RECONCILING DIGITAL CONTACT TRACING AND THE RIGHT TO PRIVACY DURING THE COVID-19 PANDEMIC IN EUROPE: A FOCUS ON THE ITALIAN CASE

Federica Cristani*
Jean Monnet Visiting Lecturer
V.N. Karazin Kharkiv National University (Ukraine)

RESUMEN: La llegada de la pandemia de la COVID-19 ha tenido, entre otras consecuencias, la utilización de diferentes tecnologías basadas en la recopilación de datos y otras actividades de procesamiento de datos por parte de Estados de todo el mundo. Los gobiernos de los diferentes Estados están empleando instrumentos tecnológicos para rastrear la propagación de la pandemia dentro de sus territorios, desarrollando diferentes tipos de aplicaciones móviles. Si bien pueden ayudar a las autoridades gubernamentales a seguir la pista de la propagación del virus y cumplir con sus obligaciones de proteger los derechos a la salud y la vida de sus ciudadanos, también traen consigo preocupaciones legales sobre la recogida y uso de datos y el respeto del derecho a la privacidad. A nivel internacional y europeo, se pide a los Estados que en el seguimiento y desarrollo de las aplicaciones móviles de seguimiento respeten sus obligaciones en materia de derechos humanos y, en particular, el derecho a la privacidad.

En el presente artículo se valora en qué medida el sistema de aplicaciones de seguimiento operativo en la actualidad en Italia se ajusta al estándar internacional del derecho a la privacidad de los ciudadanos

PALABRAS CLAVE: Derecho a la privacidad, seguimiento de la aplicación móvil, aplicación Immuni, protección de datos, COVID-19.

ABSTRACT: The outbreak of the COVID-19 pandemic has opened up to the use of different technologies based on data collection and other data processing activities

* Fecha de recepción: 30 julio de 2020
Fecha de aceptación: 1 septiembre 2020

by states around the world; countries are employing technological instruments to track the spread of the pandemic within their territories, developing different kinds of tracking mobile applications. While they can help governmental authorities in monitoring the spread of the virus and fulfil their obligations to protect the rights to health and life of their citizens, they also bring along legal concerns about the collection and use of data and the respect of the right to privacy. At the international and European levels several efforts have been taken to call on states to respect their human rights obligations, and in particular the right to privacy, while developing and implementing tracking mobile applications.

The present article offers a reflection on how the tracking app system that is now operative in Italy is in conformity with the right to privacy of citizens: after a starting overview of the development of the Italian mobile application, the article investigates the conformity of this instrument to the right to privacy, as regulated at the national, European and international levels.

KEYWORDS: Right to privacy, tracking mobile application, Immuni app, data protection, COVID-19.

RÉSUMÉ: L'arrivée de la pandémie COVID-19 a eu, entre autres conséquences, l'utilisation de différentes technologies basées sur la collecte de données et d'autres activités de traitement de données par les États du monde entier. Les gouvernements des différents États utilisent des instruments technologiques pour suivre la propagation de la pandémie sur leur territoire, en développant différents types d'applications mobiles. Bien qu'ils puissent aider les autorités gouvernementales à suivre la propagation du virus et à respecter leurs obligations de protéger les droits à la santé et à la vie de leurs citoyens, ils soulèvent également des préoccupations juridiques concernant la collecte et l'utilisation des données et la le respect du droit à la vie privée. Aux niveaux international et européen, les États sont invités à respecter leurs obligations en matière de droits de l'homme dans le suivi et le développement des applications de suivi mobile et, en particulier, le droit à la vie privée.

Cet article évalue dans quelle mesure le système de surveillance des applications actuellement en vigueur en Italie est conforme à la norme internationale du droit à la vie privée des citoyens.

MOTS-CLÉS: Droit à la confidentialité, suivi des applications mobiles, application Immuni, protection des données, COVID-19.

LABURPENA: COVID-19ren pandemiaren etorrerak, besteak beste, mundu osoko estatuek datuak biltzean eta datuak prozesatzeko beste jarduera batzuetan oinarritutako hainbat teknologia erabiltzea ekarri du. Estatu ezberdinetako gobernuak tresna teknologikoak erabiltzen ari dira pandemiaren hedapena beren lurraldeetan arakatzeko, hainbat aplikazio mugikor mota garatuz. Nahiz eta birusa hedatzeko arrastoari jarraitzen eta herritarren osasunerako eta bizitzarako eskubideak babesteko dituzten betebeharrak betetzen

gobernuko agintariei lagundu diezaieketen, datuak biltzeari eta erabiltzeari eta pribatutasunerako eskubidea errespetatzeari buruzko lege-kezkak ere ekartzen dituzte. Nazioartean eta Europan, estatuei eskatzen zaie jarraipen-aplikazio mugikorren jarraipenean eta garapenean errespeta ditzatela giza eskubideen arloan dituzten betebeharrak eta, bereziki, pribatutasunerako eskubidea.

Artikulu honetan balioesten da Italian gaur egun dagoen jarraipen operatiboko aplikazioen sistema zenbateraino egokitzen zaion herritarren pribatutasunerako eskubidearen nazioarteko estandarrari.

GAKO-HITZAK: Pribatutasunerako eskubidea, aplikazio mugikorraren jarraipena, Immuni aplikazioa, datuen babesa, COVID-19.

1. USING DIGITAL CONTACT TRACING DURING THE COVID-19 PANDEMIC: AN INTRODUCTORY OVERVIEW

The outbreak of the COVID-19 pandemic[1] has opened up to the use of different technologies by states around the world; indeed, among the different legal, political, and public health responses to COVID-19, countries are employing technological instruments to track the spread of the pandemic within their territories[2] and monitor the citizens' abidance with governmental measures such as quarantine[3].

