UNIO - *EU Law Journal*. Vol. 6, No. 2, July 2020, pp 35-48.

School of Law – University of Minho

Digital contact tracing and data protection: assessing the French and Portuguese applications

Luis Felipe Miranda Ramos*

ABSTRACT: The rapid outbreak of COVID-19 has necessitated a global response to manage the transmission, spread, and impact of the virus. Many countries started developing digital contact tracing applications to contribute to the process of lifting the restrictions imposed on its citizens. Generally, the protection of personal data is a right that appears in constitutional and legal provisions, and its processing can only be performed under very restricted circumstances, the protection of health being a valid justification. This article focusses on the systems developed as digital contact tracing tools in France (StopCovid) and in Portugal (STAYAWAY COVID), presenting their characteristics and the most relevant aspects concerning the processing of personal data. The most relevant positive characteristics of these systems are their voluntary adoption, their developers' concern with the people's security and privacy, and the transparency of their functioning. With the negative characteristics, the most relevant are the restricted interoperability with the systems from other EU countries, and the permanent risk to people's privacy of collecting lists of contacts and the circumstances of their interactions with other users of the systems.

KEYWORDS: COVID-19 applications – digital contact tracing – privacy – data protection – GDPR.

* Ph.D. candidate in Law at the University of Minho and member of the Research Centre for Justice and Governance (JusGov).

1. Introduction

The rapid outbreak of the SARS-CoV-2 ("COVID-19"), originating in Wuhan, China at the end of 2019 and the subsequent declaration of "pandemic" by the World Health Organisation ("WHO") on March 11, 2020, has necessitated a global response to manage the transmission, spread and impact of the virus.[1]

To mitigate and contain the viral spread, many countries around the world have, in a first moment, turned to restriction orders, such as mandatory quarantines and home confinements. As the disease came under some control, they started to lift the restrictions. Many countries have been taking several vital measures to contribute to this lifting process, some of which involve the use of technology.[2]

Digital innovations to educate, connect, and alert the residents via web and mobile application platforms have proliferated around the world. However, like many digital applications requiring the processing of personal data, the digital systems developed to fight COVID-19 raise concerns about the balance between public health utility and personal privacy. The success of digital interventions depends on the trust they ensure. Striking this balance has been a challenge that needs to be overcome, not only for short term COVID-19 response but also for the mid and long-term responses to the ensuing post-COVID-19 era.

In that sense, it is expected that many of these often invasive technological measures will be de-escalated when the threat of COVID-19 is over or will cease to be useful, but some will likely be maintained, enhanced, and reoriented for other purposes, if not faced with proper regulation.[3]

Nevertheless, most digital measures adopted are still recent, being in the first stages of implementation, and have not yet reached their full capacity and impact. It is already possible to realise which measures were preferred by most countries and analyse the conditions of its deployment and the possible impact they can have on the protection of personal data.

This article aims to present some of the technological measures adopted by countries worldwide and then, zeroing in on the measures of digital contact tracing ("CT"), present the characteristics and assessments on the processing of personal data performed by the systems adopted in two European Union countries, namely, France and Portugal. The reason for choosing these systems, the context of the development, their similarities, and their differences will be expanded upon within the different sections of this paper.

The remainder of this work is organised as follows: in the next section a literature review on the adoption of measures to tackle the spread of contagious diseases

[1] Qijun Gao et al., "The epidemiological characteristics of 2019 novel Coronavirus diseases (COVID-19) in Jingmen, China", SSRN, 2020, https://doi.org/10.2139/ssrn.3548755.

[2] As examples of measures adopted by some countries, it is possible to refer to China and Singapore, which adopted tracking systems through the use of migration maps and real-time data provided by smartphones and wearable devices, and to France, where some cities incorporated facial recognition technology to their public transportation video surveillance systems, in order to monitor the use of masks by their citizens. For further information on those technologies, see Sera Whitelaw et al., "Applications of digital technology in COVID-19 pandemic planning and response", *The Lancet Digital Health*, v. 2, no. 8 (August 2020): e435–40, https://doi.org/10.1016/S2589-7500(20)30142-4; Luis Felipe M. Ramos, "Evaluating privacy during the COVID-19 public health emergency: the case of facial recognition technologies", in *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance - ICEGOV'20* (Athens, Greece: ACM Press, 2020), https://doi.org/10.1145/3428502.3428526.

[3] Ramos, "Evaluating privacy during the COVID-19 public health emergency".

is presented; section 3 presents some data on the measures adopted worldwide to battle the COVID-19 pandemic, with focus on the French and Portuguese systems. Lastly, section 4 presents some conclusions.

