location, even with the use of centralized data.

As the measures for combating the pandemic were taken shortly after the beginning of the crisis, and the authorities needed to deliver a fast response to the society, it is unclear if those measures are effective to contain the spread of the virus and mitigate the aftermath. After this brief discussion of the Italian Law, it is possible to highlight some characteristics that could represent risks to the citizens, regarding data privacy as a fundamental right.

Data privacy is a fundamental right protected by important International Covenants, the European Union Law and National Law. To respect personal data and the right to privacy in the age of technology, states have to set up a dedicated governance.

However many countries are still falling behind effective regulation to the use of technology during the pandemic. One of the first gaps that can be pointed in the National Italian system and also in the GDPR is the lack of provisions concerning redress in case of leak of information or misuse of data.

Another risk that could be pointed is the use of anonymised data, even with the efforts of developers to build a very high trusting technology. The European Board

37 Available at https://www.statista.com/statistics/1106743/opinions-on-italian-government-s-response-to-coronavirus/ Accessed on 19/11/2020.
38 Ibid.
39 Available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9308774#english_version. Accessed on 24/11/2020.

stated that often the data controllers fail[40] in guaranteeing that this data can not be identified, and there are studies showing that more technology has been developed to re-identify[41] individuals[42].

When it comes to digital contact-tracing, a legal analysis will be often connected to the technical specificity of the apps which can be difficult, as for both legal and technical fields, the apps are a novelty and more time is needed to address likely failures or to develop specific features. Addressing likely risks can also raise awareness that could be used in case of a change in the actual regulation of the subject.

The Italian Garante per la Protezione dei Dati Personali has published an evaluation[43] of the *Immuni* app considering both technical and legal perspectives, mentioned in the Report of the European Union Agency for Fundamental Rights[44] , and illustrates some measures that should be taken by the state in order to guarantee fundamental rights in the use of health digital data.

The evaluation mentions that the algorithm should be open source, accessible to the scientific community and updated with the latest versions with the purpose of checking the code and evaluating possible failure. The open source character ensures that the software is developed overtime and it is also the equivalent of "free speech" in technology.[45] Moreover, the evaluation advices that the users should be informed that

40 Bradford, L. R., Aboy, M., & Liddell, K. (2020). COVID-19 contact-tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes.*Journal of Law and the Biosciences*.

41 Alexandre de Montjoye et. al., Evaluating COVID-19 contact-tracing apps? Here are 8 privacy questions we think you should ask, Computational Privacy Group (Apr. 2, 2020) https://cpg.doc.ic.ac.uk/blog/ evaluating-
contact- tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/.

42 The *Immuni App* has been using the type of protocol number 2 explained in the article of the footnote 34 where the authorities notify the individuals that have been in proximity with the infected person.

43 Available at https://images.go.wolterskluwer.com/Web/WoltersKluwer/%7Bbcbf65c6-ffe2-4b95-8931-d4e42ac03ee7%7D_garante-privacy-provvedimento-1-giugno-2020.pdf Accessed on 25/11/2020.

44 Available at https://fra.europa.eu/sites/default/files/fra_uploads/it_report_on_coronavirus_pandemic_july_2020.pdf. Accessed on 25/11/2020.

45 Available at https://www.forbes.com/sites/sap/2020/11/19/how-the-holiday-shopping-experience-will-be-different-in-2020and-what-it-means-for-frontline-staff/?sh=5f7cec3a6e8e. Accessed on 26/11/2020.

not always getting a notification can reflect a high risk condition, as the conditions can change according to the use of protection tools, like masks, for example.

Following the points of the evaluation, another recommendation is that the app should notify the users about the option to temporarily deactivate its functions and additionally introduce measures to track activities of the system's operators[46] in the database and systems, adopting measures that could mitigate likely damages.

Understandably, most of the risks are represented by technical problems or obscurities that are still unclear to not only the governments, stakeholders but also to the developers involved in the projects. What can be done is guarantee the safe use of the apps, meanwhile the citizens can rely in the already existent legal framework in the international and national levels.

On the other hand, It is also possible to discuss and address some issues that can represent risks and breaches in the Italian Framework. It is known that the health minister is the data controller which as mentioned before, builds trust, however the law also needs to predict the outcomes in case of misuse or leak of the information collected.

Regarding legal procedures, there is no provision of redress in the specific case of misuse/leak of the information during the COVID-19 – This should be provided and as it is a new field, it is important to create awareness in the society and inform about their rights in case of leak.

Furthermore, there should be installed reviews assessing the use of the app and checking the modifications, failures or other situations that might happen. This review should be done by the state and not only by the private companies that are developing the software.

46 Available at https://images.go.wolterskluwer.com/Web/WoltersKluwer/%7Bbcbf65c6-ffe2-4b95-8931-d4e42ac03ee7%7D_garante-privacy-provvedimento-1-giugno-2020.pdf. Accessed on 26/11/2020.

3. Digital Health in Switzerland

Switzerland, as of 14/10/2020 was since at the beginning of the pandemic, with in total 68,704 confirmed cases of COVID-19[47]. The country had an approach different from most countries in Europe, which can be related to its tradition of direct democracy and the features of transformative governance[48] that has been emerging in the country[49].

The policies that Switzerland used to contain the virus were decided at the federal and cantonal levels; many regulations were made based on the urgent need of each canton, aiming to quickly reduce the spread of the virus, protect the elderly and people with health problems, decrease the burden on the health care system, and eventually flatten the curve of new infections. Hence, some measures are applied all over the country, while others are applied only in some cantons[50].

The idea of having a complete shut down of the regular services were applied in the first months of the pandemic when only essential services were open. The central authorities recommended that people would remain at home and only go outside when extremely needed. However, there were not sanctions in case leaving the house for practicing sports alone, for example. Currently, (fall 2020) the requirement of wearing a mask is mandatory in public transports, supermarkets, airplanes, stores and demonstrations.[51] [52]

47 Available at https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/situation-schweiz-und-international.html#-6104062 Accessed on 14/10/2020.

48 Transformative Governance can be a new way in decision-making that specially during crisis, ensure governments that policy-making based on evidence is effective to promote social changes.

49 Willi, Y., Nischik, G., Braunschweiger, D. and Pütz, M. (2020), Responding to the COVID-19 Crisis: Transformative Governance in Switzerland. Tijds. voor econ. en Soc. Geog., 111: 302-317. doi:10.1111/tesg.12439

50 https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/massnahmen-des-bundes.html Accessed on 14/10/2020.

51 As of 1st November, the canton of Geneva has implemented a partial lockdown closing all establishments but schools and day nursers until the end of the month to contain the spread of the virus given to the rapid increase of hospitalizations. This information can be found at https://www.swissinfo.ch/eng/geneva-introduces-partial-lockdown/46134304, Accessed on 27/11/2020.

52 https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/massnahmen-des-bundes.html Accessed on 14/10/2020.

On the 25th of June, 2020, the Swiss Covid app was launched and It was the first country in the world to use the API Google and Apple technology[53]. The app was developed jointly by ETH Zurich and EPFL Lausanne on behalf of the Federal Government.[54]It also works based on Bluetooth approximation. In a range of a 100m, random IDs are detected and stored for 14 days. If a user tests positive for COVID-19, the cantonal authorities will assign her/him a code, so this person can activate the function of notification in the app and notify people that might have been in close contact with her. The Id of the infected person is anonymous; if someone receives a notification, the next step is to quarantine herself. All people who were in close contact with a tested positive within the previous two days before starting the symptoms have to be put in quarantine. [55]

The requirements for triggering the notification is to have been in contact at a distance of less than 1.5m with an infected person for at least 15 minutes. After the notification, the person who has received it, should call the cantonal info-line to be informed about the next steps. [56]As of 14/10/2020, more than 2.485,394 million of downloads has been done[57]. The federal Government has been also publishing the daily number of codes for activating the notification function that has been liberated, and as of 04/02/2021, more than 1.263 mil codes were released in the last 7 days.[58]

A Data protection statement was made by the Swiss Federal Government on the 24th of June, to explain how the data will be held and who will control them. From the statement is important to highlight that the controller of the data processing is the Federal Office of Public Health Data collected do not include information about

53 https://www.businessinsider.com/switzerland-google-apple-contact-tracing-api-launched-2020-5?r=US&IR=T Accessed on 14/10/2020.
54 https://ethz.ch/en/news-and-events/eth-news/news/2020/05/swiss-covid-app.html Accessed on 14/10/2020.
55 https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-1601404801 Accessed on 14/10/2020.
56 Ibid.
57 https://www.experimental.bfs.admin.ch/expstat/en/home/innovative-methods/swisscovid-app-monitoring.html Accessed on 04/02/2021.
58 Ibid.

location or devices, but only the randomly assigned IDs of devices that were in the user's proximity. [59]

The first part of the federal government's document describes how the app system works and the data management system, while the second part is regarding the notification management system plus the data that is stored in the device:

> The identification codes (Random ID) received from other mobile phones on which the app is running the signal strength the date and the estimated duration of proximity. In the event of an infection being confirmed in a user, the following data is recorded in the code management system: the activation code (Covid code) the date on which the first symptoms appeared, or – if the infected user is asymptomatic – the date of testing the time at which this data is to be destroyed. The PM back end contains a list with the following data: the private keys of infected users which were current in the period during which other users were potentially exposed to the coronavirus and the date of each key.[60]

3.1 Swiss Legal Framework and Risk Assessment

Switzerland as a country located in the heart of Europe , It not only shares borders with EU countries but also shares social-economic ties that lead the country to collaborate with the EU legislation as a guarantee of free movement of people and goods. As a part of the EFTA, the EU has a priority position in Swiss foreign policy and regarding that, the country operates its relations with the EU by Agreements in different subjects where the legislation needs to be enforced by the two parties of the agreements.

The Agreements allow Switzerland to trade and have mutual access to different areas of the EU market, including in areas such as research, environmental policies and migration, for instance. However, it is relevant to say that Switzerland did not transfer any legislative/decision-making power to any supranational instance, except for air transport, in order to protect the sovereignty of the country [61].

59 https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing/datenschutzerklaerung-nutzungsbedingungen.html#-11360452 Accessed on 14/10/2020.

60 Ibid, p.2.

61 Available at https://www.eda.admin.ch/dam/eda/en/documents/publications/EuropaeischeAngelegenheiten/Schweiz-und-EU_en.pdf. Accessed on 29/11/2020.

In relation to personal data protection, Switzerland in its Federal Constitution, article 13, declares that: *"Every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications. Every person has the right to be protected against the misuse of their personal data."*[62]

The Federal Act on Data Protection[63] came into force in July 1993 and its 1st article states that its aim is to protect the privacy and the fundamental rights of people when their data are processed. [64] While the GDPR came into force in 2016, the Swiss government has been a pioneer in regulating this subject and demonstrating a solid legal framework to protect Data privacy as a fundamental right.

As the country is divided in 26 cantons, the federal and cantonal authorities share some competences in the decision-making. The Federal Act on Data protection applies only on the data processing of natural and legal persons by private persons and federal bodies, while each canton has a cantonal act on data protection to the process of data by the cantonal bodies. In the Federal Act on Data Protection, it is stated which subjects the federal government will regulate and the subjects that are not included will be subject to the cantonal regulation.

The European Commission decided[65] in 2000 that the Swiss Federal Act complies with all the requirements of the European Union and that it provides protection against the unlawful processing of personal data. Moreover in the decision, the court has mentioned that all the legal standards and principle are covered by Switzerland even with the exceptions provided for the defense of public interests.[66] An emphasis in the

62 Available at https://www.admin.ch/opc/en/classified-compilation/19995395/201801010000/101.pdf. Accessed on 30/11

63 Also FADP.

64 Available at https://www.admin.ch/opc/en/classified-compilation/19920153/index.html. Accessed on 29/11/2020.

652000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland. Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000D0518. Accessed on 02/12/2020.

66 Ibid, point 10.

decision is that the state guarantees the application of the standards by providing an independent supervision that can be requested by judicial remedy.

Furthermore, in Article 3 of the Federal Act, personal data is defined as all information related to an identified or identifiable person (including natural and legal persons) and also defines health as sensitive data.

3.2 Core principles and legal provisions of the Federal Act on Data Protection

The Swiss Federal Act of Data Protection states some core rights that are also found in the previous legal frameworks analyzed and brings principles as lawfulness, good faith and proportionate.[67] The principle of proportionality embraces three different dimensions: ability that refers to the need to use the tools towards the final objective[68]which is to prevent abuse of the means; necessity, meaning that one has to demonstrate the reasons to process data; and finally, proportionality, in assessing any damage in the private life *versus* the planned objectives.

Data collection can happen only for the purposes - and data detention can be maintained for the time - indicated and provided by law. In 2008[69] an amendment was enforced enshrining the evidence as a requirement, in other words, a data subject has to be aware that her/his personal data are being collected ; This rule echoes the idea of consent, as in the previous legal framework analyzed: consent is the basis to a lawful data collection.

TheFederal act requires that all the data collected must be correct[70],enshrining the principle of the correctness. The data controller needs to guarantee that the data is correct and in case it is incorrect, the data subjects have the right to ask for correction or to delete the data.

67 Article 4th of FADP.
68 Metille, S. (2013). Swiss information privacy law and the transborder flow of personal data. Journal of International Commercial Law and Technology, 8(1), 71-80.
69 Ibid, note 61.
70 Article 5, FADP.

The FADP reinforces the remedied already contained in the civil code[71] when litigation is needed. And in Articles 35, it brings its own criminal provisions: in case of private persons if they *breach their obligations in providing information, register, cooperate with the information commissioner or if they breach their professional confidentiality* – they are liable of a fine.

Other relevant provisions in the Federal Act have a direct effect on how the data will be processed and the cautions that might be needed to assure data protection. Data subjects have the right to information safeguarded in article 8 : Any person may request information from the controller of a data file, as to whether data concerning her is being processed. Furthermore the data controller must provide her all available data concerning the subject and the source of the data, the purpose, the data recipient and other parties involved. If personal data has been processed by a third-party the controller still has the obligation to provide information.[72]

Bringing forth more accountability to the data controllers and a direct remedy to repress future or current damage to an individual's private life represent a combination that can be effective to preventing judicial litigation and also provide redress in case of real aftermath. Said that, the idea of having a proper regulation reflects on the effectiveness of the prevention on data leaking and advocates to assure governments as having the key roles in the international community, leading and giving examples to other countries to implement their data protection regulation, bearing with the difficulties in controlling the data flow.

In this sense, as globalization has softened borders, it has become crucial to regulate the cross-border data flows as much for the private persons and legal persons. Indeed, the leak of information can cause serious economic and social damages. In article 6 some important constraints are stated in case of cross-border data flows. It is

71 Article 28, Civil Code.

72 In case the controller is not domiciled in Switzerland, the obligation to provide information is of the third party. And the information should be released free of charge.

strictly forbidden to disclose personal data abroad *if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection*[73].

The above mentioned article is a clear example of how the countries could be more proactive concerning cross-border information and guaranteeing the protection of data privacy as a fundamental right and not only regulating but enforcing the law throughout the implementation of procedures and regulation. As Switzerland attracts investors from all over the world, the country must have strong laws that can allow safe investments and trustworthy.

Aiming to provide safe cross-border data flow, the Federal Data Protection and Information Commissioner[74] has published a list of jurisdictions[75] that comply at least to a certain extent to the obligations in data privacy. To some countries, for example, it is possible to transmit data only if an agreement is established, while for other countries the transmission is less problematic.[76] Countries that are considered to have adequate data protection regulations are the EEA countries, Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand and Uruguay while the remaining countries are considered to not have adequate data protection[77].

In case of inefficient regulation, the data might be transmitted adopting some rules:

> Sufficient safeguards, in particular, contractual clauses, ensure an adequate level of protection abroad; the data subject has consented in the specific case; the

73 Article 6, FADP.

74 The FDPIC has his mandates to voluntary or by third-party request to investigate, supervise, advise private and federal bodies, cooperates internally and abroad with the data authorities available at https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/the-commissioner.html and https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/task.html. Accessed on 8/12/2020.

75 The list can be found at https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html. Accessed on 08/12/2020.

76 Available at https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html. Accessed on 8/12/2020.

77 Available at https://www.lexology.com/library/detail.aspx?g=292c3925-8663-4fdb-8f1c-2eaf4b262634. Accessed on 8/12/2020.