Digital technologies that are being employed include mobile and biometric applications; in particular, those based on geolocation provide data about the geographical spread of the virus, as in the case of the call data records (CDRs), namely the data that are elaborated by telecommunication service providers and are based on telephone calls, which enable the tracing

---

1 For a general and introductory overview of the COVID-19 pandemic and the responses that are being adopted by states around the world, see von Bogdandy, A., Villarreal, P.A., «International Law on Pandemic Response: a First Stocktaking in Light of the Coronavirus Crisis», *MPIL Research Paper Series,* No. 2020-07, 26 March 2020, https://www.mpil.de (last accessed 30 July 2020), Sands, P., «COVID-19 Symposium: COVID-19 and International Law», *Opinion Juris,* 30 March 2020, http://opiniojuris.org (last accessed 30 July 2020) and the resources on COVID-19 at the Oxford University Press website https://academic.oup.com/journals (last accessed 30 July 2020).

2 On the use of technologies in tracking the spread of COVID-19, see Privacy International, *Apps and Covid-19,* 2020, https://privacyinternational.org (last accessed 30 July 2020) and McGregor, L., «Contact-tracing Apps and Human Rights», *EJIL: Talk Blog*, 30 April 2020, https://www.ejiltalk.org (last accessed 30 July 2020).

3 OECD, «Tracking and tracing COVID:Protecting privacy and data while using apps and biometrics», *OECD Policy Responses to Coronavirus (Covid-19)*, 23 April 2020, 1, http://www.oecd.org/coronavirus (last accessed 30 July 2020).

of the movements of people on both a temporal and geographical scale[4]. In this respect, the Robert-Koch Institute in Germany is using anonymised movement flows data collected by the German telecommunications provider Deutsche Telekom[5], while in Italy, an aggregated and anonymous heat map –based on anonymised datasets– for the Lombardy region to better understand population movements has been produced by Vodafone[6].

Alongside the data that can be collected by telecommunication service providers, governments are being launching new mobile applications for tracing the spread of COVID-19[7].

Singapore, for example, has been using the TraceTogether App, developed by the Government Technology Agency of Singapore in collaboration with the Ministry of Health, which has also served as a model for similar contact tracing apps in other countries. TraceTogether uses Bluetooth in order to tracks those who have been exposed to the virus, on the basis of the proximity and duration of a 'contact' between two users and alerting those who come in contact with someone who has been tested positive to the virus[8].

An additional example is the Self-quarantine Safety App, developed by the Ministry of the Interior and Safety of the Korean government and mandatory for all Koreans and long-stay foreigners, which is used by governmental authorities to monitor those who are on a compulsory self-quarantine. This app uses GPS to keep track of the location of people; moreover, those in quarantine can send updates about their health status through this mobile application to governmental officials[9].

---

4 Ibid., 2.

5 See Broszio, S., «Corona prediction: Telekom supports RKI», *Telekom*, 18 March 2020, https://www.telekom.com/en (last accessed 30 July 2020).

6 See the official webpage of Vodafone, *Vodafone launches five-point plan to help counter the impacts of the COVID-19 outbreak,* 18 March 2020, https://www.vodafone.com (last accessed 30 July 2020) and Privacy International, «Vodafone produces anonymous heat map to help Lombardy understand population movements», *Privacyinternational.org,* 18 March 2020, https://privacyinternational.org (last accessed 30 July 2020).

7 Indeed, contact-tracing is a common technique in public health surveillance. See World Health Organizazion, *Contact tracing,* 9 May 2017, https://www.who.int (last accessed 30 July 2020).

8 See the official website at https://www.tracetogether.gov.sg (last accessed 30 July 2020). For a comment, see also OECD, op. cit., 2.

9 See the official documentation prepared by the Korean Central Disaster and Safety Countermeasures Headquarters, *Guide on the Installation of "Self-quarantine Safety Protection App"*, 1 April 2020, http://ncov.mohw.go.kr (last accessed 30 July 2020). For a comment, see Kim, M.S., «South Korea is watching quarantined citizens with a smartphone app», *MIT Technology Review,* 6 March 2020, https://www.technologyreview.com (last accessed

As we well see more in detail in the following paragraphs, in Europe, several states, including Italy, are in the process of developing or have already released tracking mobile applications. While they can help governmental authorities in monitoring the spread of the virus and fulfil their obligations to protect the rights to health and life of their citizens, they bring along also a number of concerns: first, they are not necessarily available for everyone (e.g. the elderly who may not have, or be proficient in the use of, smartphones); second, some errors might occur in the collection of data (e.g. it has been reported that in some cases the app might not be able to distinguish between people in the same household and those in surrounding residences[10]); furthermore, some legal concerns arise about the collection and use of data and the respect of the right to privacy of the users of the mobile applications. Indeed, a tracking app can collect a broad range of personal data; in some cases, apps continue to run in the background even when the device is not in use, while other apps can exchange information with other devices. Moreover, a number of countries are implementing mobile applications that use facial recognition or other biometrics smartphone apps, such as in Poland, China and Russia, which may raise additional concerns, e.g. when facial recognition is based on race or ethnic origin[11].

For the most part, tracking mobile apps are designed in order to allow users to give their explicit, informed consent to the collection and sharing of their personal data. For instance, the Singapore's TraceTogether app does not collect or use geolocation data and data logs are stored in an encrypted form, and the same holds true for some European apps[12].

The following paragraphs focus on tracking mobile technologies that are being developing in Europe, with a special focus on Italy, and on the relevant debate about the right to privacy and data protection concerns.

2. DIGITAL CONTACT TRACING IN EUROPE: THE INITIATIVES SO FAR

At the European level, the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), developed by experts from eight European countries

---

30 July 2020) and United Nations Development Programme, «Compulsory self-quarantine monitoring», *Innovative Responses to COVID-19: Collection of Approaches from the Republic of Korea,* 22 April 2020, https://www.undp.org (last accessed 30 July 2020).

10 European Centre for Disease Prevention and Control (ECDC), *Mobile applications in support of contact tracing for COVID-19. A guidance for EU EEA Member States,* 10 June 2020, https://www.ecdc.europa.eu (last accessed 30 July 2020).

11 OECD, op. cit., 3-4.

12 Ibid., 3.

(Austria, Denmark, France, Germany, Greece, Italy, Spain and The Netherlands)[13], has released a software code that can be used to create apps that will help track transmission chains of COVID-19[14]. Even though the Commission has been calling for a common approach to the use of tech and data to fight COVID-19 for months[15], not all EU member states have decided to use such code to develop their national tracking mobile application[16].