2. Traditional measures against contagious disease

Traditionally, to control the spread of contagious diseases, many different measures can be adopted, from a pharmaceutical approach, like prophylactic vaccination and drug treatments, to pre-emptive culling. One possible approach is to interrupt the transmission from person to person, which can be achieved through the reduction of epidemiological contact (*i.e.*, social distancing) or through tracing the contacts of known cases (*i.e.*, contact tracing).[4]

From these measures, epidemiological CT is considered crucial to prevent further transmission of many infectious diseases, from early cases of novel infectious to endemic sexually transmitted infections.[5] This occurs due to the human behavior of moving across locations, which contributes to the transmission of communicable diseases, requiring the adoption of actions that can interrupt this contagious process.[6]

CT can be defined as identifying and examining relevant contacts of infectious cases (often called index case), performing adequate testing for the presence of infection or disease and, if necessary, providing of appropriate therapy before the occurrence of serious illness.[7] According to the WHO, three basic elements compose CT:[8]

- Contact identification: to identify persons who may have been exposed to the disease as a result of being in contact with an infected person;
- Contact listing: to trace and communicate with the identified contacts, and to provide information about suitable infection control measures, symptom monitoring and other precautionary measures such as the need for quarantine;
- Contact follow-up: to monitor the contacts regularly for symptoms.

The adoption of CT by public health authorities in the context of controlling the outbreak of COVID-19 has been recommended by the European Centre for Disease Prevention and Control ("ECDC")[9] and the WHO, which provided guidelines for its implementation.[10]

---

[4] Thomas House and Matt J. Keeling, "The impact of contact tracing in clustered populations", *PLoS Computational Biology*, v. 6, no. 3 (March 26, 2010): e1000721, https://doi.org/10.1371/journal.pcbi.1000721.

[5] Benjamin Armbruster and Margaret L. Brandeau, "Contact tracing to control infectious disease: when enough is enough", *Health Care Management Science*, v. 10, no. 4 (December 2007): 341–55, https://doi.org/10.1007/s10729-007-9027-6; Saskia Glasauer et al., "International tuberculosis contact-tracing notifications in Germany: analysis of national data from 2010 to 2018 and implications for efficiency", *BMC Infectious Diseases*, v. 20, no. 1 (December 2020): 267, https://doi.org/10.1186/s12879-020-04982-z; House and Keeling, "The impact of contact tracing in clustered populations".

[6] Bouke C. de Jong et al., "Ethical considerations for movement mapping to identify disease transmission hotspots", *Emerging Infectious Diseases*, v. 25, no. 7 (July 2019), https://doi.org/10.3201/eid2507.181421.

[7] Glasauer et al., "International tuberculosis contact-tracing notifications in Germany"; Sadamori Kojaku, Laurent Hébert-Dufresne and Yong-Yeol Ahn, "The effectiveness of contact tracing in heterogeneous networks", *ArXiv:2005.02362 [Physics, q-Bio]*, May 5, 2020, http://arxiv.org/abs/2005.02362.

[8] World Health Organization (WHO), *Contact tracing during an outbreak of Ebola virus disease* (Brazzaville, Republic of Congo: World Health Organization, September 2014), http://www.who.int/csr/resources/publications/ebola/contact-tracing-during-outbreak-of-ebola.pdf.

[9] "Contact tracing for COVID-19: current evidence, options for scale-up and an assessment of resources needed", European Centre for Disease Prevention and Control (ECDC), April 2020, https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-Contract-tracing-scale-up.pdf.

[10] "2019 novel Coronavirus (2019-nCoV): strategic preparedness and response plan", World Health

Nonetheless, the traditional CT by following up cases and contacts using public health staff is resource-intensive.[11] In this context, the adoption of solutions based on Information and Communication Technologies ("ICT"), such as contact management software (e.g., the WHO-provided Go.Data)[12] and mobile CT applications, can improve the efficiency of CT methods.[13]

Nowadays, the use of personal digital devices is ubiquitous, with an estimate 8.3 billion mobile-cellular telephone subscriptions worldwide in 2019, representing approximately 108 subscriptions per 100 inhabitants, and 97% of the world population living within reach of a mobile cellular signal,[14] which presents an outstanding tool to perform digital CT.

For that reason, we have seen many different systems being deployed worldwide, developed by governments, private actors, research institutions, among others. The variety of applications available have been developed using different specifications and characteristics, such as different mobile platforms, communication protocols, data storage, etc., and for that reason, they must be evaluated considering how much attention they pay to data protection.

Even before the outbreak of COVID-19, several contact tracking applications involving mobile applications, wireless technologies, and GPS have been presented in the literature[15]. Considering the increasing concern about the protection of personal data, some of the most recently released applications propose privacy-oriented solutions[16]. All these tools vary in purpose, features, and complexity.