> processing is directly connected with the conclusion or the performance of a contract and the PII is that of a contractual party; disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts; disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;the data subject has made the PII generally accessible and has not expressly prohibited its processing; or disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules (ie, binding corporate rules) that ensure an adequate level of protection.[78]

According to the FADP a model agreement can be found in the website and must be signed by the parties, it is based on the Swiss Law and also complies with the European commission for standards data transmission clauses, to ensure that the agreement bears the rights protection of the data subject.

Historical facts has indicated that in order to be efficient and deliver a fast response during health emergencies, global data sharing is crucial. It allows to develop vaccines, treatments and also standardized procedures of testing, research output and sources. The World Health Organization in a statement regarding data sharing during the COVID-19 pandemic[79], highlighted that during the 2013-2016 Ebola virus disease outbreak in West Africa the subject was raised of full data sharing and in 2015 an agreement was made on sharing health data during public health emergencies. Aiming to improve research and respond to the crisis , the WHO has provided a COVID-19 Open data sharing and reporting protocol to be applied during the current pandemic.

In this sense, it is essential to demand from governments proper legislation to provide anonymisation of the collected data during the COVID-19 pandemic and also to establish legal framework with a full description of procedure for cross-border data sharing, including criminal sanctions. All of these points lead the discussion to the decisive role of international cooperation. A fair cooperation focusing as the priority the

78 Ibid note 70.
79 Available at https://www.who.int/bulletin/volumes/98/3/20-251561/en/. Accessed on 8/12/2020.

solution to this current crisis, plus bearing the data privacy and building a solid action plan that can also be used in the future promoting continuous advance for Privacy Law.

3.3 Legal Framework for contact-tracing apps (SwissCovid)

The Swisscovid app has been established in Switzerland based in the article 60a[80] of the Federal Law of Epidemic[81] together with an Ordinance on the proximity tracing system for the Sars-CoV-2 coronavirus[82] and the Data Protection Statement of the Federal Office of Public Health FOPH in connection with the use of the "SwissCovid app"[83] that allows the government to run the app until June 2022.

The Data Protection Statement highlights the purpose and the duration of the data storage, mainly specifying that no geodata will be stored outside the device. The communication also highlights the rights of the users and that the SwissCovid app can only be used for its purpose of communicating to people who has been in contact with a infected person and that it cannot be exploited by the police, intelligence services or criminal authorities[84].

The user's rights enshrined in the statement are also and foremost protected by the Federal Constitution and the Federal Act of Data Protection, hence the statement mostly represents and additional provision. The principle of consent is reaffirmed in the statement as the basis of a lawful data processing. The data processor has to inform the users that a withdraw of their consent will consequently affect the whole process of data collection.

---

80 Art. 60A Available at https://www.admin.ch/opc/fr/official-compilation/2020/2191.pdf. Accessed on 09/12/2020.

81 Free Translation from the Italian term "*Legge sulle epidemie*" available at https://www.admin.ch/opc/it/classified-compilation/20071012/index.html. Accessed on 9/12/2020.

82 Available at https://www.admin.ch/opc/en/classified-compilation/20201730/index.html. Accessed 9/12/2020.

83 Available at https://www.bag.admin.ch/dam/bag/en/dokumente/cc/kom/swisscovid-app-datenschutz.pdf.download.pdf/FOPH_SwissCovid_Data_Protection_Statement_24_June2020.pdf. Accessed on 9/12/2020.

84 Available at https://blogdroiteuropeen.com/2020/07/10/covid-19-and-data-protection-issues-in-switzerland-by-alexia-pato/. Accessed on 9/12/2020.

The ordinance, in article 9, lists the authorities that are able to request the activation codes: cantonal medical officers; the Armed Forces Surgeon General; other staff of the cantonal medical services or of the Armed Forces medical services;third parties acting on behalf of the cantonal medical services or the Armed Forces medical services; staff at medical practices; staff at laboratories with authorization under Article 16, EpidA; staff at the facilities specified in Article 24 paragraph 1 letter b of the COVID-19 Ordinance 3 of 19 June 2020; staff of the Infoline under Article 7 paragraph 1 letter c.

In article 12 the ordinance states the reasons for disclosure of data for statistical elaborations, highlighting that all data will be anonymised and in article 13 it foresees that the deletion of the data should be done in 14 days after their recording, both from the database and in the mobile phone,. Based on the Swiss national Law, the cantonal legislation should implement the remaining gaps in the framework, if there is need. [85]And additionally, the Federal Government has published two guidelines on the processing of personal data and personal data health.[86]

3.4 Risk Assessment of the use of Digital Data Health in Switzerland

The final goal of digital health should be the mitigation and prevention of the virus spread, with the guarantee of data privacy protection. As explained in the sections above, Switzerland has a solid data protection regulation and often also integrates the GDPR when it is applicable.

The digital treatment of health data and the likely implications in case of a pandemic is still a brand-new practice. It has surely been an ally in tackling the pandemic, however, the importance of meeting the standard for a lawful personal data

85 Available at https://blogdroiteuropeen.com/2020/07/10/covid-19-and-data-protection-issues-in-switzerland-by-alexia-pato/. Accessed 11/12/2020.

86 Available at https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/dokumentation/guide/trattamento-dei-dati-personali-in-seno-all-amministrazione-feder.html and https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/dokumentation/guide/trattamento-dei-dati-personali-nella-sfera-medica.html. Accessed on 11/12/2020.

processing needs to be analyzed. The challenge is not only to address technical or ethical issues but also legal issues. the question is: Are the legal framework equipped to sustain and redress possible cases of abuse in processing personal data?

a risk assessment of the use of digital data on health has to consider several layers, as it is a complex and interconnected issue. concerns go from political views to governance, from legal to technical perspectives. This makes it difficult to follow one single direction without mentioning the others perspectives. Handling sensitive health data is an issue the will be discussed more and more in the next years.

In Switzerland, the decision-making regarding handling health data is made at different levels to cover the need of the cantons[87]. As explained previously, the federal government regulates until a certain extent the data processing, leaving space for the cantons to regulate details according to their reality. The present pandemic is no exception: each cantonal authority is responsible to deliberate regarding protection measures and data health, even under an emergency state.

Moreover, there are the cross-border laws that also play a significant role in the final analysis of risks. Some studies from the technical perspective can already address some issues with the app that can cause controversies in the future or even hack attacks[88].

Switzerland as mentioned before, has presented a solid data protection legal framework since 1992, in other words, when the European Union was being created[89], the country was already implementing and enforcing data protection, which it is very understandable, if taken in consideration the fact that the county attracts investors from all of the world.

87 Knobel, Isabel, Fegert, Moritz and Detreköy, Niculin (2020): “Health Data Governance: What’s in it for Switzerland?”, Zurich: Sensor Advice and foraus - Forum on Foreign Policy.

88 The technical perspective will be briefly covered based on studies already published, however it is not intended to be exhaustive but to illustrate the current scenario, as the main focus of this work is to elucidate the issue from a data privacy perspective.

89 Available at https://europa.eu/european-union/about-eu/history_en. Accessed on 21/12/2020.

It is undeniable that it is an strong legal framework and during the pandemic, the government was very careful in approving the SwissCovid app, formulating a statement that is very detailed and somewhat include and describe the legal scenario where the app is located – which obey the principle of transparency that it is required to lawfully process sensitive data enshrined in both Swiss laws and European Union Law.

In Switzerland, for instance, a clarification of the type of data collected was made by the amendment to the Epidemics Act before the release of the SwissCovid app.[90]

If the measure is proportional, the government should take into account that it will not be used to monitor citizens but only with the purpose to collect the necessary information to contain the spread of the virus, following the recommendations enclosed in the Report of the Special Rapporteur on the right to privacy as an evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic.[91]In a democratic society, the use of technology for contact-tracing must respect freedom and rights and the general welfare of the society.

One of the critiques of the public was that the Swisscovid app only works in the latest version of the Apple iOs which can affect how many people will use the app and create a digital division, that even if Switzerland with one of the highest GDP[92] in the world[93], can not benefit from the fact that the app only works in the latest iPhone system. It is unfair and it should be taken into account by the developers.

The pandemic not only has showed us the need to create fair measures and policies, but also has revealed that the monopoly of mega tech companies as Google

90 Blasimme, A., & Vayena, E. (2020). What's next for COVID-19 apps? Governance and oversight. *Science*, *370*(6518), 760-762.

91 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. 27/07/2020. Available at https://undocs.org/A/75/147. Accessed on 21/12/2020. The report has as focus the impact of the COVID-19 on the right to privacy: data protection and surveillance – where a more detailed report it is planned to be done in 2021, after more evidence about the subject.

92 Available at https://www.bfs.admin.ch/bfs/en/home/statistics/national-economy/national-accounts/gross-domestic-product.html. Accessed on 21/12/2020.

93 Hence, we can suppose that the population could afford the use of this mobile phone.

and Apple represent various concerns, not only legal but also social. In a globalized world, keeping the creative power of implementing software for the public use, together with states can represent a huge threat to data privacy if not well addressed and discussed with stakeholders.

Additionally, the novelty of the subject is a crucial point and given to that, the discussion is surrounded by some lack of evidence to build irrefutable arguments against or completely in favor of what, whereas the discussions are more about providing legal advises and guidelines to states and companies responsible with the develop of digital health technology. For a more precise analysis, indeed, it is necessary more time of use of these type of technologies to report failures or misuse of data by the controllers or by third parties.

As referred before, the monopoly of only two companies being responsible for the developing of the contact-tracing app[94] and no regulation regarding who can provide the service, has open space to private companies to develop their own application and obligate their employees to use it[95], as the country has not recommended the companies to only use the app or deny that other apps could be used/developed to internal use only[96]. These not only intervene in worker's rights but also allows more uncontrolled third parties in possess of sensitive data. Plus, identifying the party accountable in case of hack attacks, misuse of data or even leak of information would be more difficult if taken into account that some companies are internationally based and could be using services providers from abroad, also in a attempt to avoid Swiss authorities.

The start point to likely fragility is the fact that the app is not open source, so there is no way to verify if the code is safe by an independent expert, the Government is currently doing their own safety tests but if the possibility of an open source would be

94 In the context of Switzerland.
95 Ibid note 83.
96 However, the recommendation of the country is to implement working from home whenever is possible and keep the distance during in the office.

applied, the scientific community could work together to prevent possible hack attacks or other issues.

In this sense, there are other types of apps being developed with the goal of identifying if someone is a user of the SwissCovid app. This is a clear threat to data privacy – and what it is worse is to know that most of these developers can not being held accountable as the person would not even notice someone else is checking whether they use the app or not. One interesting circumstance that could happen it is, the called paparazzi[97] attack that refers to the possibility of identifying if for example a politician, a chief of state is using the app and sell the information for the tabloids. Many are the possibilities that are rising with the use of digital data health, however the legal framework is not prepared to contain the aftermath.

The recommendation would be to regulate who can develop certain apps or to only approve those apps to work trough cantonal or federal procedures. That would build more trust of the population in the government app. Oversight bodies should therefore suggest policy guidance[98] to ensure that that the private sector is aligned with constitutional rights and freedoms and will use technology to monitor employees and private citizens. Also sanctions should be applied as it raises the trusting in the apps, also in the government.

Another important point is the cross-border data: the pandemic has created some paradox that nations are currently dealing with and it has showed the importance of international cooperation, one year after the first registered case in China, the world has seen many different approaches to the pandemic and some other countries, lost the track of the way, failing in delivering a good leadership to protect the people and their rights and freedom. Therefore, it should be a priority to dialogue internationally and exchange ideas with stakeholders, universities and also use multi-level governance to implement effective measures to protect private rights.

97 Available at https://lasec.epfl.ch/people/vaudenay/swisscovid.html. Accessed on 23/12/2020.
98 The country already has published guidelines, as also did the European Union regarding it, however it should be broader shared and enforced.

Hence, the cross-border rights probably will be soon implemented also for contact-tracing apps – The European Union countries are pushing forward to link the contact-tracing apps within Europe.[99]Since October, Germany, Italy and Ireland has joined forces so their users will be also notified if they have been in contact with someone who tested positive and was using one of the three apps[100]. The idea of globalization also shortened borders, as the legal framework within Europe is mostly unified, the goal to unify the apps is clearly the next step of their policies, as traveling so far is still possible.[101]

This leads to the principle of the interoperability. The goal would be to enable the apps to work cross-border. Surely it would be more effective in terms of controlling the proximity of people crossing borders, however sensitive data going to different controllers can increase the threats to data privacy. How this can be avoided is simply throughout the implementation and enforcement of the current existent legal framework. Switzerland Covid app is not operating cross-borders due to some discrepancies in Private Law.[102]

Some countries are requiring a negative test of the COVID-19 for travelers and it has already been mentioned since the beginning of the pandemic, the implementation of digital immunity passports.[103] It seems that the population will need to incorporate to their daily lives an immunity digital passport, a contact-tracing app, therefore the regulation will also need to adapt as soon as possible, to guarantee Data Privacy and

99 Available at https://www.netzwoche.ch/news/2020-08-18/swisscovid-app-soll-in-ganz-europa-funktionieren. Accessed on 28/12/2020.

100 Available at https://www.euractiv.com/section/digital/news/european-coronavirus-tracing-apps-are-crossing-borders/. Accessed on 28/12/2020.

101 As of 20/12/2020 Switzerland has applied an entry ban to all flights coming from the UK and South Africa given to the new type of COVID-19 detected in the regions, with some exceptions. Available at https://www.gov.uk/foreign-travel-advice/switzerland. Accessed on 28/12/2020.

102 Available at https://lasec.epfl.ch/people/vaudenay/swisscovid/lessons-from-swisscovid.pdf. Accessed on 28/12/2020.

103 Singapore has implemented a Digital Health Certificate for COVID-19 in 23/12/2020 based on block chain technology. Available at https://www.businesswire.com/news/home/20201223005428/en/First-Use-of-a-Digital-COVID-19-Health-Certificate-to-Cross-an-International-Border-Completed-by-Traveller-to-Singapore. Accessed on 28/12/2020.

also the right to not use the apps without disadvantages. In this sense, it is important to highlight the technological division existent for the users of the GAEN[104] system, as the system does not work in too old versions of Apple or Google systems, and does not work in Chinese Android versions, creating a clear division and hence cannot be considered as an inclusive measure[105].

Switzerland has so far a strong legal framework and also, it is following the European Union Law and guidelines, however the provision of redress in case of offense is not so clear and the State specifies that it is not liable for likely issues/failures caused by the app[106] – As mentioned before, sanctions in case of damages immaterial or material, shall be used to ensure redress to the citizens and increase trusting in the use of technology. Criminal Law, Data Privacy Law shall be used in case of irregular use of data, however there is no specifications regarding the use of contact-tracing apps.

In a nutshell, the country should specify the sanctions in case of misuse, leak, immaterial and material damages and the liability of third parties regarding the use of sensitive private data, as well, keep the voluntary use of the app. Also, work on a safe transition to the interoperability of the app bearing in mind that the law needs to provide redress in case of misuse of any background.

4. Digital Health in China

The pandeLate December 2019, when the WHO was communicated by the Chinese Municipal Health Commission's website about the first cases of COVID-19 in the city of Wuhan.[107]The origin of the the coronavirus is still unknown, however the first cases happened in China and afterwards spread rapidly throughout the world. Already in the 10th of January 2020, China released the genome of the virus, while most of the

104 Google- Apple Exposure Notification.
105 Ibid, note 94.
106 Available at https://www.bag.admin.ch/swisscovid-data-protection-statement-and-conditions-of-use. Accessed on 28/12/2020.
107 Available at https://www.who.int/news/item/29-06-2020-covidtimeline Accessed on 16/10/2020.

other countries delayed their action to contain the spread of the new virus. Currently the total number of cases in the country is 91, 436 cases and 4.746 deceased.[108]

The origin of the virus is still unknown, however the first cases happened in China and afterwards spread rapidly throughout the world. Already in the 10th of January, China released the genome of the virus, while most of the other countries delayed their action to contain the spread of the new virus. Currently the total number of cases in the country is 91, 436 cases and 4.746 deceased.[109]

It is controversial the role that China played in the beginning of the pandemic, as many sources argue that the country should have warned the international community earlier, so to give them theoretically more chances to combat the disease. However, until the current moment, what it is very clear that even if the countries would have known the situation, the world was not prepared to respond quickly to this public emergency.