At the time of writing (30 July 2020), contact-tracing apps are already available or are quite ready to be released in Austria ("Stopp Corona" app[17]), Bulgaria ("ViruSafe" app[18]), Cyprus ("CovTracer" app[19]), Czech Republic ("eRouška" app[20]), France ("StopCovid" app[21]), Germany ("Corona-Warn-App"[22]), Hungary ("VirusRadar" app[23]), Italy ("Immuni" app), Latvia ("Apturi Covid" app[24]), Poland ("ProteGO Safe Safe" app[25]), Slovakia ("eKaranténa" app[26]) and Spain ("Radar Covid" app[27])[28].

---

13 See the official website at https://www.pepp-pt.org (last accessed 30 July 2020).

14 For a comment, see Cooper, D., Van Quathem, K., Oberschelp de Meneses, A., «COVID-19 Apps and Websites. The Pan-European Privacy Preserving Proximity Tracing Initiative and Guidance by Supervisory Authorities», *Inside Privacy*, 2 April 2020, https://www.insideprivacy.com/covid-19 (last accessed 30 July 2020).

15 Lomas, N., «Call for common EU approach to apps and data to fight COVID-19 and protect citizens' rights», *TechCrunch,* 8 April 2020, https://techcrunch.com (last accessed 30 July 2020).

16 France, most notably, has decided to develop its own source code for its national tracking mobile application. See Davis, S., «Could the coronavirus pandemic lead to mass surveillance in Europe?», *Euronews,* 31 March 2020, https://www.euronews.com (last accessed 30 July 2020).

17 See the official website at https://www.stopp-corona.at (last accessed 30 July 2020).

18 See the official website at https://virusafe.info (last accessed 30 July 2020).

19 See the official website at https://covid-19.rise.org.cy/en (last accessed 30 July 2020).

20 See the official website at https://erouska.cz (last accessed 30 July 2020).

21 See the description at the governmental website https://www.economie.gouv.fr/stopcovid# (last accessed 30 July 2020).

22 See the official website at https://www.coronawarn.app/en (last accessed 30 July 2020).

23 See the official website at https://virusradar.hu (last accessed 30 July 2020).

24 See the official website at https://covid19.gov.lv/en/covid-19/drosibas-pasakumi/apturi-covid-app (last accessed 30 July 2020).

25 See the official website at https://www.gov.pl/web/protegosafe (last accessed 30 July 2020).

26 See the official website at https://korona.gov.sk/ekarantena (last accessed 30 July 2020).

27 del Vayo, Á., «Radar COVID, la app oficial en España, ya se puede descargar», *El Espanol*, 30 June 2020, https://elandroidelibre.elespanol.com (last accessed 30 July 2020).

28 See the report issued by the European Union Agency for Fundamental Rights (FRA) analyzing the different technological solutions adopted by EU member states: FRA, «Coronavirus pandemic in the EU – Fundamental Rights Implications with a focus on contact-tracing apps», *FRA Bulletin*, 2, 28 May 2020, 52, https://op.europa.eu (last accessed 30 July 2020) and the Social Observatory for Disinformation and Social Media

Overall, EU member states have followed two different paths; while some of them (like Austria, Czech Republic, France, Germany, Hungary, Italy, Latvia, Poland and Spain) have based the implementation of the app on the Bluetooth technology, others (Bulgaria, Cyprus and Slovakia) have developed their mobile applications allowing the use of GPS location data[29].

As we will see more in detail in the following paragraphs, at the EU level, the eHealth Network and the European Commission have developed guidelines and recommendations for member states on how to best develop their mobile applications in order to comply with the EU human rights safeguards, and to ensure that the different apps are interoperable and can 'dialogue' among them[30].

2.1. The development of the 'Immuni' mobile application in Italy

Since March 2020, the discussion in Italy has been focused on the use and development of a tracking mobile application for monitoring the spread of COVID-19, especially in the so-called Phase 2 of the easing of lockdown measures[31].

On 23 March 2020, the Italian Ministry of Innovation launched a *fast call* for contribution (with the deadline set on 26 March 2020)[32]; as a result of the call, the "Immuni" app, developed by the Italian company Bending

---

Analysis (SOMA), «Is it true that Italy was the 'first major european country' to adopt a contract-tracing app?», *News*, 9 June 2020, https://www.disinfobservatory.org (last accessed 30 July 2020).

29 See Melissari, L., «Immuni e le altre app di contact tracing in Europa e nel mondo», *Internazionale.it*, 25 June 2020, https://www.internazionale.it (last accessed 30 July 2020) and FRA, op. cit., 53.

30 ECDC, op. cit.

31 While Phase 1 of the COVID-19 emergency (which started on 10 March 2020) was characterized by a strict lockdown on the Italian territory (with restriction of movement of persons and closure of commercial activities), the so-called Phase 2 (in force since 4 May 2020) and Phase 3 (from 3 June 2020) have seen a progressive easing of the restrictions. See the official website of the Italian government, http://www.governo.it (last accessed 30 July 2020).

32 See the call at the official website https://innovazione.gov.it (last accessed 30 July 2020). For a comment, Clarizia P., Schneider, E., «Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19», *IRPA – Osservatorio sullo Stato digitale*, 19 April 2020, https://www.irpa.eu (last accessed 30 July 2020).

Spoons, was selected among the projects submitted[33]. Soon after, on 31 March 2020, the Ministry of Innovation established a Task Force on data for the COVID-19 emergency ("Task force dati per l'emergenza Covid-19") that should advice the Italian government on the use of technological instruments during the COVID-19 pandemic. Among the studies produced by the Task Force, worth mentioning is the one related to the legal aspects connected to the use of mobile applications in tracking the spread of COVID-19[34]; based on this study, the government and Bending Spoons have further developed the mobile application. After the favorable opinion from the Data Protection Authority ("Garante per la protezione dei dati personali")[35], the Italian government adopted the legislative act regulating the use of the mobile application.