However, just like the traditional CT methods raise privacy concerns,[17] digital

---

Organization, March 2, 2020, https://www.who.int/publications/i/item/strategic-preparedness-and-response-plan-for-the-new-coronavirus; "Contact tracing in the context of COVID-19", World Health Organization (WHO), October 5, 2020, https://apps.who.int/iris/rest/bitstreams/1277571/retrieve; "Critical preparedness readiness and response actions COVID-19", World Health Organization (WHO), March 22, 2020, https://apps.who.int/iris/rest/bitstreams/1272587/retrieve.

[11] Alex Berke et al., *Assessing disease exposure risk with location data: a proposal for cryptographic preservation of privacy*, *ArXiv:2003.14412 [Cs]*, April 8, 2020, http://arxiv.org/abs/2003.14412.

[12] See: https://www.who.int/godata/about.

[13] de Jong et al., "Ethical considerations for movement mapping to identify disease transmission hotspots"; "Contact Tracing for COVID-19", ECDC; Luca Ferretti et al., "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing", *Science*, v. 368, no. 6491 (May 8, 2020): eabb6936, https://doi.org/10.1126/science.abb6936.

[14] International Telecommunication Union (ITU), *Measuring digital development - facts and figures 2019* (Geneva, Switzerland: International Telecommunication Union, 2019), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

[15] Thamer Altuwaiyan, Mohammad Hadian and Xiaohui Liang, "EPIC: efficient privacy-preserving contact tracing for infection detection", in *2018 IEEE International Conference on Communications* (ICC) (Kansas City, MO: IEEE, 2018), 1–6, https://doi.org/10.1109/ICC.2018.8422886; Lisa O. Danquah et al., "Use of a mobile application for Ebola contact tracing and monitoring in Northern Sierra Leone: a proof-of-concept study", *BMC Infectious Diseases*, v. 19, no. 1 (December 2019): 810, https://doi.org/10.1186/s12879-019-4354-z; Emmenual Reddy et al., "Mobile application for Dengue fever monitoring and tracking via GPS: case study for Fiji", *ArXiv:1503.00814 [Cs]*, March 2, 2015, http://arxiv.org/abs/1503.00814.

[16] Alex Berke et al., "Assessing disease exposure risk with location data: a proposal for cryptographic preservation of privacy", *ArXiv:2003.14412 [Cs]*, April 8, 2020, http://arxiv.org/abs/2003.14412; Arvin Hekmati, Gowri Ramachandran and Bhaskar Krishnamachari, "CONTAIN: privacy-oriented contact tracing protocols for epidemics", *ArXiv:2004.05251 [Cs]*, April 10, 2020, http://arxiv.org/abs/2004.05251.

[17] Matthew L Levine, "Contact tracing for HIV infection: a plea for privacy", *Columbia Human Rights Law Review*, v. 20, no. 1 (1988): 157–202; Randolph F. Wykoff et al., "Contact tracing to identify human immunodeficiency virus infection in a rural community", *JAMA: The Journal of the American Medical*

CT presents privacy risks, which must be carefully addressed for individuals to place trust in the applications. As these systems deal with personal data, location data, and sometimes even special categories of data, such as health data, they required intense scrutiny of their data protection policies and practices.[18]

The protection of privacy for infected persons, besides being a legal requirement in most jurisdictions, also represents a critical requirement to facilitate the cooperation of individuals. Risks to privacy from traditional and digital CT vary from data breaches to government surveillance. Examples of governmental mass surveillance can be seen in Israel, that approved emergency legislation allowing the government to use sensitive data to track coronavirus carriers,[19] and in South Korea, that deployed a government-controlled central database[20] that stores tracking data from mobile phones along with credit card records, surveillance video and personal interviews with patients in order to track the infectious spreading.

In order to mitigate these risks, the European Commission went ahead and issued guidelines for apps supporting the fight against COVID-19 pandemic concerning data protection,[21] while the European Data Protection Board ("EDPB") published some guidelines on the use of location data and CT tools.[22] The US Centers for Disease Control and Prevention ("CDC") has also published some criteria for evaluating digital CT tools.[23]

3. Technological tools deployed to fight COVID-19

As the understanding of the mechanisms involved in the proliferation of the virus increased and the containment measures presented relevant results in the controlling of the spreading, many countries started developing strategies to lift the restrictions imposed on their citizens and turned to digital solutions to contribute to this process.

Concerning the measures deployed worldwide, some of them may be considered more privacy-invasive, while others were adopted with the protection of personal data in mind. On the first group of measures, it is possible to highlight systems that incorporate biometric technologies, especially facial recognition technologies, which,

---

Association, v. 259, no. 24 (June 24, 1988): 3563–66, https://doi.org/10.1001/jama.259.24.3563.