Said that, China since then has been an example of effectiveness and efficiency in combating the spread of the virus.. However, the measures adopted by the country are controversial, as the country has applied very strict rules of confinement. The city of Wuhan, for instance, was under a very strict lockdown for 76 days that gradually was extended to other cities in the country; Public transport was suspended, 14.000 health checkpoints were installed across the country; some cities implemented strict control of citizens' movement , return to schools was delayed and in many cities only one person of the livelihood was allowed to leave the house every two days . [110][111]

As the country has lead many research regarding the search of a vaccine for the COVID-19, Digital Health has been one of the many tools that has set eyes in China's policies. The Government since the beginning has been very strict and was able to keep

108 Available at Https://covid19.who.int/region/wpro/country/cn Accessed on 16/10/2020.
109 Available at Https://covid19.who.int/region/wpro/country/cn Accessed on 16/10/2020.
110 China has an interesting position for the International Community and its Governance has been criticized due to many Human Rights violations. However, the goal of this Master's Thesis is to inform and discuss about the use of DBN BNigital Health, where the political discussion will be only made if extremely necessary to this work.
111 https://www.thelancet.com/action/showPdf?pii=S1473-3099%2820%2930800-8 Accessed 16/10/2020.

up the contact-tracing for a long time, what did not happen to most of the countries that were overwhelmed by it in the first days of the first's wave peak.[112]

Not only digital contact-tracing app but other tools have been use in the diagnostic of the disease, to access public spaces and to travel. [113]Digital Health strategies can save lives and save time when it comes to quickly respond an emergency. As a leader country in diverse technology, China has invest a considerable amount of money in the Digital Health industry, some innovative projects are being used and also other technologies other than Bluetooth, as for instance, the 5G technology.

4 a) Medical Robots at Wuhan Thunder Mountain Hospital

A medical robot has been used since march at the Wuhan Hospital, using AI and 5G technology, the robot has 7 showers to disinfect automatically, also it can come and go to different facilities caring out medical equipment and medicines. It can operates for eight hours with one charge and every disinfection has the level required for a surgery room, hence the robot can disinfect the boxes with medical supplement and then, the health carer can touch the box and take what it is necessary.[114]It can also disinfect an area of 120 squares meters per minute, and it can be done twice a day

4 b) 5G Thermal Image Sensors

It can be used to measure temperature even if the use of masks, can also do facial recognition in real time and works really quickly so it does not affect the traffic and it can also be used in public gatherings. It has also been used robots that can be remotely controlled and measure temperature of up to 5 people at once, detecting if someone is

112 Ibid.
113 https://news.itu.int/covid-19-chinas-digital-health-strategies-against-the-global-pandemic/ Accessed on 16/10/2020.
114 https://www.sohu.com/a/378301359_100256408 Accessed on 16/10/2020.

not wearing a mask and report to authorities, which can be helpful as no human control is required, giving more space to already heavy busy emergency controllers.[115]

Recently a Chinese company has also developed a phone with temperature sensor that can sensor a range from -20 Degrees Celsius to 100 Degrees Celsius. [116]

The police in the cities of Shenzhen, Chengdu, and Shanghai is equipped with helmets that include a sensor to measure temperatures: “An AR visor, camera that can scan QR codes, Wi-Fi, Bluetooth and 5G to provide the data from the nearest hospital, plus facial recognition technology that can show the individual’s name and medical history.”[117]Theoretically, it would be possible scan 100 people in 2 minutes.[118] In a pandemic, being effective makes a difference in the aftermath, if considered the high number of hospitalizations if the cases are higher again.

As a country with a powerful monetary status, the population can benefit directly from the high level of the technology, however, the huge control that the state is forcing its citizens is also increasing the international pressure into the country that needs to respond to the critics but so far, have not undone its own beliefs.

4 c) Drones

Chinese Government is also using drones to different activities as warning people to be at their homes, to use mask, to disinfecting public spaces, to delivering supplies and even to fever detection in crowds.[119] During the lockdown the drones were also being used to ensure that the population was following the measures, as they were also

115 https://www.allaboutcircuits.com/news/china-deploys-5g-patrol-robots-to-monitor-the-spread-of-sickness/. Accessed on 16/10/2020.
116 https://www.dailymail.co.uk/sciencetech/article-8385835/Huawei-subsidiary-unveils-smartphone-sensor-temperature.html. Accessed on 16/10/2020.
117 Extracted from https://www.theguardian.com/artanddesign/2020/mar/25/10-coronavirus-covid-busting-designs Accessed on 16/10/2020.
118 Ibid.
119 https://www.theguardian.com/artanddesign/2020/mar/25/10-coronavirus-covid-busting-designs. Accessed on 19/10/2020.

equipped with cameras.[120]However, this tool was used for another countries, as Italy, France, Spain, Germany and USA to also ensure the lockdown measures.[121]

China is the world leader in drones production and the pandemic has boost the market since the lockdown began, after being used for agriculture, drones now are taking a role of surveillance to citizen's private lives. What can be used as another manner to control the population, in this exceptional situation the world is going trough, the materials that can threaten one's life, currently can be used as an argument to apply new standards to the civil society.

4 d) Hospital on Cloud

On 9th April, 2020 China has presented in a webinar at the "AI for Good" Global Summit[122], some of the digital health strategies that has been implemented during the pandemic, including a Hospital on Clouds, a project existent since 2014[123] that was effectively implemented in the beginning of the year, in only 10 days[124], which is a remarkable milestone even for Chinese standards. The hospital is equipped to receive only COVID-19 cases and also able to receive patients in different stages of the disease.

Using cloud computing[125] and incorporating 5G the hospital is equipped with different databases: Hospital Information System, Laboratory Information System, picture archiving and communication systems, auxiliary information systems. Additionally the hospital uses different servers to host and backup database, including timely database, so the availability, reliability, security will be guaranteed. The Chinese

120 Kummitha, R. K. R. (2020). Smart technologies for fighting pandemics: The techno-and human-driven approaches in controlling the virus transmission. *Government Information Quarterly*, 101481.
121 Ibid, p.6.
122 https://aiforgood.itu.int/events/covid-19-chinas-digital-health-strategies-against-the-global-pandemic/ . Accessed on 19/10/2020.
123 https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1487056335 Accessed on 19/10/2020.
124 https://www.bbc.com/news/in-pictures-51280586 Accessed on 19/10/2020.
125 Cloud computing is a technology that provides data storage, apps, servers access via internet by a remote data center. Available at :https://www.ibm.com/cloud/learn/cloud-computing Accessed on 21/10/2020.

Government claims the benefits are the development of the applications and sharing data with the nationwide hospitals, plus having a standardized interface and data format.[126]

The idea of having an entire hospital with its database stored in clouds can be very useful to sharing information with other units and to deliver a more effective work. However, If the government do not set boundaries to use of this data, it could really be a threaten to the Data Privacy rights of citizens, if the government do not take any precautions in establishing a transparent governance. [127]

the Chinese Government is known of being controlling and use technology to oppress the population, by Big Data and Mass Surveillance. China already is an example of the use of smart cities and during the pandemic, the country is taking its measures towards a technological-approach, in other words, different of the western nations[128], China has driven its decision to a more and more technological world, which as mentioned before, can and should be used to build back better.

4 e) QR Health Codes

The country has implemented the use of a QR code to allow access to public spaces, to traveling and to aware quarantine[129]. The areas are divided by risk areas and you should be able to travel if you have a red code with your health data and has not been in red areas or in contact to infected individuals. The System works as traffic lights, if it's red the individual should go in quarantine for 14 days, if it is yellow there

126 https://aiforgood.itu.int/events/covid-19-chinas-digital-health-strategies-against-the-global-pandemic/ . Accessed on 19/10/2020.

127 The Chinese Government has for a long time been under suspicions of Human Rights violations, specially concerning personal freedoms and rights that were even more highlighted after the demonstrations in Hong Kong. More information is available here: https://www.hrw.org/news/2020/09/09/global-coalition-urges-un-address-chinas-human-rights-abuses. Accessed on 24/10/2020.

128 Kummitha R. (2020). Smart technologies for fighting pandemics: The techno- and human- driven approaches in controlling the virus transmission. *Government information quarterly*, *37*(3), 101481. https://doi.org/10.1016/j.giq.2020.101481

129 Available at https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Accessed on 04/01/2021.

is the possibility of a risk and the individual must go to quarantine for 7-14 days and finally with a green QR code, the individual can move freely in the city[130].

The code is also required for foreigners traveling to China. Passengers must present the PCR and antibodies test, then present it to the Chinese Embassy where the passenger will receive a green code which allows to enter in the country.[131] The early stages of the system was developed by the Ant Financial, a company linked with the e-commerce Alibaba Group together with the help of local government in the city of Hangzhou. Afterwards, the system is already applied in more than 200 cities, however there is no clear explanation to the population of how the system classifies the users.

According to the official police social media account[132], the police department worked closely to develop the system, however is also unclear what is the role of the department and if there are sensitive information being forwarded. The New York Times has published an article and affirms that as soon as the user allows the application, an archive called: "reportInfoAndLocationToPolice" the location, city, name and identifier code number is sent to a server[133].

Some politicians claim that the QR code should be used undefinitively and not only during the pandemic. In the G20 Summit, the Chinese president engaged a speech defending the world use of the QR code.[134]

4. 2 Risk Assessment Chinese Case

In comparison with western countries, China has a more tech-driven approach and it has demonstrated to have controlled the numbers of new COVID-19 cases. Currently, the use of a QR[135] code to access public spaces and also if in contact with someone who tested positive a following quarantine procedure is applied to the citizens. However the

130 Available at https://www.forbes.com/sites/eladnatanson/2020/12/09/alipay-leads-the-way-in-covid-19-fintech—and-its-a-lesson-for-other-platforms/?sh=5158da9f2638. Accessed on 04/01/2021.
131 Available at https://www.swiss.com/china/en/china-flight-schedule. Accessed on 04/01/2021.
132 Available at https://mp.weixin.qq.com/s/cXlYMcN-pP2oJqgwTYFweg. Accessed on 04/01/2021.
133 Ibid note 120. The New York Times does not clarify how was possible to receive this information.
134 Ibid note 121.
135 Ibid.

big concern is about their citizens data privacy rights – the state continuously controls data health and also geolocation.

For many years the Chinese population has been using a tech-driven governance approach and with the pandemic the measures have increased exponentially, strengthening the surveillance in the country. The UN already has published before the pandemic, a statement of more than 50 UN experts, detailing the gross violations of human rights happening in the country regarding mass surveillance issues and threatens to data privacy, however the Chinese government just responded as this being of gross interference of their domestic affairs.[136]

A call for more international cooperation is needed, however it can not be forgotten that China has constantly help other countries, as for example, Italy, Angola, Kazakhstan,[137] demonstrating that the country has also managed to cooperate in the fight against COVID-19 and has been leading the research for developing a vaccine.

The smart cities in China, together with the increasing of use of technology has determined also the increase of threats to data privacy that are left unanswered by the government. Additionally, human rights defenders are heavily persecuted and so far, the country has not answered any international requests for more freedom of expression. Undeniable that the pandemic was mostly controlled by the tech-driven approach of the country in exchange of the private data of its citizens. The city of Hangzhou has announced plans to make the surveillance app permanent[138], based on the argument of creating a farewell for the people health and immunity.

136 Available at https://www.hrw.org/news/2020/09/09/global-coalition-urges-un-address-chinas-human-rights-abuses. Accessed on 29/12/2020.

137 Available at https://www.weforum.org/agenda/2020/03/coronavirus-covid-19-italy-china-supplies/; http://www.xinhuanet.com/english/2020-07/05/c_139190312.htm; https://news.cgtn.com/news/2020-04-11/China-sends-medical-experts-to-Russia-to-help-fight-COVID-19-PBshI0UoaQ/index.html; Accessed on 04/01/2021.

138 Available at https://www.newsweek.com/covid-19-contact-tracing-apps-could-permanent-after-coronavirus-pandemic-1507103. Accessed on 29/12/2020 and https://privacyinternational.org/examples/3886/hangzhou-plans-permanent-role-coronavirus-surveillance-app. Accessed on 29/12/2020.

The recommendations of the UN Special Rapporteur for Data Privacy on the use of digital contact-tracing app, for example, constantly require it is to be used only if necessary and proportional[139] and all the data collected afterwards must be deleted and the use of the app should cease, avoiding the control of sensitive data by state or other third parties. *Intensive and omnipresent surveillance (???) is not the panacea for pandemic situations such COVID-19.*[140]

However, the Chinese government has initiated the work on a legislation within their Civil Law to enshrine individual's rights to privacy.[141]This would represent a milestone for the individual's right protection, as the country has more and more people with digitized data and smart cities all over the country.

The Alipay application that is now being used by a large part of China population, obviously open doors to innovative digital health commerce; however the threats of intrusive mass surveillance is a concern that must be faced before considering the permanent implementation of a health code, not only in the domestic level of China but also at the International level.

Considering that Freedom of movement is one of the bases of the Rule of Law and that according to the General Comment N° 27[142], article 11, a public health emergency is one of the exceptional circumstances that may restrict it, the restrictions must be provided by the following requirements: must be provided by law; must be necessary for a democratic society; and must be consistent with all other rights protected in the covenant of Civil and Political Rights. Also, the general comment highlights in article 12 that states by themselves should establish in the law the circumstances under which the restriction would be applicable and should also inform the legal norms in their reports in compliance with the covenant.

139 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. 27/07/2020. Available at https://undocs.org/A/75/147. Accessed on 29/12/2020.

140 Point 82, Ibid.

141 Available at https://www.reuters.com/article/us-china-parliament-lawmaking-privacy-idUSKBN2320EF. Accessed on 29/12/2020.

142 Available at. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9&Lang=en. Accessed on 04/01/2021.

And as any measures during health emergencies, inclusiveness and proportionality should be taken into account by the governments to not create more social inequalities but instead, promote equality and a state that protects its citizens rights and freedoms. Despite of it, the use of the application should be voluntary and not mandatory, otherwise inclusiveness is not guaranteed, preventing for example, elderly people to continue with their daily levels without disadvantages and nevertheless, imposing citizens to act in a certain way goes against the Rule of Law and Democracy.

More transparency should be applied not only regarding the laws but also regarding the technologies that are being created - trough open source, for example, a mechanism that help other scientists to double check the codes and also improve it. Implementing digital health tools should be implemented to create a safe environment for citizens to mitigate the aftermath of the pandemic and to strength the democracy and individual freedoms.

5. Legal Framework for contact-tracing apps in Europe

The Pandemic has enforced us to use many different strategies to contain the virus and avoid more deaths and economic recession. The virus exposed the world population to the need of having solid legal framework to ground the emergency state on legality and proportionality.

The pandemic brought into the scenario the necessity of global action to find balanced solutions grounded on human rights protection, that instead of creating unsustainable tensions between governments, population and different stakeholders, would guarantee to the people equality and non-discrimination. "*The best response is one that responds proportionately to immediate threats while protecting human rights and the rule of law.*"Affirmation given by the UN Secretary General[143] calling upon

143 Available at https://www.un.org/en/un-coronavirus-communications-team/we-are-all-together-human-rights-and-covid-19-response-and. Accessed on 04/01/2021.

states to face the global public emergency with transparency, accountability and proportionality, to fight the virus and not the people.

The Special Rapporteur on the right to privacy has published a report for the good use of health data and a statement arguing that:

> Health-related data is very sensitive and has high commercial value. There is a largely hidden industry that is already collecting, using, selling and securing health data. This has a major impact on our privacy and is of enormous concern. The recommendations set out good practices for data management, and address particular issues such as electronic health records, mobile apps, marketing, and employers' and insurers' access to health-related data. They also take into account groups with particular data protection needs, such as indigenous peoples, people living with disabilities, refugees and prisoners.[144]

Concerning the use of data in general, the countries should bear in mind the necessity to guarantee equality and social inclusion, as currently the highlights are turned to health data, it is important to address that sensitive information can cause different effects trough the society layers. Undocumented immigrants or asylum seekers for example, could be one of the part of the population most hit , even worse during the pandemic, as the countries with more capital could use the emergency as an excuse to not provide shelter or documentation to these often marginalized groups.

The effectiveness of the measures must be conducted lawfully and respecting the requirements of the state of emergency. Organizations, Governments must comply with norms and principle to ensure that no violation has been committed and that the measures are not based on personal interest or causing damage to the civil society.

5.1 The GDPR as a legal basis to process data in the European Union

The EU has engaged in providing common norms regarding diverse topics within the countries, aiming to establish more cooperation and equality within Europe. The pandemic has required fast and effective measures that can put in risk economy, health and the leadership of a country. All these factors contribute to add more pressure on the

144 https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25221&LangID=E and https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf Accessed on 26/10/2020.

decisions taken by the nation's leaders. Across the globe, the pandemic is also cause instability for politics that need to use the diplomacy but also protecting the nation's interest.