The relevant Legislative Decree was published on the Italian Official Journal on 30 April 2020[36]: it provides that the tracking mobile application should be used "only to warn those who have been in close contact with other that have been found positive to COVID-19 and safeguard their health through the preventive measures provided for the COVID-19 pandemic"[37]. This is indeed a blank provision, since the "preventive measures provided for the COVID-19 pandemic" are not clearly defined in the Decree, and instead they are linked to provisions included in other ministerial acts, which are constantly modified according to the evolving of the pandemic. The Legislative Decree specifies that the use of mobile application is voluntary[38] and the data gathered by the app will be cancelled, at the latest date, by the end of December 2020; moreover, the data collected will be used "only for the purpose of the app itself" until the end of the pandemic.

---

33 Bending Spoons has then developed and granted a permanent license for the source code to the Italian government free of charge, with the commitment to give the necessary support for the implementation of the app. See the official website of the Ministry of Innovation, https://innovazione.gov.it (last accessed 30 July 2020).

34 See the official website of the Task Force, https://innovazione.gov.it (last accessed 30 July 2020). For a comment, Clarizia and Schneider, op. cit.

35 Data Protection Authority, *Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19,* 29 April 2020, https://www.garanteprivacy.it (last accessed 30 July 2020).

36 Legislative Decree of 30 April 2020 No. 28 on urgent measures related to the COVID-19 pandemic (*Decreto Legislativo recante misure urgenti per la funzionalita' dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonche' disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*), https://www.gazzettaufficiale.it (last accessed 30 July 2020).

37 Article 6(1) of Legislative Decree 28/2020.

38 Article 6(4) of Legislative Decree 28/2020.

However, there is the possibility that they can be used also "for statistical or research purposes, in an aggregate and anonymous way"[39].

On 20 May 2020, Apple and Google released their updates, in order to allow the mobile developers around the world to proceed with the implementation of their applications. On 25 May 2020, Bending Spoons and the Ministry of Innovation published a part of the "Immuni" app source code, which follows the above-mentioned PEPP-PT software code, on the GitHub platform – a hosting platform for softwares[40].

On 8 June 2020, the "Immuni" mobile application was available for a one-week test in four Italian Regions (Liguria, Abruzzo, Marche and Apulia)[41], while it became available on the entire Italian territory on 15 June 2020, after the Data Protection Authority gave its final positive opinion[42] and after App Store e Google Play Store made available on their platforms the mobile application to be downloaded[43].

But how the "Immuni" app works in practice? This app uses the Bluetooth technology[44] to register in an anonymous way the codes from the devices it is close to[45]; it is based on a de-centralized system, so that all

---

39 Article 6(3) of Legislative Decree 28/2020.

40 See the official website of the Ministry of Innovation, https://innovazione.gov.it (last accessed 30 July 2020). See also the Editorial, «Immuni, pubblicato il codice sorgente dell'app (e l'icona ufficiale)», *Il Corriere della Sera*, 25 May 2020, https://www.corriere.it (last accessed 30 July 2020).

41 Berra, V., «Un mese di Immuni: pochi download e tanto disinteresse. Serve ancora un'app di contact tracing?», *Open*, 7 July 2020, https://www.open.online (last accessed 30 July 2020).

42 Italian Data Protection Authority, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19– App Immuni*, No. 9356568, 1 June 2020, https://www.garanteprivacy.it (last accessed 30 July 2020).

43 Pennisi, M., «Immuni, al via i test sull'app in tre Regioni», *Il Corriere della Sera*, 26 May 2020, https://www.corriere.it (last accessed 30 July 2020).

44 Even though the developers of the Bluetooth technology – Jaap Haartsen and Sven Mattisson – have recently highlighted that Bluetooth signals might be weakened by externa factors and the result of the 'tracking' might not be accurate. See Biddle, S., «The Inventors of Bluetooth Say There Could be Problems Using Their Tech for Coronavirus Contact Tracing», *The Intercept*, 5 May 2020, https://theintercept.com (last accessed 30 July 2020), Bay, J., «Automated contact tracing is not a coronavirus panacea», *Medium*, 11 April 2020, https://blog.gds-gov.tech (last accessed 30 July 2020) and Zinzocchi, R., «Ecco perché Immuni non serve e non funziona», *Orwell.live*, 16 May 2020, https://www.orwell.live (last accessed 30 July 2020).

45 Pennisi, op. cit.

data are not gathered and stored in a central server, rather, they remain on the single devices, which are 'in dialogue' with the central server[46].

In a nutshell, the procedure is the following:

1. the mobile devices on which the app has been installed, store in their own memories data from other devices they are in contact with (each external device is identified with an encrypted anonymous code) and some metadata (like the length of the contact);
2. when a user is tested positive to COVID-19, healthcare officers give her/him an authorization code through which the user can upload – at her/his own discretion – his/her encrypted anonymous code in the central ministerial server through the app;
3, other users can take from the central server the list of codes of those who have been tested positive; the device will then compare these codes with the ones that are already stored in the device; if there is a match, the app notifies the user that she/he may be at risk and provides advice on what to do next[47].

The data sent by the app to the central server can be consulted by the National Healthcare Service ("Servizio Sanitario Nazionale") to provide effective assistance to users, in compliance with Legislative Decree 28/2020[48]. The Ministry of Health has also established a national call center to support the citizens with the use of the app[49].

The Italian Ministry of Innovation Paola Pisano has declared that the app should be effective when about 25-30% of the Italian population uses it (around 12 millions people)[50]; this is in line of what the Google and Alphabet CEO Sundar Pichai has declared in a recent interview at *Wired*: "[e]ven if only 10 to 20 percent of users opt in [for the use of the tracking apps at the national level], this will have a real, meaningful

---

46 Luna, R., «Dieci cose che immuni non farà», *La Repubblica,* 25 May 2020, https://www.repubblica.it (last accessed 30 July 2020).

47 Berti, R., «Immuni, cos'è e come funziona l'app italiana coronavirus», *Agenda Digitale.eu,* 25 May 2020, https://www.agendadigitale.eu (last accessed 30 July 2020).

48 See the official description of the "Immuni" app, https://developers.italia.it (last accessed 30 July 2020).

49 See the official webpage of the Italian Ministry of Health, *Immuni contact-tracing App: available on all devices*, 4 June 2020, http://www.salute.gov.it (last accessed 30 July 2020).