[18] Shakila Bu-Pasha et al., "EU Law perspectives on location data privacy in smartphones and informed consent for transparency", *European Data Protection Law Review (EDPL)*, v. 2, no. 3 (2016): 312–23, https://doi.org/10.21552/EDPL/2016/3/7; Lawrence O. Gostin, Sam F. Halabi and Kumanan Wilson, "Health data and privacy in the digital era", *JAMA*, v. 320, no. 3 (July 17, 2018): 233, https://doi.org/10.1001/jama.2018.8374; Effy Vayena et al., "Policy implications of big data in the health sector", *Bulletin of the World Health Organization*, v. 96, no. 1 (December 1, 2018): 66–68, https://doi.org/10.2471/BLT.17.197426.

[19] Emergency Regulations (Authorization of the General Security Service to Assist the National Effort to Reduce the Spread of the Novel Coronavirus), 5780-2020, available at: https://perma.cc/96V9-HJSS.

[20] "Coronavirus disease-19", Republic of Korea, available at: http://ncov.mohw.go.kr/en/.

[21] "Mobile applications to support contact tracing in the EU's fight against COVID-19", eHealth Network, April 15, 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf; European Commission, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01, *Official Journal of the European Union 2020; 63:1-9*, April 17, 2020.

[22] "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak", European Data Protection Board (EDPB), April 21, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[23] "Digital contact tracing tools for COVID-19", Centers for Disease Control and Prevention (CDC), April 20, 2020, https://www.cdc.gov/coronavirus/2019-ncov/downloads/digital-contact-tracing.pdf.

by its characteristics, present a high risk of personal data violations.[24] On the other hand, less invasive systems adopted by many countries consist of web platforms or mobile applications, presenting different features, such as self-diagnostic/medical reporting, CT, and quarantine enforcement/isolation registration or monitoring functions.

Although digital CT applications are being adopted widely by many countries as a complementary tool to help in the process of lifting the restriction measures imposed on the general population, it is important to highlight the concerns recently expressed by the WHO, for whom these technologies still need to prove their effectiveness and their feasibility and thresholds required for large scale implementation.[25]

As a result of research performed during June 2020 concerning the deployment of technological tools, 158 systems were identified from 94 countries, and two systems were categorised as global because they were developed by a supranational institution (WHO) and an international coalition. This dataset includes web platforms and mobile applications developed to disseminate information or assist people in checking COVID-19 symptoms. Focusing on mobile applications that process personal data, 139 apps were identified. Of those, 122 were in use at the time of the research, while six were in the pilot phase, nine were announced but not yet made available, and two have been discontinued. Of the identified systems, 48 were developed by 28 European countries, being 20 European Union Member States.

In many countries, the protection of personal data is a right that appears in constitutional and legal provisions, and its processing can only be performed under very restricted circumstances, the protection of health being accepted as a valid justification.

In this paper , we will focus on the systems developed as digital CT tools in France (StopCovid) and in Portugal (STAYAWAY COVID). In the next section, the author will outline their characteristics and the most relevant aspects concerning the processing of personal data.

These systems were chosen based on the existence of a consistent legal framework for data protection in these countries, and because their development was closely monitored by France's and Portugal's national data protection authorities. Also, these systems were developed using different technical protocols, which resulted in relevant differences on the processing of personal data.

3.1. StopCovid

On 8 April 2020, the French government announced its intention to release a digital CT tool, denominated StopCovid. This tool is considered by the government a necessary measure to protect the population and is part of France's global deconfinement plan.

The official application's website[26] states that this technological solution is part of a gradual plan of epidemic control aimed at loosening the imposed restrictions and seeking to inform citizens that have been in the vicinity of carriers of the virus in the near past.

[24] Ramos, "Evaluating privacy during the COVID-19 public health emergency".
[25] "Digital tools for COVID-19 contact tracing", World Health Organization (WHO), June 2, 2020, https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1.
[26] "TousAntiCovid", Ministère de l´Économie des Finances et de la Relance, available at: https://www.economie.gouv.fr/stopcovid#.

It consists, on the users' side, of an application for smartphones and mobile devices, running Android or iOS operating systems, and on the government's side, of a central server that stores and transmits the data necessary for the overall operation of the system.

The application is based on the ROBERT protocol (ROBust and privacy-presERving proximity Tracing), which is responsible for building a comprehensive list of users of the application that had close contact with each other for at least a specific time interval. The ROBERT protocol was developed by a joint effort between French Inria and German Fraunhofer Heinrich Institut, with data minimisation and data protection by design in mind , and had its source code published on the Internet[27], allowing for an independent audit of its functioning. Also, the complete source code of the StopCovid application has been made available online,[28] reinforcing the government's compliance with transparency.