Until this moment, the time to come and what will be the aftermath of the pandemic is unknown and unpredictable, countries are learning from their mistakes and the global community is trying to overcome the situation as fast and as good as possible. From the legal perspective, innovations have been made and countries are now recreating their policies to adapt to the new scenario. Press releases, statements, uncountable meetings are marking this year in which international cooperation has been the game-changer.

Still, a clear legal framework needs to be enforced to contribute to the fight against the virus, guaranteeing the protection of fundamental rights. Said that, the European Union since 2016 created the General Data Protection Regulation[145] providing general regulations, so countries can follow it accordingly.

The GDPR was conceived to provide a more integrated regulation to the countries parties of the European Union(27 countries) plus Iceland, Liechtenstein, and Norway, representing the European Economic Area (EEA). It proved to be useful in regulating the personal data process in a health crisis but also leaves open some part of the task to the national legislation.[146] As some of the issues are left to national countries to decide, there are still many diversion in the legal framework to manage data sharing during a health crisis.

Whenever a state requires the use of data health to solve a health public emergency some requirements need to be met, so the state can modify laws and regulation skipping some decision-making steps to achieve a quicker response.

145 From now will be addressed as GDPR.
146 Becker, R., Thorogood, A., Ordish, J., & Beauvais, M. J. (2020). COVID-19 Research: Navigating the European General Data Protection Regulation. *Journal of Medical Internet Research*,*22*(8), e19799.

However, this does not allow any unlawful decision or rule to become legal or to delete or suspend fundamental rights.

It is also important to clarify that some fundamental rights can be mitigated in case of health public emergency, as for example, we have already experienced the restriction on freedom of movement in some countries in order to contain the virus. Undeniably the use of tools during public emergencies states need to be supervised and only used if extremely necessary.

Indeed, there are some studies informing that the information of people who were infected, if they proceed with personal interviews, the state would have in hands "identifiable data"[147] or at least a set of people that might have been identifiable for being in proximity with an individual that was infected. This fact, generates issues and can represent a threaten on the population's eyes. Reason why, at this moment, the recently adopted GDPR is having its first crucial test.

5.2 Article 6th as legal basis for processing data based on public interest

Given that, following the GDPR requirements, countries need to comply in order to implement a state of emergency. The first part of the article 6 is described as it follows:

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> 1.the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> 2.processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> 3.processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> 4.processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> 5.processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

For many times the regulation within the EU overlaps other regulations when it comes to data process, however many more other national regulations still leave gaps

147 Bradford, L. R., Aboy, M., & Liddell, K. (2020). COVID-19 contact-tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes.*Journal of Law and the Biosciences*.

for research and data process interpretation. The legislation however requires that the data processing should only be done when the interest is legitimate and do not nullify fundamental rights. The point 6, stresses also the use of the data processed by a third party and when the subject is a child.

The legal Analyses of the points below provides us with general rules to the use and process of health data, can be done also with consent, respecting the imbalance of the data controller and the patients. Patients might be seen as a vulnerable part and the data can be used as long as there is no more disadvantages to increase the imbalances. [148]However, the consent can be withdraw at anytime and the individual's right must be protected, regardless the previous consent.

Going further with the legal analysis, Article 6 also states that specific modifications can be done by states to adapt to the need of the situation that has been faced:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
> Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

The consent to the use of data in health research is still a challenge - considering that most of the hospitalized patients are probably in critical health status and approaching them to get more information could also be problematic (apart of the overload of work on health carer shoulder's)[149] it's a painful requirement to deal with until another solution is available to avoid as much as physical contact as possible. This

148 Becker, R., Thorogood, A., Ordish, J., & Beauvais, M. J. (2020). COVID-19 Research: Navigating the European General Data Protection Regulation. *Journal of Medical Internet Research*, *22*(8), e19799.
149 Ibid, p.2.

type of consent can be given for example by ticking a box when visiting a website, choosing certain technical settings or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing. Pre-ticked boxes or inactivity by the data subject do not constitute consent.[150]

In implementing the data collection, the state needs to meet the requirements described bellow in order to c demonstrate the public interest in all the operations made by the controller.

1The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
1. Union law; orMember State law to which the controller is subject.
2 The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
3 That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX.
4 The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

The GDPR needs to manage the consent requirement and the public interest requirement must be provided by the law. Apart from that, the countries also can design regulations that are more effective to their realities and can be useful in our context, however, it still leaves a place for misinterpretation and different standards between countries. Obtaining consent[151]to further data processing with the purpose of research, is one of the legal basis for processing data during COVID-19, however the limitations are still vague and it is necessary to obtain consider from the subject beforehand, nevertheless the right to withdraw the data also needs to be permanent.

150 Recital 32, EU GDPR.
151 Article 6, GDPR.

After the withdrawal of consent, the data must be deleted and the processing of it can only be done if there was already a regulation to guarantee the lawfulness of the content. This can also represent instability to ongoing research that depends on the collection of data and continuous analysis. This type of research will be affected by the limit[152] of consent, but the individual retains all the right to its data, and the responsible for the research can not mitigate this right, even if the public interest is involved, as in the case of the COVID-19 pandemic.

The present pandemic, it is without doubts, a public emergency, hence it is intuitive that the data collected during the pandemic can be used for research purposes, giving the countries a bit more of flexibility to process this data faster and favoring the public interest. In this regard, the GDPR[153] suggests that the laws should be made nationwide, as a result the states could design an unique regulation to their best interests.

The European Data Protection Board stresses that only consent would not be the optimal bases for public authorities to use the data, however it has not presented different options to modify the laws.[154]This affirmation lead developers to design the notification apps based on voluntary use mostly, however the GDPR reinforces that country should beforehand have the legal basis of what it is considered as public interest or vital interest to avoid that private companies would use it to different purposes claiming shallow reasons to use the data.

Therefore, some basic requirements are enshrined in Art. 6:

2.Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a

152 Becker, R., Thorogood, A., Ordish, J., & Beauvais, M. J. (2020). COVID-19 Research: Navigating the European General Data Protection Regulation. *Journal of Medical Internet Research*, *22*(8), e19799.

153 Article 6.3, GDPR.

154 Bradford, L. R., Aboy, M., & Liddell, K. (2020). COVID-19 contact-tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes.*Journal of Law and the Biosciences.*

democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

1. Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

2.The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

3.The nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

4. The possible consequences of the intended further processing for data subjects;

5. The existence of appropriate safeguards, which may include encryption or pseudonymisation.

The purpose of the data collected needs to be aligned with the initial data collected and different requirements are still needed to process the personal data. The main requirement is to protect a democratic society which companies should not develop software that are able to track individual's movement within the city to any other different purpose other than the public interest.

Nevertheless, within the consent criteria it is also necessary to write the privacy terms in a "clean" way that can be understood[155]. Most of the initial terms in privacy policy start with the affirmation: "your privacy is important to us", some psychological studies has shown that when the privacy policy start with these words, it is more likely to get the acceptance of the user.[156] As explained by T. Mulder & M. Tudorica[157] in their paper, 2 out of 3 privacy policies are written in English, which might cause some distortion with the original document but there is still not many studies explaining the correlation between the language in which the policy is written and the user acceptance.

The requirements of consent and clean language are the bridge to give more transparency in the whole data collection procedure. Identifying since the beginning of

155 Article 7 (2) GDPR.

156 T. Mulder & M. Tudorica (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, 28:3, 261-274, DOI: 10.1080/13600834.2019.1644068 and 3Article 12 GDPR.

157 Ibid.

the procedure who is the person to be hold accountable for the storage data, the consent, transparency are all basis for a maintaining a democratic society, however there are still gaps in the legislation that will be discussed in the next chapters.

In addition to the others requirements, transparency is also enshrined in the GDPR, Articles 5 (1, a) and 12 that states that any personal data should be processed in a transparent manner. Not only a requirement but also a principle that the state needs to comply to build the basis of a democratic society, as transparency as principle needs to be in any government decision, if the state shall protect the citizen's right to privacy.[158]

In a way, transparency also means to monitor what the government does, ensuring to the citizens power to protect themselves and hold governments accountable whenever the politicians positively act or omit themselves which avoid public abuse of power to enable the citizens to trust their leaders.[159] All along with the pandemic, some countries are experiencing total lack of confidence in their governance immediately not only regarding transparency but involving all spheres of public states.

Despite of being necessary to most of the government actions, transparency can also be relative[160], as some actions shall be confidential given to the public best interest and even if totally transparent there still will be gray areas of non-complete transparency. However, the principle is frequently discussed, as being totally transparent also means more expenses to be covered.

The ECHR jurisprudence has interpreted Art.8(2)[161] to mean that, regardless of the end to be achieved, no right guaranteed by the Convention should be interfered with unless a citizen knows the basis for the interference through an ascertainable national

158 Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?.

159 Brin, D. (1998). The transparent society. Will technology force us to choose between privacy and freedom? New York: Basic Books.

160 Ibid.

161 Available at: https://www.echr.coe.int/documents/guide_art_8_eng.pdf Accessed on 11/11/2020.

law.[162] This rule is also correlated with the premise of consent and also with the principle of transparency.

Concerning health-related data, the GDPR needs to afford the subject to the information of who holds the data, who process the data, which purposes, until which extent, risks, rules how to access the rights[163]. In a state of emergency is also necessary to inform the duration to storage the data and withdrawing and posterior erase of the information, also defined as the right to be forgotten.[164]

In case of data health breach is stressed on article Article 34 GDPR that in case it is *"likely to result in a high risk to the rights and freedoms of natural persons"* the data controller should inform the individual in undue delay[165]. The discussion regarding the type of data breach can also occur trough illegal data market, situation that has been more and more common in the last years that with the pandemic, gained the highlights regarding data regulation.

As another requirement and one of the most important regarding health data is the anonymisation of the data collected. Many countries in Europe as mentioned before, are using Google and Apple proximity technology and claiming that the data collected can not be identified, independent if at some point the subject was tested positive and that any other information, as for example, geographical data can be identified, as the geodata can be very specific, some studies claim to be possible to identify subjects crossing information and stealing vulnerable data.[166]

---

162 Malone v United Kingdom, 1984); Leander v Sweden, 1987

163 Ibid 32.

164 The right to be forgotten has been used by courts to base the decision of guaranteeing citizens to obtain the erasure of their data. E.g Google x Spain available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0131. Accessed on 11/11/2020.

165 The ECJ decided that the term "without undue delay" *was not compatible with a time limit of several weeks or even, as in the present case, several months, given its customary meaning in everyday language* (ECJ, judgment of 05.09.2019, C-443/18, recital 38).

166 Available at https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/ Accessed on 11/11/2020.

The data collected should be anonymised by decentralization of the data or at least be "pseudonymised" a term defined by the article 45 of the GDPR: "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*.

Google and Apple already have been trying to comply with the GDPR principles, double checking the data processing to avoid any individualization of the data, in a manner that the information can not be attributed to a specific individual.

5.3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

As part of the European legal framework in Data Privacy and communications, the " E-Directive" aims to respect the fundamental rights and principles of the Charter of the fundamental rights of the European Union, particular the ones stated in the Articles 7 and 8 of the Charter.[167][168] The most important objective of directive is to protect the processing of personal data and free data movement within the community, ensuring that their fundamental rights and privacy rights are secured[169]

The directive ensures very important rights, including the right to confidentiality of communications, in article 5th in which the directive requires the states to provide the

167 Article 2, Directive 2002/58/EC.

168 The *A*rticle 7 recites that everyone has the right to respect for his or her private and family life, home and communications, and the Article 8 states that: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

169Article 1 E-Privacy Directive.

publicly of the confidentiality of communications and traffic data by national law.[170] Furthermore, the directive also ensures that no data, communication or data traffic, shall be used by other parts than the subject, unless permitted by law. Another provision is that any type of surveillance, tapping[171] or storage is prohibit without consent[172].

7. 4 The Universal Declaration of Human Rights and The International Covenant on Civil and Political Rights as legal framework to Data Privacy.

The Universal Declaration of Human Rights in its article 12 provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Apart of the European Union legislation, data privacy is also protected as a fundamental rights and meanwhile, the International Covenant on Civil and Political Rights[173], provides in article 17: "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation" and further states that: "everyone has the right to the protection of the law against such interference or attacks."

As International Covenants, the ratification of both documents ensure the protection of data privacy and the protection of the law against interference or attacks. This premise can be provided by different manners, however the state through National Law must inform the consequences of unlawful actions or abuses. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws[174] that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific

170 Taylor, M. (2006). The EU data retention directive. *Computer Law & Security Review*, *22*(4), 309-312.
171 Interception of telephone communication by a third party often by covert.
172 Article 15(1) E-Privacy Directive.
173 From now on wards, CCPR.
174 The Right to Privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, 30/06/2014, available at: https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc. Accessed on 12/11/2020.

legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.[175]

The Rules contained in the framework of legislation mostly ensure the same basic principles in order to process data and the above mentioned two documents are cross-borders legislation that also provides citizens with the right to an effective remedy in case of abuse, article 2, paragraph 3 (b) oc the CCPR requires that States parties to the Covenant "*to ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy*". In the general comment No. 31[176] of the Human Rights Committee and in other decisions, the Committee reiterated that States must also ensure that the competent authorities enforce the remedies whenever addmitted and that the failure in investigating could lead to a breach of the Covenant.

5.4 Guideline on 04/2020 on the use of location data and contact-tracing tools in the context of the COVID-19 outbreak.

Italy as a country part of the European Union, needs to comply with the Data Privacy rules enshrined in the General Data Protection Regulation from 2016[177] and on 21th of April, 2020 the European Union, In light of the GDPR regulations and in the attempt of creating a common strategy, adopted the "Guideline on 04/2020 on the use of location data and contact-tracing tools in the context of the COVID-19 outbreak".

175 European Court of Human Rights, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984, paras. 67 and 68.

176 General comment no. 31 [80], UN Human Rights Committee (HRC). The nature of the general legal obligation imposed on States Parties to the Covenant. 26 May 2004 Available at https://www.refworld.org/docid/478b26ae2.html. Accessed on 12/11/2020.

177 Available at : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN Accessed on 25/10/2020.

Article 2 in the introduction and context section, reaffirms that given to the increase of data driven approach, it is necessary that the countries provide an effective response, protecting freedoms and fundamental human rights.[178]

Article 4 states that any measure should be taken in the use of the principles of proportionality, effectiveness and necessity. Rather than stigmatize, the measures should leverage the fight against COVID-19 and should empower individuals, and not control them. The main purpose of the guideline is to provide guidance for the use of location data tools: The tools should be used only with the purpose to estimate the spread of the virus and to assess the confinement measures; contact-tracing aiming to notify people that have been in close contact with individuals that have tested positive for COVID-19.[179]

The guideline explains the type of technology that it is currently used by countries to collect data from the citizens and it can be: location data collected by telecommunications services and location providers as navigation and location services.[180] One of the most important rules is enshrined in the article 10, that explains the rules contained in the E-privacy Directive[181] that the information can only be shared to the authorities or third parties, in case the data is anonymised by the provider, the users consent needs to be taken beforehand.

Moreover the guideline comments the findings of a large body research stating that some studies has showed that even if anonymised, eventually the location data as mobility data is very unique, tit can be vulnerable[182] and allow the individual's identification[183]. Which corroborates with the premise that a legal framework needs to

178 Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. Accessed on 26/10/2020.
179 Ibid, p.2.
180 Ibid, p.5.
181 See Art. 2(c) of the ePrivacy Directive.
182 Pyrgelis, A., Troncoso, C., & De Cristofaro, E. (2017). Knock knock, who's there? Membership inference on aggregate location data.*arXiv preprint arXiv:1708.06145*.
183 This type of technology can be used to predict visit to business at certain times which it is helpful to avoid crowds during the COVID-19 pandemic.

be precise in protecting the citizens identities, not only during emergencies but also during non-critical times.

In articles 27 onward, the guideline explains the use of contact-tracing app and how it should be designed the defaults settings regarding the data privacy terms:

> In the context of a contact-tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default: contact-tracing apps do not require tracking the location of individual users. Instead, proximity data should be used; as contact-tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification; the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.[184]

The article clearly states again the principles of transparency, necessity and the need of being anonymised data.