50 Editorial, «App Immuni, il decreto: dati cancellati entro il 31 dicembre. Pisano: 'Funziona anche se la scarica il 25% di persone'», *La Repubblica,* 29 April 2020, https://www.repubblica.it (last accessed 30 July 2020).

impact"[51]. However, at the end of July 2020 (a month and a half after its release), only 4,1 milions people have downloaded the "Immuni" app in Italy[52]; moreover, Italian newspapers have reported some disfunctions of the mobile application, that have led many people to delete it from their smartphone devices[53].

Furthermore, it should be pointed out that "Immuni" is not the only tracking mobile application that has been developed in Italy. Indeed, other apps are in the process of being developed/implemented, based on private – and in some cases also regional – initiatives. We can briefly remind the "Protetti" app, based on the idea of the software project manager Michele Sciabarrà, leader of the NoiOpen community[54]. This mobile application – which is now undergoing the test phase – is based on open source DP-3T application, the decentralized app made by Switzerland and Austria[55]. Like the "Immuni" app, it works through the Bluetooth technology and data are collected in anonymous way; however, instead of being stored on the single devices, they are gathered in a central server, which manages the data in a centralized way[56]. To date, it is not very clear how many people are testing it and whether and when it will be ready for being downloaded.

Another mobile application that has been recently released (for free) on Google Play Store (and for a test in TestFlight for iOS devices), is the

---

51 Levy, S., «Sundar Pichai Says Google Doesn't Plan to Go Entirely Remote», *Wired*, 22 May 2020, https://www.wired.com (last accessed 30 July 2020). In Singapore, reports suggest only 17% of the population use the app. See Hern, A., «Digital contact tracing will fail unless privacy is respected, experts warn», *The Guardian,* 20 April 2020, https://www.theguardian.com (last accessed 30 July 2020).

52 Berra, op. cit.

53 See, among others, Rizzi, P., «Dopo 13 giorni in ostaggio di Immuni, ho deciso di eliminarla», *Business Insider Italia*, 17 July 2020, https://it.businessinsider.com (last accessed 30 July 2020), Mucciarelli, B., «Immuni ferma a 4 milioni di download. Un'occasione persa per gli italiani contro il COVID-19?», *Hardware Upgrade*, 2 July 2020, https://www.hwupgrade.it (last accessed 30 July 2020), Villa, S., «Immuni, il nostro test: privacy rispettata, ma cosa succede a chi viene "allertato"?», *Altroconsumo.it*, 15 June 2020, https://www.altroconsumo.it (last accessed 30 July 2020) and Ricca, P., Sarcinelli, A., «Immuni, tra diffidenza e speranze. Il vox di Italiani come noi sulla app anti contagio: 'Poco diffusa, non serve', 'Strumento importante, la scarico'», *Il Fatto Quotidiano*, 18 July 2020, https://www.ilfattoquotidiano.it (last accessed 30 July 2020).

54 See the official website NoiOpen Community, https://noiopen.it (last accessed 30 July 2020).

55 Sorge, L., «COVID-19 & Open Source: a Shared Global Approach to Emergencies», *CodeMotion*, 1 May 2020, https://www.codemotion.com (last accessed 30 July 2020).

56 Zinzocchi, R., «Meglio Protetti che Immuni», *Orwell.live*, 10 May 2020, https://www.orwell.live (last accessed 30 July 2020).

SM_COVID19 app by Softmining Srl, an Italian Company; the app has been downloaded so far by more that 52.000 persons. It is also based on the Bluetooth technology (but it can also work based on the GPS system, if the user activates this specific option), it is able to work in background and the data are gathered in anonymized form in a database that is "shared with healthcare authorities". Once downloaded on its own device, the user is able to send a message in case she/he is tested positive to COVID-19; in this case, as the official website reports "a specialist will contact you to provide the relevant healthcare instructions"[57]. As in the case of the "Protetti" App, it is based on a centralized system. It is not specified with which Italian authorities Softmining is actually working for the implementation of this mobile application and whether so far some users have received alert messages. Both NoiOpen[58] and Softmining have declared their availability to share their experting with the Italian government in order to finalize the "Immuni" App, even though it is not clear whether they are all collaborating[59].

Also some Italian Regions seem to be in the process of developing alternative tracking systems, as in the case of STOPcovid19, developed by Webtek S.p.A. and based on the GPS tracking method that the Umbria Region would like to test on its territory – even though it is not ready yet[60].

Overall, this has created a fragmentation in the development of tracking mobile applications[61], as also outlined by the Data Protection Authority, who has warned against the "proliferation of […] initiatives [similar to the "Immuni" App] at the public level, which are hardly compatible with the current legal framework of reference"[62]. Indeed, it is not clear how many tracking mobile applications (apart from the "Immuni" app) will be released in their final versions and, in this case, how they will "dialogue"

---

57 See the official website at https://www.smcovid19.org (last accessed 30 July 2020). See also Mensurati, M., Tonacci, F., «Coronavirus, le polemiche su Immuni lanciano la app concorrente: boom di download per Sm-Covid-19», *La Repubblica*, 21 April 2020, https://www.repubblica.it (last accessed 30 July 2020).

58 See the official website, https://www.protetti.app (last accessed 30 July 2020).

59 Ibid.

60 See the official website, https://www.stopcovid19.it/it (last accessed 30 July 2020) and the interview by Barlassina, M., «Il creatore dell'app italiana che traccia il Coronavirus: 'Perché sarà ancora più utile dopo la fine dell'emergenza'», *Forbes*, 27 March 2020, https://forbes.it (last accessed 30 July 2020).

61 Schneider, E., «Le nuove tecnologie e l'emergenza epidemiologica da Covid-19: un'occasione da non perdere», *IRPA – Osservatorio sullo Stato digitale*, 30 April 2020, https://www.irpa.eu (last accessed 30 July 2020).

62 Data Protection Authority, *Parere sulla proposta normativa,* op. cit.

among themselves (or how they are in dialogue now, especially as regards the SM_COVID19 app) in order to avoid fragmentation in the collection of data.