Although not involving identification data directly (*i.e.*, name, telephone number, e-mail address, etc.), it generates pseudonyms used as identifiers of each person that installed the application. As these pseudonyms can be linked to each installation, it can be considered as personal data within the meaning of Article 4(1) of the EU General Data Protection Regulation ("GDPR").[29] Also, as the alert provided by the system is triggered by the information that a person presents a sufficiently high risk of having contracted COVID-19, this data can be considered as concerning health and thus benefits from the specific protection regime for such sensitive data provided by Article 9 of the GDPR.

This system is not considered a tracking application, as it does not rely on the use of geolocation data to assess the proximity between two electronic devices, but instead uses Bluetooth Low Energy communication technology to perform this assessment. This characteristic avoids the surveillance of people's geographical movements, as it does not continuously trace individuals.

The use of StopCovid is on a completely voluntary basis, not imposing any negative burdens on people who decide not to install the application, or after installing it, decide not to connect or provide information on their health status. It was developed in a way that presents many opportunities for people to choose sharing their personal data: they can have carte blanche to install the application (or not), enable the Bluetooth function on their devices (or not), or even declare their positive result to COVID-19 in the application (or not). Also, they can request the complete exclusion of their data and remove the application at any time. The system is aimed at the population residing in French territory, and the voluntary downloading and use is guaranteed by the legal framework governing the system.

The GDPR, in its Article 6, establishes a restricted list of hypotheses for lawfully processing personal data. It is important to highlight that the Regulation does not establish any hierarchy between the listed legal basis, being the responsibility of the entity carrying out the processing to determine which one better fits its objectives.

Among the possibilities presented on the Regulation, a digital CT application like StopCovid could be deployed under the consent of the data subjects or the

[27] "Robert", GitHub, available at: https://github.com/ROBERT-proximity-tracing/documents.
[28] https://gitlab.inria.fr/stopcovid19.
[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

performance of a task carried out in the public interest. However, if the processing is based on the public interest, Article 6(3) of the GDPR demands that this legal basis is laid down by Union law or a Member State law to which the controller is subject.

The fight against COVID-19 undoubtedly represents a public interest, and for that reason, the French government considered that the most appropriate legal basis for the implementation of the StopCovid application was the provision of Article 6(1)(e) of the GDPR. To fulfill the requirement of the Regulation, the government issued the Decree nº 2020-650, of 29 May 2020,[30] which designates the Ministry of Health as the data controller of the application, and defines the purposes of the processing as: (i) to inform people using the application that there is a risk that they have been contaminated by the Covid-19 virus due to the fact that they are near another user of this application having been diagnosed positive, (ii) to educate people using the application, in particular those identified as contacts at risk of contamination, on the symptoms of this virus, the barrier gestures and the conduct to be adopted to fight against its spread, (iii) to recommend to contacts at risk of contamination to refer to the competent health professionals for the purpose of taking care of them and prescribing, if necessary, a screening examination, and (iv) to adapt, if necessary, the definition of the application parameters making it possible to identify contacts at risk of contamination through the use of anonymous statistical data at national level.

This national legislation also sets a deadline for the processing of the collected data, which may not exceed six months after the cessation of the state of health emergency, declared by Law nº 2020-290, of 23 March 2020, and extended until 30 October, by Law nº 2020-856, of 09 July 2020.

During the development stage of StopCovid, the government submitted consults to the French data protection authority, CNIL (*Commission Nationale de l'Informatique et des Libertés*), which provided valuable remarks to improve the protection of personal data processed by the application, praising the government's concern to protect people's privacy, since the application respects the concept of data protection by design and by default.

On its deliberations of 24 April 2020[31] and 25 May 2020,[32] CNIL pointed as positive aspects of the approach adopted by the French government, the concern to protect people's privacy, in particular, by preventing a list of people who declare themselves as carriers of the virus to be kept centralised on a server. Also, CNIL recognised that the safeguards taken during the development of the application provide a high degree of guarantee, therefore minimising the risk of re-identification of the data subjects associated with the data stored, for a necessarily limited period, by the central server, in full compliance with the principles of data protection enlisted on Article 5 of the GDPR.

[30] Décret no. 2020-650 du 29 mai 2020 relatif au traitement de données dénommé «StopCovid».

[31] "Deliberation no. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called 'StopCovid' (request for opinion no. 20006919)", CNIL, April 24, 2020, https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_april_24_2020_delivering_an_opinion_on_a_proposed_mobile_application_called_stopcovid.pdf.

[32] "Deliberation no. 2020-056 from 25 May 2020 delivering an opinion on a draft decree relating to the mobile application known as 'StopCovid'", CNIL, May 25, 2020, https://www.cnil.fr/sites/default/files/atoms/files/deliberation_ndeg_2020-056_from_25_may_2020_delivering_an_opinion_on_a_draft_decree_relating_to_the_mobile_application_known_as_stopcovid.pdf.