Regarding the use of location data, the guideline, as can be seen in the article mentioned above, argues that should be used proximity data instead of location data, as the main core of the applications is to notify proximity and not location. This argument is reasonable, as one of the biggest concerns during the pandemic is to protect the freedom of movement[185] in general, avoiding controlling the movement of the population. With exceptions of some nations, most of the countries had declared full lockdown in the early stages of the pandemic, which requires a huge sacrifice as movement of freedom is still one of the basis of a democratic state and the rule of law, hence going backwards to the same situation, should be avoided, however can not violate other fundamental human rights[186].

As any other measure needs first to have legal basis, the guideline also explains in which basis the applications must be done. The article 29 stresses that the consent

184 Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. Accessed on 30/10/2020.

185 Calzada, Igor, Will COVID-19 Be the End of the Global Citizen? (March 20, 2020). Calzada, I. (2020), Will COVID-19 Be the End of the Global Citizen? Apolitical. , Available at SSRN:https://ssrn.com/abstract=3558029.

186 https://www.un.org/victimsofterrorism/sites/www.un.org.victimsofterrorism/files/un_-_human_rights_and_covid_april_2020.pdf Accessed on 30/10/2020.

usually won't be the basis for functioning the application, however the voluntary participation needs to be met in order to guarantee the legal basis. Also, the authority that will hold the content of the data needs to be specified, informing who will be held accountable in case of violations.[187]

The principle that is remarked at the article 29, consists in the action in the name of the public interests and strictly to this purpose, circumstance that do not correspond to this, the authorities need to ask for consent of the user.[188] This requirement is also enshrined in the Article 6(1)(e) GDPR.[189]

Regarding health data management, the guideline at the article 34, makes reference to the Article 9(2)(j) GDPR, and also allows health data to be processed when necessary for scientific research purposes or statistical purposes[190].*"The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates"* statement of the guideline that represents a clear fundamental base that governments should follow when enforcing applications that requires data collection. The main idea on having a guideline to prevent violations it is to enforce the principles and to have a common understanding of policies to be followed.

As mentioned trough out this work, the sensitive content of health data should be protected and shared only with the consent of the individuals. Apart of that, any discrimination caused by health status should be avoided, and the emergency can not be an excuse for violation of fundamental rights.

Moreover, the guideline also states that: "*Storage limitation should consider the true needs and the medical relevance(this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only*

187 See Article 28, Guideline contract tracing COVID, 2020.
188 Ibid.
189 https://gdpr-info.eu/ Accessed on 30/10/2020.
190 The guideline however does not specifies the type of research that allows the use of the data. This could be pointed as a gap in the recommendations, however as the pandemic is new in all senses, in the near future the guideline should be updated with the requirements and context that should be considered to allow the use of health data.

for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymised."[191]

The guideline describes the legal analysis for the apps, explaining how the applications should be used and how the authorities need to be accountable to ensure the rights of the citizens. At point 24[192], it is possible to notice the concerns of the board about the fact of using the app, cannot cause disadvantages to those who will not use it. Another argument raised by the board is that the voluntary use of the app implies that individuals that refuse to use the tool, can not suffer any disadvantages based on their decision.

This could also be an argument regarding old people or marginalized groups. In the case of marginalized groups, it is already a fact that the pandemic is enlarging the social-economic gap in our society and so far, technology can be used in the fight against COVID-19 by developed countries, however, developing countries are still facing different fights that cross over the pandemic layer. In other words, the use of technological tools could increase the imbalance between the nations, therefore it could be seen as an opportunity to develop solutions based on the SDG goals that can help communities to recover and explore mechanisms that can promote equality to all men, as enshrined in article 7, of the Universal Declaration of Human Rights.[193]

Continuing the comments about the legal analysis in the guideline, one of the basic content of the use of any location data or proximity data is the definition of which entity will be responsible for collecting and managing the data. So far, countries are holding health authorities as the legal responsible for managing, storing and if necessary, sharing the dataset.[194]

191 Articles 34 and 35, Guideline contact-tracing app, COVID-19.
192 Ibid. p. 7.
193 https://www.un.org/en/universal-declaration-human-rights/ Accessed on 01/11/2020.
194 Guideline contact-tracing App, COVID-19.

Moreover, in case it is necessary different actors to play this role, each one of the actors must be specified and clarified in the document used to enforce the principles and rules the app will be developed and the management of the storage data.[195] All the actions that can and should be deployed by these actors must be informed and explained to the users. Also, attending the principle of purpose, the final objective of the measurements should be clearly stated to avoid gaps and other types of misinterpretation that could lead to extending the use of the applications for others purposes other than combating the COVID-19 pandemic.

Theoretically, the users should be guaranteed that the applications are serving to the only purpose of mitigating the spread of the virus, working together to protect health-related needs and our data privacy in order to prevent abuse of power by the governance and implementing safer policies that can be reliable and effective.

The legal basis for storing data should be the article Art. 6(1)(a) and art. 9(2)(i) GDPR to manage all the data concerning health status, in case of health public emergencies and only for the public interest purpose to ensure that strict requirements are met. Apart of the European Union legislation, some states are also part of other international conventions that should be respected and they will be mentioned moreover in the next chapters. [196]

Having strict and clear requirements for the use of data health is crucial when it comes to prevent human rights violations and guarantee the well function of the rule of law whenever there is an health public emergency. As the pandemic happened in a very fast pace, can be affirmed that most part of the countries were not ready to a rapid response in any of the necessary levels: not on the social level, not in the economic level, and consequently not even from the legal perspective[197].

195 Ibid.
196 Ibid.
197 Golinelli, D., Boetto, E., Carullo, G., Landini, M. P., & Fantini, M. P. (2020). How the COVID-19 pandemic is favoring the adoption of digital technologies in healthcare: a rapid literature review.*medRxiv*.

Some countries have already very well structured laws and regulations that can lead to an effective implementation of digital data on health, however, many countries are still developing slowly a digital health legal framework. The situation can be eventually more challenging if there is a lockdown, as no meetings are allowed, the discussions to edit or to create new regulations can become slower even if the country is still operating in the public emergency state.

Regularizing a subject that is still an unknown field is very difficult, specially if technical knowledge is necessary, hence, states should only rely on trustworthy sources to implement an action plan that legitimately can offer effectiveness and legality[198]. Also, considering the opinion of different stakeholders, can increase the liability of the regulations.

Along the following points after the 24th point, the guideline clarifies that the data might be processed with the purpose of research or statistics[199], however it can only happen if the data is processed during the COVID-19 crisis, taking into consideration true medical reasons, and if afterwards, the data should be anonymised or deleted. Those considerations are made given to the fact that the digital tools can not be an excuse to storage data permanently, but also taking into account the the data is helpful for estimating new cases and hotspots.

Not only a matter of regulation, the necessary clarification for the use needs to comply with internationals and nationals law, hence, the guideline recommends that the contact-tracing should not only be automated[200] but only one more support for health authorities to contact people who have been in proximity with people who tested positive for the virus. This procedures should be mainly human-driven that work closely with qualified staff to avoid false positives.

198 De Hert, P., & Papakonstantinou, V. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably un agency. I/S: Journal of Law and Policy for the Information Society, 9(2), 271-326.
199 See points 34 and 35 of the Guideline for contact-tracing app, Covid-19.
200 Ibid.

The guideline also highlights the importance of having a risk assessment before implementing the application. Apart of that, the guideline explain both technical and legal practical actions that should be provided. The Algorithm should regularly be reviewed, aiming to reach accountability, fairness and compliance and the this review should be made by independent experts. From the technical point of view, the codes should also be open source, grounded on the principle of transparency.

It is well known that false positive cases will be certain, therefore measures to mitigate it should be applied retaining false positives to the minimum as possible. The collection of data should follow the principle of data minimization, and never be related to not needed information, as civil status, messages, call logs, location data, device identifiers. These security measures should be contained in the default settings.

Last point highlighted in the guideline: *The reporting of users as COVID-19 infected on the application must be subject to proper authorization, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status. The controller, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national contact-tracing app in order to mitigate the risk that individuals use a third-party app.*[201]

Avoiding frauds, the notification to self isolate should be only permitted with a code or through the confirmation of a health authorities to guarantee that no false positive notifications[202] will be sent to other users as it can affect individual's life directly. The recommendations contained in the guideline are general comments to be observed, however the design of the regulation should be done at the member state level and be adapted case by case to better adequate the terms to each scenario.

201 Ibid.
202 Ibid.

6. General Risk Assessment for the use of Digital Health Technology

The main measures used in the COVID-19 pandemic has brought innovative tools that are often linked to new technologies, some countries are leading the race, as they have more capital to invest on it, while other countries, already behind the more developed countries, are struggling with the added problems that the COVID-19 has brought into the world. Regarding the analyses of such subject, it can have multi faced perspectives but will always been connected to political and economic views, specially in the current pandemic, as the whole world is facing the same threat but defending themselves with different tools.

Obviously the pandemic not only brought damage but proliferated the creation of other business types – already pushing forward some advanced technology- that otherwise would have taken more years to become reality. However, the main point of discussion in this Master's thesis is in which sense these new digital health technologies can affect Data Privacy as a Human Rights. There are many different levels of human rights and the pandemic also has shown the vulnerability of those rights – the worlds surely is going trough deep transformations in all aspects of lives and once again, it is experienced the importance of protecting and providing freedoms, rights and privacy.

After almost a whole year facing the pandemic, some countries have changed a lot its usual social-economic function manner: from teleworking to telemedicine, to drone surveillance to zoom meetings – to warm human contact to social distancing. However so far, there is no real answer in what is the best way to combat the pandemic, as in any other matter, different solutions apply to different countries. Regardless the need of the countries individually, basic human rights, international cooperation and freedoms must be priority in this moment.

Some human rights can be mitigated under laws that permit sort of interruption of this rights, as for example, the freedom of movement when most of the countries under the legal basis of state of emergency implemented quarantine to the citizens to stop the

rapid spread of the virus, aiming to relief the health system. However, simple principles should be taken into account and only during the necessary time to fight the virus. It is when the problematic starts : there is no prediction for the duration of the pandemic, people are been vaccinated in some countries but so far, there is no clear guarantee for how long this pandemic will last and what will be the aftermath.

Aiming to clarify and stand up for human rights, it is necessary to safeguard principles, can be ethical principles or legal principles, together they are main actors to guarantee not only data privacy but other rights, as right to work, right to health, access to education and many others.

As a characteristic of this pandemic, the decisions were taken too fast and also the whole path of spread was to fast, but from a argumentative point of view, can now the measures be more analyzed without the fear of failure? Are we still in the same start point or now governance is more decentralized and more effective in maintaining a standard level of protection to the population?

These questions might only be answered in the years ahead, nevertheless the discussion surrounding the legitimacy of the use of digital data health needs to start now to raise awareness and prevent more damage to the world population. The pandemic affects people differently but everyone suffers its affects.

The legality and ethical issues are relevant and will undergo modifications as long as the use of digital data health will be contiguous – as mentioned there is not really a prediction for how long they will last but most intrusive ways of digital health, as for example, temperature measurement in stores, trains or other public spaces – possibly will finish. In a nutshell, the thesis intends to discuss other types of measures – contact-tracing apps, QR health codes and other interactive solutions that could represent data privacy threats or mass surveillance to citizens.

With the pandemic, our lives became more virtual – and all levels of the society has been affected by this reality shifting – at the moment, from regular classes to high-level political decisions are made via internet through private platforms. Hence, our data health has also become the center of this new reality. However are the governments, the legal framework prepared to tackle with the social, ethical and legal challenges that these new technologies are requiring? And in the long run? Will they enhance our democratic sates or introduce big data surveillance to citizens?

The experimental nature of the new digital health technologies are in fact very problematic and governments are incorporating the private sector and each country has engaged envisioning their own approaches, however mostly using the GAEN technology which represents already two issues: the fact that there is no common approach, within the European context, so far, the initiative to promote a common app for the EU area is small.

Also using the same technology from the monopoly Google/Apple might not be the best approach as concentrating all sensitive data that has been collected in one single private hands can lead to leak of data and unsupervised data use, also together with a weak legal framework can result in serious damage in the long term run. For example, during the first wave of the pandemic, the Governor of the Veneto Region in Italy suggested the privacy laws could be suspended to contain the spread of the virus by the use of digital mass surveillance.[203]

According to the European Convention on Human Rights[204], the International Convention on Civil and Political Rights[205](ICCPR) and the United Nations Siracusa Principles[206], the measures during a health emergency must be proportional, necessary, scientifically valid and temporary. Moreover, the mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of

203 Available at https://www.repubblica.it/politica/2020/03/26/news/zaia_sospensione_privacy-252373104/. Accessed on 06/01/2020.
204 Available at https://www.echr.coe.int/documents/convention_eng.pdf. Accessed on 06/01/2020.
205 Available at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. Accessed on 06/01/2020.
206 Available at https://undocs.org/pdf?symbol=en/E/CN.4/1985/4. Accessed on 06/01/2020.

Health-Related Data, released in 2019 also provides guidance on the purpose, the legal basis and the handling of health-related data[207].

The legitimate use of data is describes as follows in the point 4.2 of the recommendation of the protection and use of health-related data:

> 4.2 The legitimate purposes for processing health-related data are: a. where there are or will be direct benefits to the data subject such as health diagnosis, care, treatment, rehabilitation and convalescence of the data subject; b. preventive health purposes and purposes of health diagnosis, administration of care or treatment, or management of health services by health workers, subject to the conditions provided for by law; c. reasons of public health, for example mandatory notifiable diseases, protection against health hazards, communicable disease identification and containment, environmental hazards, humanitarian action or in order to attain a high standard of quality and safety for health treatment, protection against health products and medical devices, subject to the conditions provided for by law; d. the purpose of safeguarding the vital interests of the data subject or of another individual where consent cannot be collected from the data subject, the other individual, or both; e. reasons relating to the obligations of controllers and to exercising the rights of the data subject regarding employment and social protection, in accordance with law or any lawful collective agreement; f. the public interest in the accountability of the planning, funding and management of the healthcare services, management of claims for social welfare and health insurance benefits and services, subject to the conditions provided for by law; g. processing for archiving purposes in the public interest as defined by law, for scientific or historical research purposes assessed with reference to the role of the legal entity carrying out the activity, the role of the individual(s) carrying out the activity, quality standards including use of scientific methodology and scientific publication or statistical purposes subject to the conditions defined by law in order to guarantee protection of the data subject's fundamental rights and legitimate interests (see in particular the conditions applicable to the processing of health-related data for scientific research under Chapter IX); h. reasons essential to the recognition, exercise or defence of a legal claim in relation to the health-related data intended for data processing; and i. reasons essential to the identification of missing persons, or the location of a missing person, where there is no reason to believe that the individual said to be missing merely wishes to avoid contact, and the circumstances of the person 10 being missing raises concerns for their safety and well-being, on the basis of a law which provides for suitable and specific

207 Available at https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/FINALHRDDOCUMENT.pdf. Accessed on 06/01/2020.

measures to safeguard the fundamental rights and the interests of the data subject and their relatives.

The legal framework presented in the previous paragraph provides similar purposes and principles for a lawful health-related data processing. During the pandemic, the states are in different levels of existent legal framework, however the international legal framework is valid as a guidance to the countries that can not yet achieve the same level of data protection as developed countries.

From the legal perspective, the essential goal at the moment is to raise awareness and call upon states to be more transparent and proportional in implementing the measures to contain the spread of virus, also discuss the current challenges, as contact-tracing apps, cross-border data processing, centralized data and the lack of open source. Around 40 countries are using the Google/Apple exposure notification technology.[208]

After the scientific community identifies gaps, promoting more engagement from states to enhance the laws aiming the long term solutions and avoiding the use of intrusive measures to become permanent, simultaneously preparing the legal framework to the future challenges. Some countries are moving forward to implement permanently the use of the contact-tracing apps for different purposes. Singapore for example, has announced that the police will be allowed to use the contact-tracing data to criminal investigations.[209]

Providing a risk assessment for the different layers surrounding the use of digital data health it is indeed very difficult as it can be a very broad subject with many crossing subjects, however some aspects of the use of digital technology has already been discussed for this first year in the pandemic scenario.

208 Available at https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/. Accessed in 06/01/2021.

209 Available at https://www.reuters.com/article/us-health-coronavirus-singapore-contact-idUSKBN2990X8. Accessed on 06/01/2021.

Since countries have a different legal framework, more has been discussed regarding the ethical principles that should be bear in mind while deploying the use of technology in fighting the pandemic. First of all, ethical principles are largely applied and must be present in any decision making process and regarding the use of new technologies, many initiatives already have been created to support the simultaneous growth and development of an unique framework for the use of AI, obviously that would be an optimal virtue of the international cooperation, but so far, it is a goal that has not been achieved yet[210].