3. TRACKING MOBILE APPLICATION(S) AND THE RIGHT TO PRIVACY: WHERE DO WE STAND NOW IN EUROPE?

Tracking mobile applications, like the "Immuni" app in Italy, raise a number of questions about the right to privacy and data protection. The mobile applications will be "in dialogue" with a central platform gathering information from the private citizens' smartphones where the apps will be downloaded and installed; this means that data will flow between private devices and a central (governmental) server. Here we briefly recall which are main privacy issues at stake when we talk about tracking mobile applications, also in light of the European and international legal framework of reference.

When talking about tracking mobile applications, two main questions should be answered, namely (1) whether the use of the mobile application will be mandatory or not (or whether citizens will be "invited" to use the app so that to gain some benefits of any kind)[63] and (2) whether the right to privacy is respected, namely which data will be collected (e.g. location data and/or other identifiable information), by whom and through which forms, for how long and for which purposes.

Since the use of tracking mobile applications is being implementing by several governments around the world, privacy-related concerns have been addressed not only at the national and European levels, but also at the international level.

On 13 May 2020, the UN Office for the Coordination of Humanitarian Affairs (UN OCHA) issued a "Guidance COVID-19" with a call to respect human rights during the COVID-19 pandemic; with regard to the right to privacy, the UN OCHA has made it clear that "surveillance and monitoring [techniques] should be specifically related to and used exclusively for public health-specific aims"[64]. This document follows the joint call that

---

63 See McGregor, op. cit.

64 UN Office for the Coordination of Humanitarian Affairs, *Guidance COVID-19,* 13 May 2020, https://www.unocha.org/covid19 (last accessed 30 July 2020).

Human Rights Watch and more than 100 other organisations adopted on the use of digital surveillance by governments during the COVID-19 pandemic, which recalls that "[…during] extraordinary times, […] human rights law still applies"[65].

Indeed, while governments should protect the public health[66], they should still respect the other fundamental human rights. As recalled by the United Nations Committee on Economic, Social and Cultural Rights, "[t] he right to health is closely related to and dependent upon the realization of other human rights, […] including […] *privacy*, access to information […]. These and other rights and freedoms address integral components of the right to health" [emphasis added][67].

Nevertheless, it is also true that in times of a global pandemic such as COVID-19, governments can adopt extraordinary measures to prevent and mitigate the health crisis[68]; by doing so, they "may take measures derogating from their [human rights] obligations" (including also the right to privacy), as specified by article 4 of the International Covenant on Civil and Political Rights[69] and article 15 of the European Convention on Human Rights[70]. However, such derogations should meet some strict requirements, namely

---

65 Human Rights Watch, «Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights», 2 April 2020, https://www.hrw.org (last accessed 30 July 2020).

66 According to article 12 of the International Covenant on Economic, Social and Cultural Rights, everyone has the right to "the highest attainable standard of physical and mental health" and governments are obligated to take effective steps for the "prevention, treatment and control of epidemic, endemic, occupational and other diseases". See the text of the International Covenant on Civil and Political Rights, adopted on 16 December 1966 and entered into force on 23 March 1976, https://www.ohchr.org (last accessed 30 July 2020).

67 United Nations Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12),* 11 August 2000, https://www.refworld.org (last accessed 30 July 2020).

68 United Nation Human Rights Office of the High Commissioner, *COVID-19: States should not abuse emergency measures to suppress human rights*, 2020, https://www.ohchr.org (last accessed 30 July 2020).

69 Article 4: "1. In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation […]".

70 Article 15: "1. In time of […] public emergency […] any […] Party may take measures derogating from its obligations under [the] Convention to the extent strictly required by the exigencies of the situation […]". See European Court of Human Rights, *Guide on Article 15 of the European Convention on Human Rights,* 31 December 2019, https://www.echr.coe.int (last accessed 30 July 2020).

they should be lawful, necessary, proportionate, and limited in duration[71], as also established by the jurisprudence of the European Court of Human Rights[72].

At the European Union (EU) level, the European Commission adopted on 8 April 2020 a recommendation calling for a coordinated approach on the use of tracking mobile applications in Europe, in order to ensure the protection of "fundamental rights and freedoms, particularly the rights to privacy and protection of personal data"[73], In particular, any "restrictions on the exercise of the fundamental rights and freedoms laid […] must be justified […] proportionate [….and] temporary"[74].

The European Commission Recommendation is in line with the current European legislative framework: article 8 of the EU Charter of Fundamental Rights recognizes the right to protection of personal data[75], while Regulation 2016/679 (General Data Protection Regulation or GDPR)[76] on the protection of personal data of natural persons regulates the condition under which personal data, including data related to health, can be processed. In particular, "such data may be processed […] when a data subject gives her explicit consent or when processing is in the public interest as specified in Member State or Union law, in particular for monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health"[77].

---

71 The United Nations Human Rights Committee stated that restrictions on the right to privacy must take place only "in cases envisaged by the law" and should be "proportionate to the end sought, and [...] necessary in the circumstances of any given case". United Nations, *Human Rights Instruments. Volume I. Compilation of general comments and general recommendations adopted by human rights treaty bodies,* HRI/GEN/1/Rev.9 Vol. I, 27 May 2008, 193.

72 See, e.g., European Court of Human Rights (First Section), *Catt v. the United Kingdom*, Application no. 43514/15, Judgment, 24 January 2019, para. 109 and European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights,* 31 August 2019, https://www.echr.coe.int (last accessed 30 July 2020).

73 Commission Recommendation 2020/518 of 8 April 2020 *on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data,* C/2020/3300, para. 3.

74 Commission Recommendation 2020/518, para. 23.

75 Article 8 (Protection of personal data): "1. Everyone has the right to the protection of personal data concerning him or her". See the text of the Charter of Fundamental Rights of the European Union at https://eur-lex.europa.eu (last accessed 30 July 2020).

76 Regulation 2016/679 of the European Parliament and of the Council *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* 27 April 2016.

77 Article 6(1)(c) or (e) and Article 9(2)(i) of Regulation 2016/679.

Following the European Commission recommendation, the eHealth Network[78] issued on 15 April 2020 a *Common EU Toolbox for Member States* for developing and implementing tracking mobile applications[79]. The aim is to offer a practical guide for member states and to avoid "[…a] fragmented and uncoordinated approach to contact tracing apps [which] risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis, whilst also causing adverse effects to the single market and to fundamental rights and freedoms"[80].