The compliance with the personal data protection principles, in particular, the proper information of the persons concerned, the respect of their rights and, more generally, of the provisions of the GDPR and the French Data Protection Act, is likely to promote the confidence of the users of the application and, consequently, the effectiveness of the planned system.

In its deliberations, CNIL also highlighted the importance of the voluntary approach, the fact that the government made the deployment, the precise definition of the purposes of the data collection, and the existence of a date to cease the operation of the app as decisive factors to ensure there is confidence in the system and to encourage its adoption by a significant proportion of the population.

Nevertheless, regarding the system's effectiveness, the CNIL draws attention to the system's limitations. On the one hand, there are technical conditions to be addressed, in particular, the possibility of adoption by a sufficient portion of the population to access and use the application under good conditions, which means the availability of the system on a sufficient number of mobile application stores and compatibility with the majority of mobile devices currently in use, both in terms of hardware and software.

On the other hand, it is essential to notice that a portion of the population may not possess adequate mobile devices to install the application or may have difficulties installing and using it. In particular, people most vulnerable to the disease, such as the elderly or children, or people without any kind of mobile device, but who can significantly contribute to the spread of the disease, must be particularly concerned. Also, some people may contract the disease without presenting any symptoms, which may result in them not alerting their contacts.

These limitations must be adequately addressed because the temporary invasion of privacy imposed by the implementation of the system can only be accepted to the point where the government has sufficient information to have reasonable assurance that such a measure will be useful in managing the COVID-19 crisis, and bringing the population out of its mandatory confinement, which in itself constitutes a severe infringement of the freedom of movement.

As a negative aspect of the overall system, CNIL pointed out that competition from other digital CT applications being developed by different actors is likely to undermine the French system's effectiveness. Also, as a weakness, the CNIL pointed to a possible difficulty in interoperability with applications from other EU Member States, as France has opted to adopt the ROBERT protocol, which made it a unique system in Europe.

Finally, the CNIL recommended that the system's impact on the overall health strategy be studied and documented regularly so that the effectiveness over time can be assessed. This becomes more important because, between the release of the application on 2 June 2020, and the three following weeks, more than 1.9 million people downloaded the application and more than 1.8 million activated the system, but only 68 users declared a positive COVD-19 test result, and the application sent only 14 notifications to related contacts,[33] which demonstrates that, in general, people may still not trust this kind of application.

[33] Romain Dillet, "French contact-tracing app StopCovid has been activated 1.8 million times but only sent 14 notifications", TechCrunch, June 23, 2020, https://techcrunch.com/2020/06/23/french-contact-tracing-app-stopcovid-has-been-activated-1-8-million-times-but-only-sent-14-notifications/.

3.2. STAYAWAY COVID

In Portugal, the development of a digital CT application was announced at the end of April 2020, by a joint initiative between a private research institution, INESC TEC (*Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência*), and a non-profit public association, ISPUP (*Instituto de Saúde Pública da Universidade do Porto*). Although not directly involved in the project, the Portuguese national government endorsed its development.

The official application's website[34] states that this technological solution aims to be a complementary measure, within the framework of a comprehensive strategy to combat the pandemic. It intends to assist people in taking measures to interrupt the transmission chain of the infection, by alerting its users of any close contact that person may have had with another user who received a positive diagnosis.

The application was developed within the scope of the DP^3T (Decentralised Privacy-Preserving Proximity Tracing) project,[35] an international consortium of European researchers, who built a proximity tracing system to be applied at large scale, aiming to minimise privacy and security risks for its users and guarantee the highest level of data protection.

It consists, on the users' side, of an application for smartphones and mobile devices, running Android or iOS operating systems, and on the other side, by two different servers, one responsible for diagnosis authentication (SLD – *Serviço de Legitimação de Diagnóstico*) and the other responsible for diagnosis publication (SPD – *Serviço de Publicação de Diagnóstico*).

The SLD generates a 12 characters code that is provided to the authorised health professional responsible for the medical examination that returned a positive diagnosis for COVID-19, and who is responsible for delivering it to the patient, who can then insert the code into the application to inform of his or hers health status. It also registers the date of the patient's first symptoms or, in the case of asymptomatic patients, the testing date. If during the 24 hours of validity of the code provided by the SLD server, the patient inserts it in the STAYAWAY COVID application, then the SPD server receives an identifier from the mobile device, known as temporary exposure key (TEK), and then matches this identifier with all other users that came into close contact with the infected patient, sending them a notification of the risk of contagion.

Along with the notification, the user receives varying information on how to proceed next, according to the level of proximity she or he had with the infected patient.

The application is based on the Exposure Notification framework provided by the software developers Google and Apple, consisting of a protocol that allows CT applications to access some functionalities of the device's operating system, and that had its technical specifications and Application Programming Interface ("API") published on the Internet.[36] Although these specifications are not as informative as the complete source code of the protocol, they still allow for some independent

[34] "Stayaway COVID", Direção-Geral da Saúde, República Portuguesa, available at: https://stayaway.inesctec.pt/.