Taking it into consideration the fact that there is no unique framework to rely on, the best option to the actual governance it is to comply with the regulations that are present in the domestic and international level and assess future implementations of more reliable laws. That said, first point to be analyzed is the proportional use of a measure: It should be provided by law before hand, as can be seen, many countries have approved amendments in its law to be able to start the use of digital health technology[211] and any measure must be proportional to its purpose, in case of the contact-tracing apps, they should be used only and during the pandemic, the app should be time-bonding once the number of new cases are under control, its use should be suspended.

The governments shall bear in mind the original reason why the measure is being implemented which It is to contain the spread of the virus, once this goal is achieved, the governs should assess the service and stop the use of the measure. This is the starting point of data protection as human right, when the limits are determined, should be more uncomplicated to prevent breaches and enhance the data protection. Not only to set up a duration for the implementation but also frequently reassesses the need or the manner the measure has been conducted. The government should also incentive stakeholders to conduct aside tests/assessments and open calls for inputs that will

210Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689-707.

211 For example, in Italy : https://www.jdsupra.com/legalnews/italian-data-protection-authority-s-62316/, Accessed on 08/01/2021 and In Switzerland: https://www.thelocal.ch/20200609/swiss-parliament-approves-coronavirus-tracing-app. Accessed on 08/01/2021.

strengthen the relation between government and society plus, enhance the effectiveness of the measure.

Monitoring and evaluation of the measures should address the failures and enhancing of the mechanism, however would be more effective to enforce oversight laws and demand more technical response, this would enable both tech driven approach and urgent need to benefit and build trust along the years. The challenge at stake [212]is to balance the proportionality of the measures, sync those measures with the legal framework, prevent harm and effectively help in containing the virus. Consider what it is needed from time to time will moreover bring better results, than interpret the situation only trough one point of view.

The benefits of digital data health are somewhat proved to be effective, however even being in a state of emergency, the measures applied today could possibly bring more trust, although it is encountered not only by the introduction of innovative initiatives but also explaining how the community and individuals will benefit from digital data health development.[213]

Apart of the proportionality of the measures, they must necessarily be transparent, as mentioned in the previous chapters, the content, the purposes, the data handling and controllers, plus the possibilities of redress in case of harmful data leak or misuse should be clarified to the users and trough completely transparent data processing.

As data health is considered that makes more likely to have hack attacks and can be revealed even with anonymisation[214] of the database, consequently, the principle of transparency also links the governance[215] approach to the scenario, as establishing a transparent governance regarding data processing will ensure accountability, and

212 Vayena, E., Haeusermann, T., Adjekum, A., & Blasimme, A. (2018). Digital health: meeting the ethical and policy challenges.*Swiss medical weekly*, *148*, w14571.
213 Ibid.
214 Cho, H., Ippolito, D., & Yu, Y. W. (2020). contact-tracing mobile apps for COVID-19: Privacy considerations and related trade-offs.arXiv preprint arXiv:2003.11511.
215 Urs Gasser,Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy, 130HARV.L.REV.F.61 (2016).

legitimacy, both requirements to pursue democracy and the rule of law. This is also one of the big challenges of the pandemic, all at once, the pandemic disposed basic freedoms and rights and at a global level which the effects will be for years calculated and surely the pandemic already has created a revolution in our lives.

Given to that, governments should play a bigger role – more innovative, keeping in mind the long term results and achievements. The institutionalization of the contact-tracing apps for example, could be designed considering privacy as the priority with the only purpose of avoiding the spread of the virus and not cause more inequalities within the already so divided society. It should be improved the best practices and incorporated to the national and international laws[216], avoiding misinformation and any misuse of data would undermine the category of data processing.[217]

The principles of proportionality and transparency should only bear very strict restrictions to support their fundamental base for the protection of human rights, the laws should be designed aiming to achieve a high standard of protection and hold companies accountable for unethical or illegal behavior. Additionally[218], the states should also invest in research and improve the technical skills of their own organizational matters, before blindly trusting sensitive data to the private companies. This would exponentially improve governance, also ensuring mandates to independent organizations to investigate and promote lawfulness, transparency and fairness in Cybersecurity.

216 Available at https://algorithmwatch.org/wp-content/uploads/2020/10/Governing-Platforms_DSA-Recommendations.pdf. Accessed on 11/01/2021.

217 The pandemic represents a milestone for the international legal framework for Data Privacy as in short time, many guidelines, laws, reports and all sorts of spaces to share information are been released month by month which has just confirmed the already existent necessity to fill the gaps the world was facing in regard AI.

218 Ibid. The Article reports some points to be consider in order to promote fairness and lawfully within cybersecurity. The promotion of lawfully data processing should not only be based on the legal framework but should also be explored and engaged within the digital workers. In the future, law-making and AI will be more and more linked and professionals that can cross both subjects will be necessary to keep the development of these subjects, creating a balance that now it is already missed, as one side is growing much faster than the other while the law making are still engaging in discussions and not in enforcement and innovative laws.

With more proportional and transparent laws, the measures will ensure the fairness in the use of digital data health and tech-driven approach. What can be seen in the word it is what can be called the technological division, one of the biggest problems in implementing digital health technology and not taking into account how much unevenness it could cause in the long run.

Despite of being a basic service in developed and developing countries, only the half of the world population[219] has access to internet which leads to the fact that any measure based only on the internet or mobile phones, in some countries will not be an inclusive measure and will contribute to the increasing of the inequality gap. This is also a concern in reference to contact-tracing apps, the apps should not be the only manner to contact trace individuals that have been in contact with individuals that tested positive for COVID- 19.

Considering social-economic differences, law-makers should not engage in measures that are unfair to the population, enabling only digital contact-tracing will not ensure that people with little to no digital literacy would be included into this and will contribute to social unfairness. Also, internet based measures can raise the inequalities for vulnerable groups in the society.

The aftermath of the pandemic can not yet be completely measured but it is an on going monitoring of the impacts in the society, however some of the predictions are not really encouraging the development of economy but in reality is more harmful and affect all layers of the society. Given to the fear of going backwards, many technologies has been deployed in a rush, without proper evaluation and risk assessment in a attempt to find solution to the current crisis, avoiding a even bigger recession.

Interesting argumentation presented by Ciro Cattuto and Alessandro Spina[220] stressing that not always the digital path is the best way to approach the fight against the

219 Available at https://ourworldindata.org/internet. Accessed on 11/01/2021.
220 CATTUTO, C., & SPINA, A. (2020). The Institutionalisation of Digital Public Health: Lessons Learned from the COVID-19 App.*European Journal of Risk Regulation*,*11*(2), 228-235.

pandemic. The researches explain that it could be a misconception that can potentially lead to the acceptance of intrusive measures and digital surveillance. Their argument is based in the non-prooved effectiveness of the contact-tracing app[221] and the rush to implement measures without publishing risk assessments and results of effectiveness. Additionally the researches argues that there are not enough studies demonstrating the effectiveness of the app, as also they are recently being used to mitigate the spread of the virus. Instead, they are in favor of implementing more fair policies that can reach the society equally.

Together with social equality another issue can be analyzed is the acceptance of digital health for low-medium incoming countries. As can be noticed, developed countries can be first in the technological race and open calls for private companies that are developing software. However, as some researches has shown, the current digital health it is based in data and the decreasing[222] the cost of digital health technologies could engage in making it available for the low and middle income countries. The policy-approach should envisage this inclusive policy as a mid-term goal, at least, as what it is at stake right now is to contain the virus and its effects for society.

Moving forward with the discussion, addressing another legal basis is the principle of necessity, the big question about not only the use of digital data health but also to the whole package of measures, how necessary are the polices to undertake the COVID-19? From a global perspective it can be seen many different standards that lead countries to decide what it is considered necessary and unnecessary.

Taking into account that no country was prepared to deal and govern during a pandemic, left the governance in a blind spot. Even with the guidance of WHO and other international agencies, the principle of necessity can be very relative. Nevertheless, the decisions also became very much political – the form of each country is governed reflected directly in their decision in how to approach the pandemic.

221 Available at https://www.nature.com/articles/d41586-020-01264-1. Accessed on 13/01/2021.
222 Ibid note 203.

Some countries, reinforcing their more liberal politics did not imposed a completely lockdown with movement restrictions but let the citizens free, keeping their freedom of movement intact. Others, for many reasons, inclusive the exponential increase of the cases, decided for imposing a very strict lockdown for its citizens.

Even if Data Privacy is a relative right, it cannot be denied and suspended in any case, it is recognized as a basic fundamental right[223] and its guarantee is the base to provide Rule of Law in a democracy state. Meaning that Data privacy is not a privilege but rather a basic and fundamental right[224] and the threats to it, must be avoided, addressed and redress also must be provided. One of the most common arguments for implementing the digital health is the less human contact which directly affects the number of new cases and regarding contact-tracing app would be the replacement of this technology instead of a lockdown.

A strict lockdown already can represent harm to many human rights[225], according to the ICCPR, for example: police and drones to ensure lockdown compliance[226] (Article 12: protection of privacy), movement restrictions (Article 13: the right to freedom of movement), church closures (Article 18: the right to practice religion), the closure of businesses (Article 23: the right to work), closure of gyms, social clubs and restrictions on larger gatherings (Article 24: the right to rest and leisure).

Transparency will allow citizens to understand the functionalities of digital health and decide if they would like to use the services available, another reason why the services should be voluntary, as in case one sees certain app or service as intrusive, still can deny the use without any discrimination. As a side policy, states could engage in

223 Article 17, International Covenant of Political and Civil rights.
224 Available at https://www.forbes.com/sites/forbestechcouncil/2019/11/12/data-privacy-as-a-basic-human-right/?sh=2ba9be0a4cbf. Accessed on 15/01/2021.
225 Ryan, M. (2020). In defence of digital contact-tracing: human rights, South Korea and Covid-19. *International Journal of Pervasive Computing and Communications*.
226 Available at https://www.businessinsider.com/coronavirus-italian-police-monitoring-lockdown-with-drones-2020-3?r=US&IR=T. Accessed on

providing public information trough websites about legal frameworks, policies and surveillance[227].

When it comes to innovations during emergence states, from the legal perspective, any recommendation or law modifications should be time-bonded, should only be applied during a certain period of time. In the midst of a pandemic, one characteristic for implementing innovative approaches is that they were pretty much decided in the rush of the chaos, and even after one year facing the pandemic of the COVID-19, it is still not clear the effectiveness of the use of digital data health.

In some Asian countries as Singapore[228], Japan[229], China[230], the containment of the virus, can been seen, however the approach for achieving this result can be intrusive and not transparent, the long term costs for data privacy can be much more than with less harmful measures. The idea of being prevented of individual privacy rights given to the pandemic is a misconception of the true goal and put at stake the trusting in the global governance.

The technology that has been introduced during 2020 has enlarged the path of developing technologies, however the legal framework remains the same for years. It is crucial that law makers develop decisions envisioning the current challenges and also being pioneers in evaluating harmful technologies to privacy rights.

A fight against the virus can not be based on intrusive measures – For example, considering the contact-tracing apps, the effectiveness of the apps are not yet established and the implementation of them are being legally based on laws approved in a rush,

227 Available at https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx#:~:text=The%20right%20to%20privacy%20is%20a%20fundamental%20human%20right%2C%20recognized,considered%20as%20the%20presumption%20that. Accessed on 14/01/2021.

228 Available at https://www.statista.com/topics/6066/coronavirus-covid-19-outbreak-in-singapore/. Accessed on 14/01/2021.

229 Available at https://www.statista.com/topics/6087/coronavirus-disease-covid-19-in-japan/. Accessed on 14/01/2021.

230 Available at https://www.statista.com/topics/5898/novel-coronavirus-covid-19-in-china/. Accessed on 14/01/2021.

without assessment of the risks and most of the times lacking on transparency. The GAEN technology is not an open source system, what increase the difficulties to the scientific society in estimating likely harms it could cause to privacy rights. The open code provided by Apple and Google are a sample of the original code, the consequences are that more and more other private companies are creating their own apps which soon will go out of hands the research and assessment of those apps.

The liability of the companies developing such technologies need to be provided to the public information, hence a way to prevent intrusive surveillance is to establish oversight bodies, independent of the states with the scope of providing impartial risk assessment. These oversight bodies should be introduced by the governments in a attempt to promote and engage in the accountability for those private companies.

Also a unique legal framework would be a game changer also to countries that do not have yet a concrete scheme for privacy rights protection. The developed countries should be pioneers in establishing clear laws that prevent misuse of health data during the pandemic, together with providing redress to unlawful data processing and for third parties. The transparency of laws would contribute to withdraw technologies that are not inclusive and regulate other spheres of privacy rights, e,g. Cases of minor data or discrimination based on gender.

Ensuring that the data collected will be deleted after the pandemic and that all data will be anonymised and if used, used with only scientific scope will successfully assure that data privacy is protected and will help to overcome this crises without being a failure to the health responses.

7. International Cooperation and Policies Implementation for Guaranteeing Privacy Rights during a State of Emergency

The pandemic has brought to the world many different situations that were never seen before, not only from the legal perspective but also, and mainly from the political

point of view. The world has literally stopped to seek for a solution, world leaders for the first time in decades could not meet in person and the fear of the uncertainties were faced all across the globe.

Plenty of problems and few solutions, equation that lead each government, democratic or not, to be focused in one single subject that affected everyone. Even though the fact that the pandemic is a global problem, the international cooperation still needs to be enhanced aiming to find solutions that can be shared by the countries and promote equality and efficiency during this crisis.

A an example of how important it is the international cooperation and how the pandemic showed that a higher collective sense is indeed a key to mitigate the aftermath of the virus, is that in March 2020 the UN Secretary General[231] issued an urgent appeal for a global ceasefire, arguing that the true fight was against one single enemy: the COVID-19. Following the appeal of the Secretary General, in June 2020 more than 170 countries signed a joint statement, reinforcing the call for a global ceasefire[232]. This diplomatic action marks how important international cooperation is during a global health crisis.

The attempts to call for international cooperation were not only concentrated in war related issues but in a global act to coordinate a fairly defense against the COVID-19, that even with the joint coordination of international agencies, as the G7, G20, WHO and the UN, did not reach all countries, despite of that, some countries did not have a proper action plan to contain the virus by their own and are in truly need of international aid.

Given to this, most countries were working to implement measures that could be used as model for other countries, consulting experts, taking into account WHO statements and building up their own strategy to face the pandemic. Apart of that, the

231 Available at https://www.un.org/en/globalceasefire. Accessed on 15/01/2021.
232 Available at https://news.un.org/en/story/2020/06/1066982. Accessed on 15/01/2021; https://news.un.org/en/story/2020/05/1064852 Accessed on 15/01/2021.

incentives for a humanitarian aid were continuously made for helping less income countries to survive during the hard months of strict lockdown.

In many countries the health system collapsed given to the high numbers of cases and cases in a severe stage of the disease. For that reason, the international cooperation was the key to engage in a global vision for helping other countries in defending themselves against the crisis. China for example, a country that has been heavily criticized for alleged human rights violations, was one of the most engaged countries in helping other countries with health treatment and in researchers to develop a vaccine[233].

Notwithstanding, a vaccine to be fairly distributed also needs international cooperation, e.g to organize countries to sell/buy the vaccines, and delivery it in most remote areas of the globe. None of that can be achieved without a global mobilization; The vaccine can not arrive safely in all countries, if the nations do not negotiate a sage way to distribute the doses bearing in mind, other countries, as many of them have no capital to buy vaccines to the whole population. However the “nationalism vaccine” has increased due to the vaccine developing race, instead of cooperating to develop a common vaccine. This gap of cooperation was somewhat expected, according to the decrease of trade integration after the II World War.[234]

If the pandemic is faced by all countries, indeed, the solutions for that should be in a global level, strategies should be discussed by the leaders, implementing best practices to afford stability for the society to manage the health critical scenario. Along with the inequalities present in our societies, it would not be different from facing a pandemic, around the globe, countries experience the challenges against the COVID-19 differently and hence, also need different policies to achieve effectiveness. Said that, the importance to engage in global decisions, it is also important to keep the balance with applying appropriated measures to each context.

233 Available at http://www.china-un.ch/eng/zgyw/t1839532.htm. Accessed on 15/01/2021.
234 Brown, G., & Susskind, D. (2020). International cooperation during the COVID-19 pandemic. *Oxford Review of Economic Policy*, *36*(Supplement_1), S64-S76.