In particular, according to the Toolbox, the mobile applications should present the following "essential requirements […] namely that they be: voluntary; […] privacy-preserving […]; and dismantled as soon as no longer needed"[81]. Additionally, the eHealth Networks calls for a special attention to cybersecurity: to this end, "Member States are recommended to carry out a national risk assessment to identify and mitigate possible risks of abuse"[82].

Based on this Toolbox, and on further consultation with the European Data Protection Board (EDPB), on 16 April 2020 the European Commission issued a set of guidelines for the development of contact tracing and warning apps, making it clear that "[t]he functionalities included in the apps can have different impact on a wide range of rights enshrined in the Charter of Fundamental Rights of the EU, such as human dignity, *respect for private and family life, protection of personal data*, the freedom of movement, nondiscrimination, freedom to conduct a business, and freedom of assembly and of association" [emphasis added][83]. Consequently, the European Commission restated that the mobile applications should comply with EU data protection rules, in particular with the GDPR provisions[84]. All these requirements have been then reiterated in the guidelines adopted on 21 April 2020 by the EDPB[85].

---

78 The eHealth Network was set up under article 14 of Directive 2011/24/EU of 9 March 2011 *on the application of patients' rights in cross-border healthcare* in order to provide a platform of Member States' competent authorities dealing with digital health. See the official webpage at https://ec.europa.eu (last accessed 30 July 2020).

79 eHealth Network, op. cit.

80 Ibid., 7.

81 Ibid., 5.

82 Ibid., 18.

83 European Commission, *Communication. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection,* 2020/C 124 I/01, 16 April 2020, 4.

84 European Commission, *Digital technologies – innovative solutions during the coronavirus crisis,* May 2020, https://ec.europa.eu (last accessed 30 July 2020).

85 European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,* 21 April 2020, https://edpb.eu-

At the European level, it is also worth recalling also that the 47 member states of the Council of Europe are parties of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was signed in 1981and then updated in 2018[86].

This Convention includes rules and principles which are similar to those provided by the EU GDPR[87]. Furthermore, a recent joint statement of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe calls for member states to implement digital contact-tracing in line with the Convention for the protection of individuals with regard to the processing of personal data[88].

Overall, the European regional data protection framework provides that, while processing personal data, member states respect a set of principles, including lawfulness, fairness and transparency[89].

In the next paragraph, we will see more in detail how, in the case of Italy, the Legislative Decree 28/2020 has addressed the privacy concerns regarding the "Immuni" app and which questions are still unanswered.

3.1. A focus on the debate in Italy

In Italy, after the adoption at the EU level of the GDPR, the relevant national legal framework on the right to privacy and data protection has been modified so that to be in line with the EU regulations; in particular,

---

ropa.eu/edpb_en (last accessed 30 July 2020). For a comment, see van Kolfschooten, H., de Ruijter, A., «COVID-19 and privacy in the European Union: A legal perspective on contact tracing», *Contemporary Security Policy*, 41, 30 May 2020, 488, Davis, S., «Could the coronavirus pandemic lead to mass surveillance in Europe?», *Euronews*, 31 March 2020, https://www.euronews.com (last accessed 30 July 2020) and FRA, op. cit.

86 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, signed on 28 January 1981, and Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223, signed on 10 October 2018. The consolidated text of the Convention is available at http://rm.coe.int. (last accessed 30 July 2020).

87 Mendos Kuskonmaz, E., Guild, E., «Covid-19: A New Struggle over Privacy, Data Protection and Human Rights?», *European Law Blog*, 4 May 2020, https://europeanlawblog.eu. (last accessed 30 July 2020).

88 Committee of Convention 108, Data Protection Commissioner of the Council of Europe, *Joint Statement on Digital Contact Tracing*, 28 April 2020, https://rm.coe.int (last accessed 30 July 2020). For a comment, see FRA, op. cit.

89 Mendos Kuskonmaz and Guild, op. cit..

the Legislative Decree 101/2018[90] made substantial amendments to the so-called data protection code (Legislative Decree 196/2003, which was also based on EU law, i.e. on Directive 95/46/EC)[91].

The debate in Italy over privacy concerns in the implementation of tracking mobile applications during the COVID19 pandemic has been well summarized in the Open letter on the use of tracking mobile applications prepared by the Nexa Center for Internet & Society of the Politecnico of Turin in Italy[92], which recalls the above mentioned European safeguards in the development and implementation of the mobile application.

To date, the "Immuni" app seems to respect the main technical characteristics suggested at the EU level, as specified in the Legislative Decree 28/2020: it is not mandatory[93]; it uses a decentralized system of collecting data[94]; the data collected (which will not include personal or

---

90 Legislative Decree No. 101/2018 of 10 August 2018 (*Decreto Legislativo. Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*), Official Journal N. 205 of 4 September 2018, https://www.gazzettaufficiale.it (last accessed 30 July 2020).

91 Legislative Decree No. 196/2003 of 30 June 2003 (*Decreto Legislativo. Codice in materia di protezione dei dati personali*), Official Journal No. 174 of 29 July 2003. English translation at http://www.privacy.it (last accessed 30 July 2020).

92 Nexa Center for Internet & Society, *Tracciamento dei contatti e democrazia: lettera aperta ai decisori*, 20 April 2020, https://nexa.polito.it (last accessed 30 July 2020). For similar articles that have been published on Italian and foreign newspapers, see, among other, Ulivieri, V., «App Immuni: prima di tracciare i contagi ci vuole chiarezza sui dati», *Osservatorio Diritti*, 22 April 2020, https://www.osservatoriodiritti.it (last accessed 30 July 2020), Iaselli, M., «App Immuni vs Covid-19: ma è una soluzione davvero efficace?», *Altalex*, 20 April 2020, https://www.altalex.com (last accessed 30 July 2020), Amante, A., «Italy launches COVID-19 contact-tracing app amid privacy concerns», *Reuters*, 1 June 2020, https://www.reuters.com (last accessed 30 July 2020) and Amante, A., Pollina, E., «Italians embrace coronavirus tracing app as privacy fears ease», *Reuters*, 11 June 2020, https://www.reuters.com (last accessed 30 July 2020).