[35] "DP^3T - Decentralized Privacy-Preserving Proximity Tracing", GitHub, available at: https://github.com/DP-3T.

[36] See the sites: https://www.apple.com/covid19/contacttracing/ and https://www.google.com/covid19/exposurenotifications/.

audit of its functioning. Also, the complete source code of the STAYAWAY COVID application has been made available online,[37] reinforcing the developers' compliance with transparency.

It is important to highlight that Google and Apple announced that access to the protocol would be conceded to public health authorities exclusively, and only one application per country would be accepted. This requirement made the Portuguese national government endorse the development of the STAYAWAY COVID application.

Although not involving identification data directly (*i.e.*, name, telephone number, e-mail address, etc.), it generates temporary exposure key ("TEK") and rolling proximity identifiers ("RPI") that are used as random identifiers of each person that installed the application. As these TEK and RPI can be linked to each installation, it can be considered personal data within the meaning of Article 4(1) of the GDPR. Also, as the alert provided by the system is triggered by the information that a person presents a sufficiently high risk of having contracted COVID-19, this data can be considered as concerning health and thus benefits from the specific protection regime for such sensitive data provided by Article 9 of the GDPR.

As with the French application, it is not considered tracking , as it does not rely on the use of geolocation data to assess the proximity between two electronic devices, but instead, it uses the less intrusive Bluetooth Low Energy communication technology to perform this assessment. This characteristic allows the system to fulfill its goal without knowing the user's physical location or where the contact with other users took place.

The use of STAYAWAY COVID is in a completely voluntary and self-determining basis, not imposing any negative burdens on people who decide not to install the application, or after installing it, decide not to connect or provide information on their health status. It was developed in a way that presents many opportunities for people to choose sharing their personal data. People can install the application (or not), enable the Bluetooth function on their devices (or not), or even declare their positive result to COVID-19 in the application (or not). Also, they can request the complete exclusion of their data and remove the application at any time.

As previously referred, the GDPR, on its Article 6, establishes a restricted list of hypotheses for lawfully processing personal data. In the case of the STAYAWAY COVID application, the legal basis was the provision of Article 6(1)(a) in conjunction of Article 9(2)(i) of the GDPR, consisting of the data subject consent to the processing of his or her personal data, including special categories of personal data, namely, data concerning health.

In order to specify the data controller responsible for the processing of the collected data, the government issued the Decree-Law no. 52/2020, of 11 August,[38] designating the DGS (*Direção Geral de Saúde*) as the entity responsible for the data processing, and regulating the intervention of the health professional on the system, in accordance with Article 9(2)(i) of the GDPR.[39] It also defined the purpose of

[37] "Stayaway - The official COVID-19 exposure notification app for Portugal", GitHub, available at: https://github.com/stayawayinesctec.

[38] Decreto-Lei no. 52/2020, de 11 de agosto, estabelece o responsável pelo tratamento dos dados e regula a intervenção do médico no sistema STAYAWAY COVID.

[39] Article 9(2)(i) of the GDPR requires that Member States law shall establishes the entity responsible for the processing of special categories of personal data, which includes data concerning health, providing for suitable and specific measures to safeguard the rights and freedoms of the data subject.

the processing as to notify people of individual exposure to contagious factors for SARS-CoV-2, due to close contact with other users of the application that lately received a positive diagnosis of COVID-19. This national legislation also sets a deadline for the processing of the collected data, which may end with the cessation of the epidemic situation.

During the development stage of STAYAWAY COVID, its developers submitted a Data Protection Impact Assessment (DPIA) to the Portuguese data protection authority, CNPD (*Comissão Nacional de Proteção de Dados*), which provided valuable remarks to further protect the processing of personal data by the application, praising the developers' concern to protect people's privacy, since the application respects the concept of data protection by design and by default.

On its deliberation of 29 June 2020[40] and its Opinion of 21 July 2020,[41] CNPD pointed as positive aspects of the approach adopted by the application developers, the concern to protect people's privacy, in particular by preventing a list of people who declare themselves as carriers of the virus to be kept centralized on a server. Also, CNPD recognised that the safeguards taken during the development of the application provide a high degree of guarantee, therefore minimising the risk of re-identification of the data subjects associated with the data stored, for a necessarily limited period, in full compliance with the principles of data protection set out in Article 5 of the GDPR.

The compliance with the personal data protection principles, in particular the proper information of the persons concerned, the respect of their rights and, more generally, of the provisions of the GDPR, is likely to promote the confidence of the users of the application and, consequently, the effectiveness of the planned system.