In this sense, digital health is a global phenomenal, however as the other spheres of the pandemic, it also evolves differently between the countries. Enough reason to lead a global initiative in order to promote good practices and guidance for other countries that do not necessarily have a well established legal framework for processing digital data health.

The international cooperation not only requires guidance and discussions, but also requires solid actions regarding the economic aspects to digital health, the decrease of implementing digital health technologies will provide the possibility to low and middle income countries to have access to this type of technology, guaranteeing the right to access to health. In this regard, the Global Observatory of EHealth from WHO, recently published demonstrates that 83% of the WHO countries are using Ehealth.[235]

Also, the WHO aiming to support international cooperation and decrease the costs to access digital health, the organization created the COVID-19 Technology Access Pool(C-TAP) and the Access to COVID-19 Tools Accelerator(ACT)[236] to promote data sharing, intellectual propriety and knowledge to produce digital health technology, so low income countries could have access to them.

There are still a lot to be done, however addressing the issues can represent a way to find the balance between the international cooperation as global action and policies implementation from a more local perspective. In this regard, the same objective should be carried out in the protection of Privacy Rights: more international cooperation in implementing laws that enable the implementation of innovative technologies, without suspending or harming Privacy Rights.

Privacy protection during the pandemic, promotes not only the protection of identification of individuals(in the case of contact-tracing apps, for example) but also protects the privacy rights of groups and fair treatment to them. During the pandemic,

235 World Health Organization. Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth [Internet]. Geneva: WHO Document Production Services; 2016. Available from: http://apps.who.int/iris/bitstream/10665/252529/1/9789241511780-eng.pdf?ua=1.

236 Ibid, note 225.

most of gatherings were forbidden, however some important social rituals are still allowed to happen, for instance, mourning.

Throughout this Master's Thesis were analyzed the difficulties in implementing technology in the midst of a rush to effectively deal with the pandemic and how intrusive tech should be avoided to preserve data privacy rights as a basic and fundamental human rights that sustain the Rule of Law and enable democracy to thrive. Therefore, promoting global guidance and having a solid international legal framework are a blueprint to prevent gaps and avoid discrimination towards vulnerable groups.

7. 1 Digital Divide, Ethical Governance and the Protection of Data Privacy

Cooperation between countries can also impact the effects that implementing digital health, as mentioned before, the nations have different levels of digital capacity and literacy. Whenever applying a new measure, the governments should also take into account the level of literacy of the country with the scope of fair distribution of the services, in respect of fundamental rights. At this point, international cooperation can open doors to share knowledge that can help other countries to use the digital services without compromising the part of the society that does not have access to the digital world.

Considering the responsibility of international agencies as the UN, WHO – that already had published joint statement – "*reinforcing its commitment to using data and new technologies in ways that respect the right to privacy and other human rights and promote sustainable economic and social development.*"[237] and the responsibility of developed countries as an international community, it is extremely relevant that those countries exchange technology in solidarity with low incoming countries to tackle the pandemic.

237 Available at https://www.iom.int/news/joint-statement-data-protection-and-privacy-covid-19-response. Accessed on 16/01/2021.

Therefore, international cooperation is not only aiming the contribution to trade goods or people, but also, bearing in mind the digital divide already institutionalized in the world, protect privacy rights through exchange of knowledge and promotion of guidance. For instance, Nigeria, one of the most populated countries in the world that has approximately 46.6%[238] of the population online, however with strict laws that threats directly data privacy rights[239] where its citizens do not feel comfortable to express themselves online.

Instead of engaging in policies that will increase the inequalities in the world, the pandemic can be seen as an opportunity to narrow international relationships and promote a sustainable advance of technology, if the nations can agree in working towards one vision, foremost the progressive tackle of the pandemic, supporting better Cybersecurity, leading the countries to take similar policies to consolidate privacy rights as a base for fighting the virus, should be decisive for the future of privacy rights and to achieve positive results.[240]

How the Global Governance will manage to promote policies that can tackle the balance between the digital divide and implementation of digital health, bearing in mind the necessity to protect privacy rights, is still unseen; However some initiatives can lead to a safe way to conduct an ethical use of the digital health, where all layers of society can benefit from the new technologies. Promoting long-terms digital social programs would increase the digital literacy of the population of the least developed countries and also legal provision for companies and third parties would safeguard private rights without compromising the objectives to fight the pandemic.

238 Available at https://www.statista.com/statistics/183849/internet-users-nigeria/#:~:text=In%202020%2C%20Nigeria%20had%2099.05,reach%2065.2%20percent%20in%202025.&text=Nigeria%20is%20one%20of%20the%20most%20populous%20countries%20worldwide. Accessed on 16/01/2021.

239 Available at https://paradigmhq.org/wp-content/uploads/2018/05/State-of-the-Nation-Status-of-Internet-Freedom-in-Nigeria-2016.pdf. Accessed on 16/01/2021.

240 Still, countries need to keep in mind the relative function of policies, adapting international policies or guidance to their current situation or choosing what effectively will work better for them.

Conclusion

In this Master’s thesis, the existent legal frameworks for data processing in the use of digital health technology in Italy, China and Switzerland, along with the legal framework with the European Union, were analyzed and discussed, aiming to elucidate possible gaps and unethical regulations. Notwithstanding, the thesis described the use of different technologies in those countries in order to build a risk assessment for their implementation during a state of emergence and in particular during the pandemic of the COVID-19.

Addressing data privacy as a fundamental human right is a necessity for the current world crisis, as we see the rapid advance of the technology with a unmatched advance of the legal framework that can represent a huge threat to our private life, if we allow intrusive measures to take place with the excuse of a state of emergence or public interest.

There is not enough evidence that contact-tracing apps can prevent identification of individual data, but this might change in the future where the systems will likely be enhanced and become safer. However, this master's thesis has discussed some points that should be taken into account in the implementation of digital health technologies, in order to safeguard privacy rights.

The main findings are that countries should establish a robust legal framework that can promote a transparent mechanism of accountability for data processing and provide information to the data subjects regarding their rights and risks in using digital health technology and that the use of tracing apps should not be mandatory. The legal framework should be based in the principles of proportionality, transparency, public interest and time-bonding and before its implementation a risk assessment involving different stakeholders should be delivered in the attempt to avoid intrusive and unequal technology.

Also, the data storage should happen only during the pandemic/state of emergence and minimum data should be collected and deleted as soon as possible. The current legal framework is not able to address provisions to all the range of ethical issues in data processing, hence states should engage in open source initiatives and long-term solutions based in the adaptation of rules, avoiding mass surveillance or incorporating permanently the measures into the society.

Along with provisions of redress in case of data misuse, states should implement independent oversight bodies that could review the law and the software and provide guidance for the government. It is fundamental that states can ensure a well designed policy that could balance the control and information sharing between countries with the only purpose to contain the spread of the virus or for scientific research with the allowance of the data subject.

States should engage in International Cooperation to develop strategies for the legal provisions, in order to have a clear guidance regarding the use of digital health technology and decrease the costs of new tech and shorten the digital divide, so least developed countries could also be able to tackle the pandemic with guarantee the data processing will be safely conducted.

The advance of the technology and the use of digital health data during the pandemic should not represent a threat to data privacy rights and other fundamental rights, instead it should represent a milestone for both legal and scientific fields which finally should walk together to build a trusting and sustainable environment for developing new technologies, promote democracy and avoid intrusive mass surveillance measures. Therefore, a global initiative to guarantee privacy rights with a transparent approach to the data processing, together with the respect of ethical principles should be the right approach to tackle together the pandemic and prepare the society for the future, based in fairness and trust.

REFERENCES

Agenda Digitale, 2020. https://www.agendadigitale.eu/sicurezza/privacy/covid-19-il-difficile-equilibrio-tra-diritto-alla-salute-e-tutela-della-privacy/. Accessed on 19/11/2020.

AI For Good, 2020. China Digital Healzh Strategies against the global pandemic. https://aiforgood.itu.int/events/covid-19-chinas-digital-health-strategies-against-the-global-pandemic/. Accessed on 19/10/2020.

Alexandre de Montjoye et. al., Evaluating COVID-19 contact-tracing apps? Here are 8 privacy questions we think you should ask, Computational Privacy Group (Apr. 2, 2020) https://cpg.doc.ic.ac.uk/blog/ evaluating-contact- tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/. Acessed in 22/01/2021.

Algorithm Watch, 2020. Governing Platforms. https://algorithmwatch.org/wp-content/uploads/2020/10/Governing-Platforms_DSA-Recommendations.pdf. Accessed on 11/01/2021.

Apple, 2020. https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf. Accessed on 18/01/2021.

Apple, 2020. Contact-Tracing. https://covid19.apple.com/contacttracing. Accessed on 18/01/2021.

BBC News, 2020. https://www.bbc.com/news/world-europe-52594570. Accessed on 30/09/2020.

BBC, 2020. Coronavirus: The hospital built in a matter of days.https://www.bbc.com/news/in-pictures-51280586. Accessed on 19/10/2020.

Becker, R., Thorogood, A., Ordish, J., & Beauvais, M. J. (2020). COVID-19 Research: Navigating the European General Data Protection Regulation.*Journal of Medical Internet Research*,*22*(8), e19799.

Bilder, R. (2010). An overview of international human rights law. *GUIDE TO INTERNATIONAL HUMAN RIGHTS PRACTICE, 4th Ed., Hurst Hannum, ed*, 3-18.

Blasimme, A., & Vayena, E. (2020). What's next for COVID-19 apps? Governance and oversight. *Science*, *370*(6518), 760-762.

Bradford, L. R., Aboy, M., & Liddell, K. (2020). COVID-19 contact-tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes.*Journal of Law and the Biosciences*.

Brin, D. (1998). The transparent society. Will technology force us to choose between privacy and freedom? New York: Basic Books.

Brown, G., & Susskind, D. (2020). International cooperation during the COVID-19 pandemic. *Oxford Review of Economic Policy*, *36*(Supplement_1), S64-S76.

Buergenthal, T. (2006). The evolving international human rights system.*Am. J. Int'l L.*, *100*, 783.

Bundesamt für Gesundheit, 2020. Coronavirus measures and ordinance.https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/massnahmen-des-bundes.html. Accessed on 14/10/2020.

Bundesamt für Gesundheit, 2020. SwissCovid app and contact-tracing. https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing/datenschutzerklaerung-nutzungsbedingungen.html#-11360452. Accessed on 14/10/2020.

Bundesamt für Gesundheit, 2020.Situation Coronavirus Switzerlan.https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/situation-schweiz-und-international.html#-6104062 Accessed on 14/10/2020.

Business Insider, 2020. Italian police monitoring lockdown with drones.https://www.businessinsider.com/coronavirus-italian-police-monitoring-lockdown-with-drones-2020-3?r=US&IR=T. Accessed on 14/01/2021.

Business Wire, 2020. First Use of a Digital COVID-19 Health Certificate to Cross an International Border.https://www.businesswire.com/news/home/20201223005428/en/First-Use-of-a-Digital-COVID-19-Health-Certificate-to-Cross-an-International-Border-Completed-by-Traveller-to-Singapore. Accessed on 28/12/2020.

Business Insider, 2020. Switzerland Google and Apple contact-tracing app launched. https://www.businessinsider.com/switzerland-google-apple-contact-tracing-api-launched-2020-5?r=US&IR=T. Accessed on 14/10/2020.

Calzada, Igor, Will COVID-19 Be the End of the Global Citizen? (March 20, 2020). Calzada, I. (2020), Will COVID-19 Be the End of the Global Citizen? Apolitical. Available at SSRN:https://ssrn.com/abstract=3558029.

CATTUTO, C., & SPINA, A. (2020). The Institutionalisation of Digital Public Health: Lessons Learned from the COVID-19 App.*European Journal of Risk Regulation*,*11*(2), 228-235.

CCPR, 1999. International Covenant on Civil and Political Rights. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9&Lang=en. Accessed on 04/01/2021.

CGTN, 2020. China sends medical experts to Russia to help fight COVID-19- https://news.cgtn.com/news/2020-04-11/China-sends-medical-experts-to-Russia-to-help-fight-COVID-19-PBshI0UoaQ/index.html. Accessed on 04/01/2021.

Cho, H., Ippolito, D., & Yu, Y. W. (2020). contact-tracing mobile apps for COVID-19: Privacy considerations and related trade-offs.arXiv preprint arXiv:2003.11511.

Computational Privacy Group, 2020. Evaluating contact-tracing apps?Here are 8 privacy questions we think we could ask.https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/. Accessed on 11/11/2020.

Council of Europe, 1950. European Convention of Human Rights. https://www.echr.coe.int/documents/convention_eng.pdf. Accessed on 06/01/2020.

Dailymail, 2020. Huawei Subsidiary Unveils Smartphone Sensor Temperature.https://www.dailymail.co.uk/sciencetech/article-8385835/Huawei-subsidiary-unveils-smartphone-sensor-temperature.html.Accessed on 16/10/2020.

De Hert, P., & Papakonstantinou, V. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably un agency. I/S: Journal of Law and Policy for the Information Society, 9(2), 271-326.

Eidgenössische Technische Hochschule Zürich, 2020.https://ethz.ch/en/news-and-events/eth-news/news/2020/05/swiss-covid-app.html.Accessed on 14/10/2020.

Eur-Lex, 2000.Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland.https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000D0518. Accessed on 02/12/2020.

Eur-Lex, 2014. Malone v United Kingdom, 1984; Leander v Sweden, 198.https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0131. Accessed on 11/11/2020.

Euractiv, 2020. European Coronavirus Tracing apps are Crossing Borders. https://www.euractiv.com/section/digital/news/european-coronavirus-tracing-apps-are-crossing-borders/. Accessed on 28/12/2020.

European Court of Human Rights, 2020. Guide on article 8 of the European Convention on Human Rights. https://www.echr.coe.int/documents/guide_art_8_eng.pdf.Accessed on 11/11/2020.

European Data Protection Board, 2020.Guidelines 04/2020 on the use of location data and contact-tracing tools in the context of the COVID-19 outbreak.https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.Accessed on 26/10/2020.

European Union Agency for Fundamental Rights, 2020. https://fra.europa.eu/sites/default/files/fra_uploads/it_report_on_coronavirus_pandemic_july_2020.pdf. Accessed on 25/11/2020.

European Union Agency for Fundamental Rights, 2020. https://fra.europa.eu/sites/default/files/fra_uploads/italy-report-covid-19-april-2020_en.pdf. Accessed on 16/11/2020.

European Union Agency for Fundamental Rights, 2020. https://images.go.wolterskluwer.com/Web/WoltersKluwer/%7Bbcbf65c6-ffe2-4b95-8931-d4e42ac03ee7%7D_garante-privacy-provvedimento-1-giugno-2020.pdf. Accessed on 26/11/2020.

European Union, 2020. The History of the European Union. https://europa.eu/european-union/about-eu/history_en. Accessed on 21/12/2020.

Federal Constitution of the Swiss Confederation. ,1999. https://www.admin.ch/opc/en/classified-compilation/19995395/201801010000/101.pdf. Accessed on 30/11.

Federal Data Protection and Information Commissioner,2020. https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html. Accessed on 08/12/2020.

Federal Department of Foreign Affairs, 2020.Switzerland and the European Union. https://www.eda.admin.ch/dam/eda/en/documents/publications/EuropaeischeAngelegenheiten/Schweiz-und-EU_en.pdf. Accessed on 29/11/2020.

Federal Office of Public Health, 2009. https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/dokumentation/guide/trattamento-dei-dati-personali-in-seno-all-amministrazione-feder.html. Acessed in 11/12/2020. Federal Office of Public Health, 2006. https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/dokumentation/guide/trattamento-dei-dati-personali-nella-sfera-medica.html. Accessed on 11/12/2020.

Federal Office of Public Health, 2020. Data Protection Statement of the Federal Office of Public Health FOPH in connection with the use of the “SwissCovid app. https://www.bag.admin.ch/dam/bag/en/dokumente/cc/kom/swisscovid-app-

datenschutz.pdf.download.pdf/FOPH_SwissCovid_Data_Protection_Statement_24_June2020.pdf. Accessed on 9/12/2020.

Federal Office of Public Health, 2020. Swisscovid Data Protection Statement and Conditions of Use.https://www.bag.admin.ch/swisscovid-data-protection-statement-and-conditions-of-use. Accessed on 28/12/2020.

Federal Statistical Office, 2020. Gross Domestic Product. https://www.bfs.admin.ch/bfs/en/home/statistics/national-economy/national-accounts/gross-domestic-product.html. Accessed on 21/12/2020.

Federal Statistical Office, 2020. https://www.experimental.bfs.admin.ch/expstat/en/home/innovative-methods/swisscovid-app-monitoring.html.Accessed on 14/10/2020.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations.*Minds and Machines*,*28*(4), 689-707.

Forbes, 2020. Alipay leads the way in covid-19 fintech and its lesson for other platforms. https://www.forbes.com/sites/eladnatanson/2020/12/09/alipay-leads-the-way-in-covid-19-fintech—and-its-a-lesson-for-other-platforms/?sh=5158da9f2638. Accessed on 04/01/2021.

Forbes, 2020. Data Privacy as a basic human right.https://www.forbes.com/sites/forbestechcouncil/2019/11/12/data-privacy-as-a-basic-human-right/?sh=2ba9be0a4cbf. Accessed on 15/01/2021.

Forbes, 2020. https://www.forbes.com/sites/sap/2020/11/19/how-the-holiday-shopping-experience-will-be-different-in-2020and-what-it-means-for-frontline-staff/?sh=5f7cec3a6e8e. Accessed on 26/11/2020.

Garante per la Prottezione dei Dati Personali, 2020. https://images.go.wolterskluwer.com/Web/WoltersKluwer/%7Bbcbf65c6-ffe2-4b95-8931-d4e42ac03ee7%7D_garante-privacy-provvedimento-1-giugno-2020.pdf. Accessed on 25/11/2020.

Garante per la Prottezione dei Dati Personali, 2020. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9308774#english_version. Accessed on 24/11/2020.

Garante Privacy, 2020. Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni"- Available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9357972. Accessed on 16/11/2020.

Gazzetta Ufficiale, 2020. https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg. Accessed on 17/11/2020.

Gazzetta Ufficiale, 2020. https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg. Accessed on 18/11/2020.

General Data Protection Regulation(GDPR).https://www.privacy-regulation.eu/en/recital-46-GDPR.htm. Accessed on 19/11/2020.

Github, 2020. https://github.com/immuni-app/immuni-documentation. Accessed on 01/10/2020.

Github, 2020. https://github.com/immuni-app/immuni-documentation. Accessed on 01/10/2020.

Gittleman, R. (1981). The African Charter on Human and Peoples' Rights: A Legal Analysis.*Va. J. Int'l L.*,*22*, 667.

Golinelli, D., Boetto, E., Carullo, G., Landini, M. P., & Fantini, M. P. (2020). How the COVID-19 pandemic is favoring the adoption of digital technologies in healthcare: a rapid literature review.*medRxiv*.

Google- Apple Exposure Notification.

Governo Italia, 2020. http://www.governo.it/node/15350, Accessed on 16/11/2020.

Human Rights Watch, 2020. Global coalition urges UN address chinas human rights abuses. https://www.hrw.org/news/2020/09/09/global-coalition-urges-un-address-chinas-human-rights-abuses. Accessed on 24/10/2020.

IBM, 2020. Cloud Computing.https://www.ibm.com/cloud/learn/cloud-computing. Accessed on 21/10/2020.

Immuni, 2020. https://www.immuni.italia.it/. Accessed on 30/09/2020.

International Organization for Migration, 2020. Joint Statement on Data Protection and Privacy in the COVID-19 Response.https://www.iom.int/news/joint-statement-data-protection-and-privacy-covid-19-response. Accessed on 16/01/2021.

ITU News, 2014. https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1487056335. Accessed on 19/10/2020.

ITU News, 2020. Covid-19 China's Digital Health Strategies against the Pandemic. https://news.itu.int/covid-19-chinas-digital-health-strategies-against-the-global-pandemic/. Accessed on 16/10/2020.

J. M. Bahi, A. Makhoul and A. Mostefaoui, "A Mobile Beacon Based Approach for Sensor Network Localization,"Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), White Plains, NY, 2007, pp. 44-44, doi: 10.1109/WIMOB.2007.4390838.

James, Luke, 2020. China Deploys 5G Patrol Robots to monitor the Spread of The sickness. https://www.allaboutcircuits.com/news/china-deploys-5g-patrol-robots-to-monitor-the-spread-of-sickness/.Accessed on 16/10/2020.

Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?.

JD Supra, 2020. Italian Data Protection Authority's approval of the contact-tracing app Immuni.https://www.jdsupra.com/legalnews/italian-data-protection-authority-s-62316/, Accessed on 08/01/2021 and In The Local, 2020. Swiss parliament approves coronavirus tracing app.https://www.thelocal.ch/20200609/swiss-parliament-approves-coronavirus-tracing-app. Accessed on 08/01/2021.

Knobel, Isabel, Fegert, Moritz and Detreköy, Niculin (2020): "Health Data Governance: What's in it for Switzerland?", Zurich: Sensor Advice and foraus - Forum on Foreign Policy.

Kummitha, R. K. R. (2020). Smart technologies for fighting pandemics: The techno-and human-driven approaches in controlling the virus transmission. *Government Information Quarterly*, 101481.

Kunz, J. (1949). The United Nations Declaration of Human Rights. *American Journal of International Law, 43*(2), 316-323. doi:10.2307/2193039

Lexology, 2019. Data Protection and Privacy in Switzerland. https://www.lexology.com/library/detail.aspx?g=292c3925-8663-4fdb-8f1c-2eaf4b262634. Accessed on 8/12/2020.

Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the protection of Health Data ,2019.Recommendation on the protection and use of health-related data https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf. Accessed on 26/10/2020.

Metille, S. (2013). Swiss information privacy law and the transborder flow of personal data. Journal of International Commercial Law and Technology, 8(1), 71-80. at https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/the-commissioner.html and https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/task.html. Accessed on 8/12/2020.

Morisi, M., & Cazzola, F. (1981). LA DECISIONE URGENTE. USI E FUNZIONI DEL DECRETO LEGGE NEL SISTEMA POLITICO ITALIANO.*Italian Political Science Review/Rivista Italiana Di Scienza Politica,11*(3), 447-481. doi:10.1017/S0048840200011977.

Nature, 2020.Show evidence that apps for COVID-19 contact-tracing are secure and effective.https://www.nature.com/articles/d41586-020-01264-1.Accessed on 13/01/2021.

Netzwoche, 2020. https://www.netzwoche.ch/news/2020-08-18/swisscovid-app-soll-in-ganz-europa-funktionieren. Accessed on 28/12/2020.

News Week, 2020. Contact-Tracing Apps Could Become Permanent Once the Pandemic Is Over. https://www.newsweek.com/covid-19-contact-tracing-apps-could-permanent-after-coronavirus-pandemic-1507103. Accessed on 29/12/2020.

Official Journal of the European Union, 2016. Regulation(EU) 2016/679 Of The European Parliament and of the Council.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.Accessed on 25/10/2020.

Okere, B. (1984). The protection of human rights in Africa and the African charter on human and peoples' rights: comparative analysis with the European and American systems. *Human Rights Quarterly, 6(2),* 141-159.

Our World in Data, 2020. Internet. https://ourworldindata.org/internet. Accessed on 11/01/2021.

Paradigm Initiative Nigeria, 2018. Status of internet freedom in Nigeria. https://paradigmhq.org/wp-content/uploads/2018/05/State-of-the-Nation-Status-of-Internet-Freedom-in-Nigeria-2016.pdf. Accessed on 16/01/2021.

Pato, Alexia. Blog Droit Europeen, 2020. Covid-19 and Data Protection issues in Switzerland. https://blogdroiteuropeen.com/2020/07/10/covid-19-and-data-protection-issues-in-switzerland-by-alexia-pato/. Accessed on 9/12/2020.

Permanent Mission of the people's Republic of China to the United Nations, 2020. Serving the Country and Contributing to the World: China's Diplomacy in a Time of Unprecedented Global Changes and a Once-in-a-Century Pandemic. http://www.china-un.ch/eng/zgyw/t1839532.htm. Accessed on 15/01/2021.

Privacy International, 2020. Hangzhou plans permanent role for coronavirus surveillance. https://privacyinternational.org/examples/3886/hangzhou-plans-permanent-role-coronavirus-surveillance-app. Accessed on 29/12/2020.

Pyrgelis, A., Troncoso, C., & De Cristofaro, E. (2017). Knock knock, who's there? Membership inference on aggregate location data.*arXiv preprint arXiv:1708.06145*.

Refworld, 2004.The nature of the general legal obligation imposed on States Parties to the Covenant. https://www.refworld.org/docid/478b26ae2.html. Accessed on 12/11/2020.

Report of the Office of the United Nations High Commissioner for Human Rights, 2014.The Right to Privacy in the digital age.https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc. Accessed on 12/11/2020.

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. 27/07/2020. Available at https://undocs.org/A/75/147. Accessed on 21/12/2020.

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci.27/07/2020. Available at https://undocs.org/A/75/147.Accessed on 29/12/2020.

Repubblica, 2020. Coronavirus Veneto, la proposta di Zaia: "Sospendere in tutta Italia le norme sulla privacy". https://www.repubblica.it/politica/2020/03/26/news/zaia_sospensione_privacy-252373104/. Accessed on 06/01/2020.

Repubblica,2020.https://www.repubblica.it/tecnologia/2020/08/25/newscoronavirus_l_app_immuni_a_5_milioni_di_download_ma_e_solo_il_13_-265432164/. Accessed on 01/10/2020.

Reuters, 2020. In land of big data, China sets individual privacy rights. https://www.reuters.com/article/us-china-parliament-lawmaking-privacy-idUSKBN2320EF. Accessed on 29/12/2020.

Reuters, 2020. US Health Coronvirus Singapore contact ID.https://www.reuters.com/article/us-health-coronavirus-singapore-contact-idUSKBN2990X8. Accessed on 06/01/2021.

Ryan, M. (2020). In defence of digital contact-tracing: human rights, South Korea and Covid-19.*International Journal of Pervasive Computing and Communications*.

Smith, R. (2020).*International Human Rights Law*. Oxford University Press, USA.

Sohu, 2020. https://www.sohu.com/a/378301359_100256408.Accessed on 16/10/2020.

Statista, 2020. Coronavirus covid-19 outbreak in China. https://www.statista.com/topics/5898/novel-coronavirus-covid-19-in-china/. Accessed on 14/01/2021.

Statista, 2020. Coronavirus covid-19 outbreak in Japan. https://www.statista.com/topics/6087/coronavirus-disease-covid-19-in-japan/. Accessed on 14/01/2021.

Statista, 2020. Coronavirus covid-19 outbreak in Singapore.https://www.statista.com/topics/6066/coronavirus-covid-19-outbreak-in-singapore/. Accessed on 14/01/2021.

Statista, 2020. Nigeria. https://www.statista.com/statistics/183849/internet-users-nigeria/#:~:text=In%202020%2C%20Nigeria%20had%2099.05,reach%2065.2%20percent%20in%202025.&text=Nigeria%20is%20one%20of%20the%20most%20populous%20countries%20worldwide. Accessed on 16/01/2021.

Statista, *2020*.https://www.statista.com/statistics/1106743/opinions-on-italian-government-s-response-to-coronavirus/. Accessed on 19/11/2020.

Swiss Air Company, 2020. China flight schedule. https://www.swiss.com/china/en/china-flight-schedule. Accessed on 04/01/2021.

Swiss Info, 2020. https://www.swissinfo.ch/eng/geneva-introduces-partial-lockdown/46134304. Accessed on 27/11/2020.

T. Mulder & M. Tudorica (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, 28:3, 261-274, DOI: 10.1080/13600834.2019.1644068.

Taylor, M. (2006). The EU data retention directive. *Computer Law & Security Review*, *22*(4), 309-312.

The Guardian, 2020. https://www.theguardian.com/artanddesign/2020/mar/25/10-coronavirus-covid-busting-designs.Accessed on 16/10/2020.

The Guardian, 2020. https://www.theguardian.com/world/2020/mar/19/generation-has-died-italian-province-struggles-bury-coronavirus-dead. Accessed on 30/09/2020.

The New York Times, 2020. China coronavirus surveillance. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Accessed on 04/01/2021.

The Publication Platform for Federal Law, 2020. Ordinance on the proximity Tracing System for the Sars-Cov-2 Coronavirus.https://www.admin.ch/opc/en/classified-compilation/20201730/index.html. Accessed 9/12/2020.

UK Government, 2020. https://www.gov.uk/foreign-travel-advice/switzerland. Accessed on 28/12/2020.

UN News, 2020. 170 signatories endorse UN ceasefire appeal during COVID crisis. https://news.un.org/en/story/2020/06/1066982. Accessed on 15/01/2021

UN News, 2020. UN welcomes three-day ceasefire announcement by Afghan government and Taliban during Eid al-Fitr. https://news.un.org/en/story/2020/05/1064852. Accessed on 15/01/2021.

UN Special Rapporteur on the right to privacy, Joseph Cannataci,2019. UN expert warns of enormous privacy concerns over health data as he unveils international protection standards. https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25221&LangID=E. Acessed in 26/10/2020.

United Nations, 1948. https://www.un.org/en/universal-declaration-human-rights/ Accessed on 01/11/2020.

United Nations, 1966. International Covenant on Civil and Political Rights. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. Accessed on 06/01/2020.

United Nations, 1984. Status of the International Covenants on Human Rights. https://undocs.org/pdf?symbol=en/E/CN.4/1985/4. Accessed on 06/01/2020.

United Nations, 2020. Call for global ceasefire. https://www.un.org/en/globalceasefire. Accessed on 15/01/2021.

United Nations, 2020. COVID-19 and Human Rights.https://www.un.org/victimsofterrorism/sites/www.un.org.victimsofterrorism/files/un_-_human_rights_and_covid_april_2020.pdf. Accessed on 30/10/2020.

United Nations, 2020. We are all in this Together: Human Rights and COVID-19 Response and Recovery.https://www.un.org/en/un-coronavirus-communications-team/we-are-all-together-human-rights-and-covid-19-response-and. Accessed on 04/01/2021.

University of Harvard, 2020.https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf?m=1586179217.Accessed on 22/01/2021.

Urs Gasser,Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy, 130HARV.L.REV.F.61 (2016).

Vaudenay, Serge. 2020. The Dark Side of the SwissCovid.https://lasec.epfl.ch/people/vaudenay/swisscovid.html. Accessed on 23/12/2020.

Vayena, E., Haeusermann, T., Adjekum, A., & Blasimme, A. (2018). Digital health: meeting the ethical and policy challenges.*Swiss medical weekly*,*148*, w14571.

Weforum, 2020. Coronavirus covid-19 Italy China Supplies. https://www.weforum.org/agenda/2020/03/coronavirus-covid-19-italy-china-supplies/. Accessed on 04/01/2021.

Weixen, 2020. https://mp.weixin.qq.com/s/cXlYMcN-pP2oJqgwTYFweg. Accessed on 04/01/2021.

Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*.

Willi, Y., Nischik, G., Braunschweiger, D. and Pütz, M. (2020), Responding to the COVID-19 Crisis: Transformative Governance in Switzerland. Tijds. voor econ. en Soc. Geog., 111: 302-317. doi:10.1111/tesg.12439

World Health Organization, 2020. ://www.who.int/southeastasia/news/opinion-editorials/detail/together-forward-in-the-fight-against-covid-19. Accessed on 18/01/2021.

World Health Organization, 2020. Covid Timeline.ww.who.int/news/item/29-06-2020-covidtimeline.Accessed on 16/10/2020.

World Health Organization, 2020. https://covid19.who.int/region/euro/country/it. Accessed on 30/09/2020.

World Health Organization, 2020. https://www.who.int/bulletin/volumes/98/3/20-251561/en/. Accessed on 8/12/2020.

World Health Organization, 2020. https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19. Accessed on 02/10/2020.

World Health Organization. Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth. Geneva: WHO Document Production Services; 2016. Available from: http://apps.who.int/iris/bitstream/10665/252529/1/9789241511780-eng.pdf?ua=1.

World Heath Organization, 2020. Covid Situation.Https://covid19.who.int/region/wpro/country/cn. Accessed on 16/10/2020.

XDA Developers, 2020. https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/. Accessed on 22/01/2021.

Xinhuanet, 2020. China sends humanitarian aid to Kazakhstan to fight COVID-19. http://www.xinhuanet.com/english/2020-07/05/c_139190312.htm. Accessed on 04/01/2021.

Zwizwai Ruth, 2020. China's successful control of COVID-19.https://www.thelancet.com/action/showPdf?pii=S1473-3099%2820%2930800-8.Accessed 16/10/2020.