93 Article 6(4) of Legislative Decree 28/2020.

94 In a centralized systems, a central server gathers all the signals transmitted between devices by the Bluetooth technology; in a de-centralized system, on the other hand, the central serve gathers only the signals that a device sends. While the centralized system has the advantage to monitor in a more accurate way the 'map' of contacts, the risks of privacy violations are higher. This is why also from the European Commission and the Italian Data Protection Authority there has been a request to use a de-centralized system. See European Commission Recommendation (EU) 2020/518 of 8 April 2020 and the interview to the President of the Data Protection Authority Antonello Soro at Radio Capital Circo Massimo on 22 April 2020, https://www.garanteprivacy.it (last accessed 30 July 2020). For a comment, Schneider, E., «Immuni e tutela della privacy:

sensitive data, but only "data necessary to alert the user that she/has been in contact with someone who has been tested positive to COVID19"[95]) will be cancelled at the end of the health emergency and will be used "only for the purpose of the app itself" and "for statistical or research purposes, in an aggregate and anonymous way"[96].

However, some questions are still unanswered. Firstly, Legislative Decree 28/2020 does not specify how many subjects/entities will have access to the data collected by the app: in the implementation phase, it has been established that the data are accessible by the Ministry of Health and the National Healthcare Service, but it is not clear whether, for example, the Italian company that has developed the mobile application (Bending Spoons), or Apple and Google, as technology providers, have the possibility to access some data[97]. Secondly, it is still not very clear what the person receiving the alert from the app should do: for now, the mobile application sends an alert to the users with the indication to call her/his doctor (who, in turn, should contact the local health authority for any further steps to take), but it is still unclear whether she/he should put her/himself immediately in self-isolation (and, if so, for how many days). Another issue concerns the anonymization of data: since anonymized data can be combined[98] with other data to re-identify individuals[99], it would be necessary for the government to clearly prohibit the practice of "re-combination" of anonymized data[100].

The Italian Data Protection Authority has also warned against the cybersecurity (like malware or identity theft) and data breaches risks of the mobile application: even though the government has introduced some

---

'un nodo irrisolto'», *IRPA – Osservatorio sullo Stato digitale*, 30 April 2020, https://www.irpa.eu (last accessed 30 July 2020).

95 Article 6(2b) of Legislative Decree 28/2020.

96 Article 6(3) of Legislative Decree 28/2020. For all the technical characteristics of the "Immuni" App, see the dedicated webpage of the Italian Ministry of Innovation, https://innovazione.gov.it (last accessed 30 July 2020).

97 Article 6(3) of Legislative Decree 28/2020.

98 See Thompson, S.A., Warzel, C., «Twelve Million Phones, One Dataset, Zero Privacy», *New York Times,* 19 December 2019, https://www.nytimes.com (last accessed 30 July 2020).

99 See Harrison, S., «When Is Anonymous Not Really Anonymous?», *The Markup*, 24 March 2020, https://themarkup.org (last accessed 30 July 2020).

100 Article 6(2d) of Legislative Decree 28/2020 states that the Ministry of Health will ensure that "adeguate measure [will be taken] to avoid the risk of re-indentification of the owners of the data that have been pseudonymised"; it does does not clearly prohibit the re-indification practice, and does not refer to anonymized data.

cybersecurity safeguards, the Data Protection Authority has called for a more transparent communication of such risks to all users and for the enhancement of further safeguards (for example, establishing for how long the single mobile devices should store the data gathered from other devices, and keeping track of all operations of the governmental data protection officers when collecting and processing the data). Furthermore, the Data Protection Authority has insisted on gathering feedback from the users of the mobile application (for now, the Ministry of Health has decided to postpone the feedback phase "due to the relevant debate on media tools and the necessity to take immediate and urgent measures to monitor the spread of the COVID-19 pandemic") and to take into due account the opinions received in the further development of the "Immuni" app[101].

Finally, another important question is whether the app will be the only mobile application in Italy or whether it will be operative together with the other mobile applications that are being developing (and partly implementing) in these days (like the above mentioned "Protetti", SM_COVID19 and STOPcovid19 apps). These mobile applications use different data storage systems (for example, the SM_COVID19 allows the use of geo-location data collected through the GPS system, which has been expressly excluded by Legislative Decree 28/2020)[102]; the use of such applications may pose some problems with respect to the right to privacy and data protection of the users.

To date, the Data Protection Authority has simply warned against the proliferation of different initiatives similar to the "Immuni" app and it remains to be seen whether the governmental authorities will take some decisions in this respect.

4. SOME CONCLUDING REMARKS

As the previous paragraphs have shown, at the international and European levels several efforts have been taken to call on states to respect their human rights obligations, and in particular the right to privacy, while developing and implementing tracking mobile applications to monitor the spread of the COVID-19 pandemic. In Italy, the "Immuni" app seems to positively answer the main privacy concerns, even though some questions

---

101 Data Protection Authority, *Provvedimento di autorizzazione*, op. cit.

102 Article 6(2c) of Legislative Decree 28/2020.

are still unanswered; moreover, the proliferation of alternative tracking mobile applications risks to complicate the framework of reference.

To this end, it seems important that national governmental authorities increase their efforts to finalize a single mobile application that ensures the highest level of safeguards to protect the right to privacy and data protection of users. In this respect, a governance approach should be adopted, not only at the national level, establishing an effective dialogue with all the relevant stakeholders[103], but also at the European and international level, in order to ensure that the several mobile applications will be similar in their use and will ensure the same level of privacy, in order to avoid discrimination among citizens living in different countries and having access to different apps[104].

As recalled by the eHealth Network, "an *integrated governance* is useful to prepare and implement the measures [related to the tracking mobile applications], involving not only health, but also other authorities (including data protection authorities), as well as the private sector, experts, academics and stakeholders such as patients groups" [emphasis added][105].

---

103 As also outlined by the OECD, op. cit., 4.

104 Access Now, *Recommendations on Privacy and Data Protection in the Fight against COVID-19*, March 2020, 24, https://www.coe.int (last accessed 30 July 2020).

105 eHealth Network, op. cit., 20-21.