In its deliberations, CNPD also highlighted the importance of the voluntary approach, the availability of the application's source code, the precise definition of the purposes of the data collection, and the existence of a date to cease the operation of the app as decisive factors to ensure the confidence in the system and encourage its adoption by a significant proportion of the population.

However, CNPD also pointed out that, although not having to register to use the applications, the users must be registered on Google's or Apple's application marketplaces to download the STAYAWAY COVID app. This authentication process results in personal data being provided to those companies, who then have a full register of all persons that adopted the system.

As a negative aspect of the overall system, CNPD pointed out that the adoption of the Bluetooth technology does not represent a complete protection of the user's identity or location, as it can still be traced back to the mobile device's MAC (Media Access Control) address, which is a unique identifier of the equipment. Nevertheless, it is possible to mask the MAC address with a random value, the technical specifications of the Exposure Notification framework raise concerns regarding the possibility of Google or Apple – who shall maintain a register of the real MAC address - to follow a track of the contacts or even revert the masking process.

In the Portuguese law, although the DGS was selected as data controller, CNPD criticized that choice, stating on its Parecer/2020/82 that the data controller should be an authority with legal duties and powers, which would be the Health Director-General, and not the public office.

[40] "Deliberação/2020/277", CNPD, June 29, 2020, https://www.cnpd.pt/home/decisoes/Delib/DEL_2020_277.pdf.

[41] "Parecer/2020/82", CNPD, July 21, 2020, https://www.cnpd.pt/home/decisoes/Par/PAR_2020_82.pdf.

Also, since the Exposure Notification framework is property of private companies, there is a risk of unilateral modifications of the system without previous notice to its users and without any guarantee that the data will not be used for different purposes than initially specified, with negative consequences for the application and the users.

Finally, CNPD recommended conducting a pilot test, under real conditions, restricted to a portion of the national territory, to identify and correct security flaws. This pilot test commenced on August 17, 2020 and lasted for two weeks. The official release of the applications occurred on September 1, 2020, and during the first month of operations, the system registered more than 1.26 million downloads, and provided 106 notifications of contacts with people that tested positive for COVID-19.[42]

4. Conclusion

The adoption of digital CT applications as complementary measures to contribute to the end of the restrictions imposed by many countries to its citizens should be recognised as relevant and greeted as a new tool to be deployed in a globalised world.

The COVID-19 pandemic came disrupting many aspects of our regular lives and imposing the adoption of new behaviors. Although not yet rooted in our routines, the use of mobile devices to report health conditions is being strongly incentivised.

In this paper, we aimed to briefly assess this new reality and present the systems developed in France and Portugal to notify people of the risk of having been in close contact with someone who came to receive a positive diagnosis for COVID-19.

The most relevant characteristic of both systems is their voluntary approach, allowing people to try the applications and develop trust in the systems. As these systems can only fulfill their objectives through the processing of personal data, it is paramount that every user can trust the application.

This trust is reinforced by the transparency that both systems present, having made available their source codes so any interested party can audit its functioning and report any identified issues, contributing to the overall improvement of the systems.

It is also relevant to notice that the two systems present a specific deadline to cease their operations, determined by the legislation that grants the legal basis for their general functioning.

As digital CT applications are relatively new systems, it is essential to have an overview by the national data protection authorities of each country interested in deploying this kind of system. That was observed in the French and Portuguese cases, where both CNIL and CNPD actively participated in the development, providing relevant recommendations and guidelines to increase the protection of people's privacy.

Concerning the French application, both the government and the protocol developers have already referred to the intention of evolving the system to enable EU-wide interoperability, which would represent an increase in the system's efficiency. However, they may result in new privacy risks that must be adequately addressed.

In a comparison between the two systems, it seems that the Portuguese may easily provide future interoperability with applications from other countries, based

[42] "Mais de um milhão de pessoas já instalaram a aplicação StayAway Covid", *SIC Notícias*, October, 02, 2020, https://sicnoticias.pt/especiais/coronavirus/2020-10-02-Mais-de-um-milhao-de-pessoas-ja-instalaram-a-aplicacao-StayAway-Covid.

on the Exposure Notification framework that has been adopted by many other digital CTtools.

However, the STAYAWAY COVID application developers do not hold full control of the data processing, as part of the system runs code that cannot be audited. On the other hand, the French application, because it is based on a different protocol, that strives for transparency, may provide greater security and privacy for its users.

The interoperability of CT applications within the European Union has recently been discussed by its Member States, which agreed on a set of technical specifications[43] that any system must observe to allow the exchange of information between different national applications when users travel through the EU.

As any novel system, it is expected that during the use of these systems, some flaws may be identified, as some other points that can be improved to deliver greater personal data protection.

[43] "EHealth network guidelines to the EU Member States and the European Commission on interoperability specifications for cross-border transmission chains between approved apps", eHealth Network, June 12, 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf.