DATA PROTECTION IN THE CONTEXT OF COVID-19

A SHORT (HI)STORY OF TRACING APPLICATIONS

Elise Poillot, Gabriele Lenzini,
Giorgio Resta, Vincenzo Zeno-Zencovich

Consumatori
e Mercato 12

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Nella stessa Collana

1. V. Zeno-Zencovich (a cura di), *Cosmetici. Diritto, regolazione, bio-etica*, 2014

2. M. Colangelo, V. Zeno-Zencovich, *Introduction to European Union transport law*, I ed. 2015; II ed. 2016; III ed. 2019

3. G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, 2015

4. V. Zeno-Zencovich, *Sex and the contract* (II ed.), 2015

5. G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, 2016

6. A. Zoppini (a cura di), *Tra regolazione e giurisdizione*, 2017

7. C. Giustolisi (a cura di), *La direttiva consumer rights. Impianto sistematico della direttiva di armonizzazione massima*, 2017

8. R. Torino (a cura di), *Introduction to European Union internal market law*, 2017

9. M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, 2020

10. L. Scaffardi, V. Zeno-Zencovich (a cura di), *Cibo e diritto. Una prospettiva comparata*, 2020

11. A.M. Mancaleoni, E. Poillot (a cura di), *National Judges and the Case Law of the Court of Justice of the European Union*, 2020

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

**Elise Poillot, Gabriele Lenzini,
Giorgio Resta, Vincenzo Zeno-Zencovich**

DATA PROTECTION IN THE CONTEXT OF COVID-19

A SHORT (HI)STORY OF TRACING APPLICATIONS

Consumatori e Mercato 12

Roma TrE-Press
2021

The LEGAFIGHT project was conducted with the financial support of the GRAND-DUCHY OF LUXEMBOURG, *Fonds National de la Recherche* in the frame of the Covid-19 research funding scheme.

The part of the research which was coordinated by professors Giorgio Resta and Vincenzo Zeno-Zencovich falls within the Progetto di Ricerca di Interesse Nazionale (PRIN 2017) *Governance of/through Big Data: Challenges for European Law* [2017BAPSXF], leading research unit Università degli studi Roma Tre, local units Università Luigi Bocconi, Milan; Università del Salento, Lecce; Università LUMSA, Rome.

Coordinamento redazionale e editoriale:
Gruppo di Lavoro *RomaTrE-Press*

Collana pubblicata nel rispetto del Codice etico adottato dal Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, in data 22 aprile 2020.

Elaborazione grafica della copertina: MOSQUITO. mosquitoroma.it

Caratteri tipografici utilizzati:
Brandon Grotesque (copertina e frontespizio)
Adobe Garamond Pro (testo)

Impaginazione e cura editoriale: Colitti-Roma colitti.it

Edizioni: *RomaTrE-Press* ©
Roma, novembre 2021
ISBN: 979-12-5977-055-4

http://romatrepress.uniroma3.it

L'attività della *RomaTrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma

Presentazione della collana "Consumatori e Mercato"

Direttore: Vincenzo Zeno-Zencovich
Comitato Scientifico:
Guido Alpa, Marcello Clarich, Alberto Musso

La Collana "Consumatori e mercato", pubblicata in open access dalla Roma TrE-Press, intende essere una piattaforma editoriale multilingue, avente ad oggetto studi attinenti alla tutela dei consumatori e alla regolazione del mercato. L'intento è di stimolare un proficuo scambio scientifico attraverso una diretta partecipazione di studiosi appartenenti a diverse discipline, tradizioni e generazioni.

Il dialogo multidisciplinare e multiculturale diviene infatti una componente indefettibile nell'àmbito di una materia caratterizzata da un assetto disciplinare ormai maturo tanto nelle prassi applicative del mercato quanto nel diritto vivente. L'attenzione viene in particolare rivolta al contesto del diritto europeo, matrice delle scelte legislative e regolamentari degli ordinamenti interni, e allo svolgimento dell'analisi su piani differenti (per estrazione scientifica e punti di osservazione) che diano conto della complessità ordinamentale attuale.

****

The "Consumer and market" series published, in open access, by Roma TrE-Press, aims at being a multilingual editorial project, which shall focus on consumer protection and market regulation studies. The series' core mission is the promotion of a fruitful scientific exchange amongst scholars from diverse legal systems, traditions and generations. This multidisciplinary and multicultural exchange has in fact become fundamental for a mature legal framework, from both the market practice and the law in action standpoints. A particular focus will be given on European law, where one can find the roots of the legislation and regulation in the domestic legal systems, and on the analysis of different levels, in line with the current complexity of this legal sector.

Contents

Executive Summary

This book derives form a report drafted in the frame of a research project on tracing applications: the LEGAFIGHT project (standing for LEGAlly FIGHTting Covid-19) aiming to propose a draft legislation for a tracing application in Luxembourg.

The project was supported by a research grant awarded in spring 2020 by the Luxembourg Fonds National de la Recherche. It was conceived as an interdisciplinary and international project bringing together researchers from two disciplines (computing science and law): Professor Gabriele Lenzini, Associate Professor at the Interdisciplinary Centre for Security, Reliability and Trust of the University of Luxembourg, who has decennial expertise in the design of security and privacy for socio-technical systems; Professor Elise Poillot, Professor of Civil law at the University of Luxembourg, a specialist of consumer law who is currently developing her research in the field of consumer protection in digital surroundings and more specifically on customers profiling in digital contracts; Professor Giorgio Resta, Professor of Comparative law at the University of Rome 3, an expert in the field of law applied to digital technologies and Professor Vincenzo Zeno-Zencovich, Professor of Comparative law at the University of Rome 3 and whose research is devoted, among other topics, to legal aspects of information and communication technologies.

The LEGAFIGHT project addressed two critical research questions.

The first one related to the strategy to put in place in order to develop a quick route to ease Luxembourg out of the lockdown regime that was implemented when the project was designed and submitted for funding. The strong impact of EU law in the field of data protection, a topic of crucial interest when it comes to the development of a digital tracing system to combat the pandemic, could optimistically lead the group to think that what could be done for Luxembourg could be then replicated at the European level. The second question was to reflect on how to develop a sustainable legal framework for the management of epidemiological data in Luxembourg.

Since the project started, more than one year has passed. One can reasonably say that during this twelve-month period, both the epidemiological situation and the political developments were rather unpredictable. Tracing applications were initially considered as a key instrument for "a quick exit out of the crisis" and quite rapidly sparked a lively debate as to their intrusive nature and their possible instrumentalization by States to track citizens. The existence of such debate led the Luxembourg prime minister, Xavier Betel, to strongly express his opposition to the development of a Luxembourg tracing application. From a more global perspective, it became also rapidly obvious that the exit strategies would remain decided and implemented at the domestic level. The European Union demonstrated to have an extremely limited role in any political decisions and policy making regarding the sanitary crisis. This obviously impacted the research project, which had to reconsider its objectives. From the ambition to propose a draft legislation that could have been an inspiration for an EU policy, it moved to that of conducting comparative research aiming to understand whether such digital tracing systems could be considered as a threat to citizens' fundamental rights and what lessons could be learned from such developments. But just as in life, the pandemic turned out to be full of surprises. While the research group was somehow celebrating the funeral of tracing applications before burying the report, the second and third waves of the pandemic revived the interest in tracing applications that had been, in the meanwhile, reviewed and reshaped by governments who turned them into communication instruments and support for various certificates that were now fully part of everyday life (at some point having a PCR test done was like going to the supermarket). Tracing applications should not be buried. On the contrary they could be and were revisited in order to accompany citizens in a "Covid-19 world" that could change our way of living and travelling for quite a while and to facilitate, not to mention the fact that they will allow for a better response to new pandemics, already predicted to erupt.

In our contemporary world, sanitary applications, if one prefers to refer to them in a more neutral manner, can be very useful tools to allow us to cross borders, to take planes, to be informed on places where we can go or where we cannot, to know until what time we are allowed to go for a walk in the evening etc. The LEGAFIGHT experts' group consequently decided that a recommendation on a draft legislation on tracing applications for Luxembourg was still of interest. Such a recommendation had to be put

in its context, which is both technical and legal. This is what **part 1** of the study aims to do while **part 2**, drawing the conclusions of the technical and legal study, makes some recommendations as to the content of a normative text regarding a national tracing application. Eventually **part 3,** based on insights from the previous chapters, intends taking one step back in an attempt to understand what lessons can be learned from the short life of tracing applications and how they could potentially evolve in the future.

I would like to take the opportunity of this introductory note to thank all the practitioners, researchers and students who participated in this project, Dr. Clarissa Giannacari (University of Rome 1 – La Sapienza); doctoral researcher Damien Negre (University of Luxembourg); Damien Dietrich, former Chief Medical Digital Officer of the Robert Schuman Hospitals (Luxembourg), now Secretary General for Medical Affairs of the Swiss medical Network; Victor Cobuscean and Cécile Meyer, Master Students in EU law and Abetare Shabani, Master student in Information and Computer Science. I am also very grateful to Giovanni Dini for his diligent proofreading of the LEGAFIGHT's report.

Elise Poillot

This Research is the result of a common endeavour. The various parts have been written as follows: Chapter I, 1 – Gabriele LENZINI; Chapter I, 2.1 – Elise POILLOT (with Gabriele LENZINI for France); Chapters I, 2.2.1, 2.2.2. and 2.2.7. – Elise POILLOT; Chapters I, 2.2.3. and 2.2.4. – Giorgio RESTA; Chapters I, 2.2.5 and 2.2.6. – Vincenzo ZENO-ZENCOVICH; Chapter I, 2.3 – Damien NEGRE; Chapters II and III – Elise POILLOT, Giorgio RESTA and Vincenzo ZENO-ZENCOVICH.

I

Technical and legal frameworks of tracing applications

1. *Technical framework*

1.1. *General considerations on digital contact tracing applications*

The outbreak in December 2019 of the coronavirus disease COVID-19 (the acute syndrome caused by the SARS-CoV-2 virus), forced countries to implement different measures to reduce the spread of the infection.

One such measure relies on the fact that modern smartphones come with powerful sensors. An application using GPS, Wi-Fi and Bluetooth antennas can receive and process signals and track not only where a user goes (as we all know from using maps) but whom he or she encounters. Using the Bluetooth Lower Energy technology, a phone can detect short-range power signals from other phones, and an application can identify them and estimate the distance and duration of the encounter.

With some additional information, i.e., that an encountered phone belongs to a person found positive for the virus, an application can estimate whether there has been a risk of infection. *Digital Contact Tracing (DCT)* works exactly this way.

DCT apps could enormously improve the work of health workers because they are more efficient and more scalable than *manual contact tracing,* which tracking operators employ to find out (by using patients registers and phone calls) with whom a COVID-positive individual has been in contact.

Today, there are more than 40 mobile DCT apps [1] in the world, 28 of which in the EU[2]. They notify a user when he or she has been in proximity

[1] M. Sato, "Why some countries suspended, replaced, or relaunched their covid apps", MIT Technology Review, December 23, 2020; https://www.technologyreview.com/2020/12/23/1015557/covid-apps-contact-tracing-suspended-replaced-or-relaunched/(accessed April January 2021)

[2] M. Ciucci, and F. Gouardères, "National COVID-19 contact tracing apps", IP/A/ITRE/2020-0, European Parliament, Directorate-General for Internal Policies, May 2020. http://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_

with someone else who has tested positive for the virus. Since the user is at risk of infection, he or she is recommended to take a COVID19 test and, if also found positive, to self-isolate and reduce the further spread of the virus.

Technical Notes

DCT applications are classified depending on their communication technology (GPS or Bluetooth) and on the data processing protocols (centralised or decentralised).

GPS vs Bluetooth

To gather data, DCT apps rely on two communication technologies:

- Bluetooth Low Energy *(proximity detection)*;
- GPS *(location-based detection)*.

The following table summarises the essential differences:

Technology	DCT using GPS/Wi-Fi: Location History/Matching	DCT using Bluetooth Direct Proximity Detection/Matching
How it works	It calculates, using satellites and Wi-Fi tower signals, the geolocation coordinates of the device. It keeps track of "*location trails*", lists of time-stamped coordinates. When a person tests positive, the app shares the person's location trails. By intersecting trails, one can assess whether there has been a risk of exposure (risk score).	By measuring the intensity of Bluetooth signals it detects the presence of other devices in proximity. If the time and distance of the exposure are epidemiologically relevant (long and close enough to cause infection), the app stores the identifiers of nearby phones and keeps them in a "*contact history*". When a person tests positive, his or her phone's identifier (i.e., his or her "key") is shared[3]. By matching this "key" with the list of "keys" kept in the contact history, one can assess whether there has been a risk of exposure (risk score).

BRI(2020)652711_EN.pdf - Doi: 10.2861/ 808426

[3] Keys are unique ephemeral identifiers. By sharing its key, a phone leaves a trace that can be referred later, e.g., when the phone informs that its owner tests positive. Sharing keys works also cross-border thanks to an EU Interoperability Gateway that makes possible to efficiently receive and pass on arbitrary identifiers between national apps.

There are pros and cons in both technologies in terms of several factors, such as:

- *Accuracy*: GPS is about 5m, Bluetooth ranges from 1-10m;
- *Reliability of the signals*: GPS does not work well where the satellite signal is disturbed, like in dense urban areas; Bluetooth works mainly indoors and within close range;
- *Quality of information*: neither can see whether people use masks or if they are separated by a wall;
- *Battery consumption*: GPS is more demanding than Bluetooth;
- *Compatibility*: GPS is standard in all phones, Bluetooth not always.

A difference is however in how the two technologies are seen in terms of respect of privacy. In reference to the EU Data Protection Regulation, the GDPR, an application should comply with the data minimization principles: tracking a user's location seems unnecessarily invasive from this perspective. The less invasive "Direct Proximity" detection using Bluetooth is the most adopted technological solution for DCT applications.

Centralised vs Decentralised

Depending on where identifiers, metadata and contact histories are stored and processed, DCT apps are split into two large categories

- *centralised*;
- *decentralised*.

In both categories, a person that tests positive for the virus uploads data to a back-end server, but they differ on where the location trail or the contact history are stored and where the risk scores are calculated. The following table summarises the essential differences:

Technology	Centralised	Decentralised
How it works	Data (personal data, phone identifiers, location trails or contact histories, metadata) are stored and processed on a server operated by health authorities. Risk scores are calculated on the server.	Data (personal data, phone identifiers, location trails or contact histories, metadata) are stored and processed on the phones. Risk scores are calculated on the phone (after some back-end data is downloaded).

Examples of application in this category.	ROBERT (ROBust and privacy-presERving proximity Tracing protocol), PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing), BlueTrace	DP-3T (Decentralised Privacy-Preserving Proximity Tracing), TCN (Temporary Contact Numbers), Google/Apple Exposure Notification API

Both categories can be implemented in such a way as to ensure privacy (see next section), usually by using ephemeral, randomly generated and regularly changed identifiers, and by encrypting data.

Both are considered viable options (e.g., see European Data Protection Supervisor Guidelines, 21/04/2020), but *decentralised solutions are considered to be more in line with the minimalization principle,* to use the minimum amount of data required to process a certain service (e.g., European Commission Guidance 16/04/2020), although the GDPR suggests that processing personal data necessary for humanitarian purposes is considered lawful (art. 46). For an account of this legal basis see other sections of this report and the EU briefing "National COVID-19 Contact Tracing Apps"[2].

Other factors relevant to categorise DCT

DCT apps can also be distinguished because of other functional features, namely:

- *interoperability* (whether a DCT app can communicate with others for international cooperation);
- usability (the degrees of easiness in using the app for the purpose it has been designed);
- *user experience* (the degree users perceive the app is being useful and trustworthy in what it is doing, and other hedonistic qualities);
- *privacy* (how much personal data a DCT app requires, how privacy-intrusive it is);
- *security* (how a DCT app protects user privacy from attempts of intrusion into phones or servers).

Privacy Matters: A Brief History

Privacy and security have been particularly debated within the scientific

community and the media. As soon as the idea of using DCT emerged, many started to be concerned about privacy.

One concern was about the access permission that DCT apps may require (e.g., contact details, call history, web searches, camera permissions, access to call records, messages and mobile media). The other concern was about where the data, including the location trails or contact histories, are stored and processed and how they are protected from unauthorised access. Depending on implementation (i.e., anonymised using ephemeral IDs vs encrypted) and on the underlying communication (e.g., security protocols) and data management architectures (i.e., centralised vs decentralised) DCT apps offer different guarantees of security.

Most of today's applications are, to different degrees, privacy-preserving. There has been an ongoing animated discussion about what architectures and protocols are stronger for the purpose.

In Europe, the first application was produced by the "Pan-European Privacy-Preserving Proximity Tracing" (PEPP-PT) initiative. PEPP-PT offered a Bluetooth Low Energy solution, with a centralised architecture. The solution is based on the "ROBust and privacy-presERving proximity Tracing" (ROBERT) scheme[4].

Another, also using Bluetooth Low Energy but with a decentralised architecture is the "Decentralised Privacy-Preserving Proximity Tracing (DP3T)" app. DP3T was born out of members of the PEPP-PT consortium leaving on April 18th 2020, due to a controversy about a 'lack of transparency and clear governance'[5].

The Apple/Google Exposure Notification project is based on similar principles as the DP-3T protocol[6], and supports a variant of it since May 2020. Huawei added a similar implementation of DP-3T to its Huawei Mobile Services APIs known as "Contact Shield" in June 2020[7].

[4] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Métayer, and V. Roca, "ROBERT: ROBust and privacy-presERving proximity Tracing", HAL Id: hal-02611265; URL: https://hal.inria.fr/hal-02611265 (accessed Apr. 05, 2021).

[5] L. Clarke, "PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear", *NS Tech*, Apr. 20, 2020; http://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear (accessed Apr. 03, 2021).

[6] Apple | Google, "Exposure Notifications: Help slow the spread of COVID-19, with one step on your phone"; https://www.google.com/intl/en_us/covid19/exposurenotifications/ (accessed Apr. 05, 2021).

[7] Huawei, "Contact Shield," *ContactShield - Developers*; https://developer.huawei.com/consumer/en/doc/development/HMS-Plugin-References-V1/contactshield-

There is still some ongoing discussion about which architecture, centralised or decentralised, better serves DCT's privacy. But although privacy invasion may indeed occur, and despite the interesting insights from describing attack scenarios, not everything that can happen necessarily will happen. In balancing risks, one should not forget other factors. Laws and regulations, for instance, impose restrictions over personal data processing and hold accountable those who pursue malpractices. These instruments also help to defend one's right to privacy in addition to the technical privacy-by-design guarantees. The same happens with banks and credit card companies to whom we all entrust our financial histories, apparently with fewer concerns than those that have been raised about DCT and public health.

ROBERT has been validated by CNIL (Commission Nationale de l'Informatique et des Libertés), the French authority for data privacy and data protection regulation. Other countries (see below) decided instead to base their DCT application on DP3T.

In Europe, where above all the General Data Protection Regulation (GDPR) (Article 9) dictates that data processing can only take place under strict requirements, countries have been free to choose their DCT of preference, but following EU guidelines[8]:

- contact tracing and warning Apps should only be voluntarily installed and used;
- the data minimisation principle should be employed in the app design;
- apps should use proximity data based on Bluetooth technology;
- no location data is requested or utilised by the tracing App;
- contact tracing and warning apps do not track people's movements;
- the data should not be stored longer than necessary – 14 days;
- data should be protected through state-of-the-art techniques, including encryption;
- the applications should be de-activated as soon as the pandemic is over.

The following table summarises the mobile contact tracing apps among the member states:

0000001061565786-V1 (accessed Apr. 05, 2021)

[8] European Commission, "Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID19 crisis, in particular concerning mobile applications and the use of anonymised mobility data," Official Journal of the European Union, Apr. 2020; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020H0518&from=EN

Countries	*App*	*Is this app potentially interoperable?*	*Is it interoperable?*
Austria	Stopp Corona App	Yes	 Yes
Belgium	Coronalert	Yes	 Yes
Bulgaria	The deployment of a contact tracing app is not foreseen.		
Croatia	Stop COVID-19	Yes	 Yes
Cyprus	CovTracer-EN	Yes	 Yes
Czechia	eRouška	Yes	 Yes
Denmark	Smittestop	Yes	 Yes
Estonia	HOIA	Yes	 No
Finland	Koronavilkku	Yes	 Yes
France	TousAntiCovid	No	 No
Germany	Corona-Warn-App	Yes	 Yes
Greece	Contact tracing app under development.	Yes	

Hungary	VirusRadar	No	 No
Ireland	COVID Tracker	Yes	 Yes
Italy	Immuni	Yes	 Yes
Latvia	Apturi Covid	Yes	 Yes
Lithuania	Korona Stop LT	Yes	 No
Luxembourg	The deployment of a contact tracing app is not foreseen.		
Malta	COVIDAlert	Yes	 No
Netherlands	CoronaMelder	Yes	 Yes
Norway	Smittestopp	Yes	 Yes
Poland	ProteGO Safe	Yes	 Yes
Portugal	StayAway COVID	Yes	 No
Romania	Romania is exploring the development of a contact tracing app.		 No
Slovakia	A contact tracing app is being developed.		

Slovenia	#OstaniZdrav	Yes	Yes
Spain	Radar Covid	Yes	Yes

1.2. *Overview of some national systems*

European Countries

Belgium

Belgium launched its DCT app, CoronAlert, on September 30th, 2020.

CoronAlert's system architecture runs on IOS and Android, relies on Bluetooth Low Energy to gather data by proximity detection, has decentralised data management and processing and uses the Apple/Google APIs. It deletes any data collected after 14 days.

The functionality of the "CoronAlert" app is based on the Corona-Warn-App launched in Germany: it has the same user interface and the same workflow. This DCT app is compatible with other European DCT apps

According to the website corona-tracking.info[9], by the end of March 2021, it had been installed by 2,617,000 people (22% of the population, 29% of the population with smartphones), and 623,200 test results had been received on the app, among which 58,200 positives. Among this latter, 21,300 shared their keys (36.6% of the positives).

[9] "Tracing against corona", web site https://www.corona-tracking.info/app/coronalert-counter/(accessed Apr. 03, 2021).

The following table summarises the main information about this DCT app:

Country	App Name	Platform	Permission Required	Data Collected	Privacy Policy	No. of Downloads	No. of positive users	App reviews
Belgium	Coro-nAlert	Android/ IOS	Bluetooth, Exposure Notification, permission to upload keys	Collected data such as anonymous ID and test result are uploaded to the server managed by Sciensano in the European Union - otherwise, no personal data is collected.	No specific information about sharing data with third parties.	2,617,000	21,300	Though the number of reviews for this app is lower compared to the others, 65% are positive. The main complaint is that statuses are not being updated in real time; test results are not being recorded to the app.

France

France's previous and current version of DCT apps (StopCovid and TousAntiCovid respectively) rely on Bluetooth Low Energy, thus on proximity detection, with a centralised architecture based on the ROBERT protocol. Installation of either app requires permission to use Bluetooth and to collect data such as name, phone number andpostcode. It asks for permission to share these data with a third party (National Health Department).

The first version (StopCovid) was launched on June 2nd 2020. With only 2.8 million downloads after two months, it was not a success. According to government reports[10] the failure of the app was due to poor advertising and guidelines, some defective functionalities (by the end of August 2020 it is reported to have sent only 78 positive test notifications), and some lack of trust by the public[11].

On October 26th 2020, France decided to launch the second version of the application (TousAntiCovid). The app still uses the same system architecture but has improved functionality and it was advertised better. By the end of February 2021, TousAntiCovid reached a total number of downloads of 13.979.446 (16,74% of the population), with 122.457 notifications sent, and 205.814 positive users reported.

[10] Comité de Contrôle et de Liasion Covid-19 (CCL-Covid), Societé Civile et Parlement, "Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie." Avis du 15 Septembre 2020.
[11] C. O'Brien, "France tries to salvage failed StopCovid tracing app as cases surge," *Venture Beat*, Sep. 2020 https://venturebeat.com/2020/09/18/france-tries-to-salvage-failed-stopcovid-tracing-app-as-cases-surge/ (accessed Apr. 03, 2021).

The following table summarises the main information about these DCT apps:

Country	App Name	Platform	Permission Required	Data Collected	Privacy Policy	No of Downloads	No of positive users
France	TousAntiCovid	Android/ IOS	Bluetooth, Bluetooth connection history, notification alert, camera	authentication key shared by the application, country codes, username, proximity history	Data sharing with the Ministry for Solidarity and Health	13,979,446	205,814
France	StopCovid	Android/ IOS	Bluetooth, Bluetooth connection history, notification alert, camera	authentication key shared by the application, country codes, username, proximity history	Data sharing with the Ministry for Solidarity and Health	1,932,231	78

Germany

Like many countries, Germany saw it was worth having a DCT app as well. Corona-Warn-App was launched on June 15th, 2020 by the government of Germany. It relies on Bluetooth with a decentralised architecture. "Corona-Warn-App" uses Apple/Google APIs. By the end of February 2021, it reached 26.2 million downloads (40,31% of the popultaion), with 478,172 notifications sent of which 286,470 to positive users (60% of the notified)[12].

The following table summarises the main information about this DCT app:

Country	App Name	Platform	Permission Required	Data Collected	Privacy Policy	No of Downloads	No of positive users
Germany	Warn-App-Corona	Android/ IOS	Bluetooth, Exposure Notifications	Does not store any data - however it accesses the IP address, date and time of retrieval, transmitted data volume and the notification messages of whether the data was successfully exchanged. These data are used for system functioning.	No specific information about sharing data with third parties.	26,254,908	286,470

[12] Corona-Warn-App Open Source Project, "Kennzahlen zur Corona-Warn-App." Robert Koch Institute, Mar. 2021.

Italy

Immuni was launched on June 1st 2020 by the government of Italy, for both IOS and Android platforms. It relies on Bluetooth Low Energy with a decentralised architecture and leverages the A/G Framework and Huawei Framework[13].

For its implementation, six guiding principles have been followed: utility, scalability, accessibility, transparency, privacy and accuracy. At the time of writing, "Immuni" has reached 10.400.709 downloads (19,5% of the population with smartphones) with a total number of 15.526 positive users who have updated their keys[14]. Although there is a linear increment in downloads, Immuni is still far from reaching the hoped for 60% of the population[15].

"Immuni" also provides interoperability with other European DCT apps. From October 1 2020, the app supports key exchange protocols with the EU Interoperability Gateway and can communicate with other DCT apps of EU countries.

The following table summarises the main information about this DCT app:

Country	App Name	Platform	Permission Required	Data Collected	Privacy Policy	No of Downloads	No of positive users
Italy	Immuni	Android/IOS	Bluetooth, Exposure Notifications, Location (Android only)	Does not collect any identifying data	No specific information about sharing data with third parties.	10,375,062	14,843

[13] "Immuni Documentation," *GitHub*, Jan. 2020; https://github.com/immuni-app/immuni-documentation (accessed Apr. 03, 2021).
[14] "The numbers of Immuni," Immuni Web Site, Presidenza del Consiglio dei Ministri Apr. 01, 2020. http://www.immuni.italia.it (accessed Apr. 03, 2021).
[15] T. Mackinson, "Immuni: ecco perché, dopo nove mesi, l'applicazione per il contact tracing è una incompiuta abbandonata dalla politica," *Il Fatto Quotidiano*, Apr. 04, 2021. https://www.ilfattoquotidiano.it/2021/04/04/immuni-ecco-perche-dopo-nove-mesi-lapplicazione-per-il-contact-tracing-e-una-incompiuta-abbandonata-dalla-politica/6139505/ (accessed Apr. 05, 2021).

Non European Countries

United Kingdom

On September 2020, the British government launched its NHS COVID-19, available to download in England and Wales (Scotland and Northern Ireland have their own). The app runs on Android and iOS smartphones and can be used by anyone aged 16 and up.

A pilot version, developed by the American software company VMware was made available already in May 2020, but this centralised version was later abandoned due to privacy concerns. Indeed, although the government stated that the collected data would not have been accessible outside the NHS, VMware made it clear that the data might be shared with third party companies. The Commission of Human Rights presented the possibility of personal data being misused. The current second version of the app addressed these concerns by employing a decentralised framework, the Apple/Google Exposure Notification system.

By the end of March 2021 "NHS COVID-19" had reached 22.210.299 downloads[16](38% of the population of England and Wales), with a total of 1.842.261 alerts sent, in response to 902.798 positive test results linked to the app.

[16] NHS, "NHS COVID-19 app statistics," Mar. 2021. https://stats.app.covid19.nhs.uk/ (accessed Apr. 03, 2021).

The following table summarises the main information about this DCT app:

App Name	Platform	Permission Required	Data Collected	Privacy Policy	Country	No of Downloads	No of positive users
NHS-COVID-19	Android/ IOS	Location(Android only), phone, media, storage, camera, microphone, Wi-Fi, device ID,call information, download files without notification, run at startup, prevent the device from sleeping.	The postcode district The symptom information The QR poster codes scanned at venues	No specific information about sharing data with third parties	United Kingdom	22,210,299	902,798

Australia

On April 14th, 2020 Australia launched COVIDSafe. The app has a centralised system architecture and relies on proximity tracing using BlueTrace, the privacy-preserving contact tracing protocol proposed by the Government Technology Agency of Singapore. "COVIDSafe" has already reached 7.453.274 downloads (29% of the population). It collects name, age range, mobile phone number and postcode from its users[17].

On the 6th May 2020, because of issues related to performances with IOS devices, the government of Australia proposed to switch from BlueTrace, a centralised solution, to the decentralised Apple/Google ENF. The switch presented several drawbacks, including affecting the state health authority, which would no longer be in charge of determining or contacting any person from any close contact list. On June 28 2020, the Deputy Chief Medical Officer declared that the government is not interested in solutions that do not have human-in-the loop reporting[18].

The following table summarises the main information about this DCT app:

Country	App Name	Platform	Permission Required	Data Collected	Privacy Policy	No of Downloads	No of positive users
Australia	COVIDSafe	Android/IOS	Bluetooth, battery optimisation, location, list of contacts for 7 days	mobile phone number, name, age range, postcode	Data sharing with the Ministry of Health	7.3 million	

[17] Australian Government Department of Health, "COVIDSafe app," *Australian Government Department of Health*, Apr. 24, 2020.https://www.health.gov.au/resources/apps-and-tools/covidsafe-app (accessed Apr. 03, 2021).
[18] "COVIDSafe," *Wikipedia*. Apr. 01, 2021, https://en.wikipedia.org/w/index.php?title=COVIDSafe&oldid=1015370513. (accessed: Apr. 03, 2021)

2. *Legal framework*

2.1. *The EU Legal Framework*

Collecting and storing personal data is the essence of tracing applications[19]. Any data stored on individual phones is "information 'related' to an individual"[20]. As such, any digital tracing systems put in place within the EU territory must comply with the EU legal framework regarding the protection of personal data: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereafter the GDPR). The immediate reaction of several EU institutions concerning the possible use of tracing applications to combat the pandemic not only confirms the applicability of the GDPR to such systems[21] but also the categorization of this data as "personally identifiable" (GDPR art. 4) and as part of the "special categories" subject to specific requirements for their processing (GDPR art. 9).

Before exposing the conclusions that must be drawn from such wording, it is worth recalling the general principles driving the processing of personal

[19] It is not in doubt that information broadcast by devices and collected by the app are to be considered personally identifiable information as defined by the GDPR because they allow the identification of the users (article 4).

[20] Kirsten Bock et al., Data Protection Impact Assessment for the Corona App v. 1.6 46 Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. [hereinafter DPIA for the Corona App], https://www.researchgate.net/profile/Joerg_Pohle/publication/341041607_Data_Protection_Impact_Assessment_for_the_Corona_App_Version_16/links/5eaa6932299bf18b9587dc54/Data-Protection-Impact-Assessment-for-the-Corona-App-Version-16.pdf?origin=publication_detail (accessed June. 29, 2020).

[21] Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis: A toolkit for member states, 07/04/20 ; Commission recommendation 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)2296 final of 8/04/20; EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels, réf. OUT2020-0028; E Health Network: Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States Version 1.0 15.04.2020; Communication from the Commission Guidance on Apps supporting the fight against COVID-19 pandemic in relation to dataprotection C(2020) 2523 final of 16 /04/20; European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, 19/03/20).

data according to article 5(1) of the GDPR, namely the lawfulness, fairness, and transparency of the processing (1); the principle of purpose limitation (2); data minimization (3); accuracy (4); storage limitation (5); integrity and confidentiality (6) and accountability (7)[22]. The application of these principles has been commented in the various reactions of the EU institutions when considering the development of tracing applications.

2.1.1. *General Principles under the GDPR*

(1) Lawfulness, fairness, and transparency

Collecting and using personal data relies on an appropriate lawful basis. Even if the proximity- tracing app takes place on a voluntary basis, "it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest i.e. Art. 6(1)(e)

GDPR." It requirement for "the enactment of national laws, promoting the voluntary use of the app without any negative consequence for the individuals not using it, could be a legal basis for the use of the apps[23]."

To guarantee fairness, how the processing may affect individuals targeted by the app must be considered. "In order to ensure their fairness, accountability and, more broadly, their compliance with the law[24], algorithms must be auditable and should be regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny[25]".

Transparency implies that all information related to the data processing is made available to individuals concerned.

[22] Please note that the following general presentation (1.2.1.1.) is retrieved from a document issued by the WP05 scientific advisory group of the Luxembourg task force on Covid-19 that collaborated with the LEGAFIGHT experts' group. The document quoted is the 3Report on Digital Tracing Proximity in the Context of the Covid-19 crisis of 27/04/2020, authors D. Dietrich, G. Lenzini, Ph. Valoggia, G. Fagherazzi, R. Gomez Bravo, J. Schulz, D. Pogorelov, R. Vaccarolli.

[23] EDPB, Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, *loc. cit.*

[24] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit.*

[25] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, *loc. cit.*

(2) Purpose limitation

Personal data can only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose"[26], meaning that data collected by proximity-tracing solution must only be used to achieve the purpose of the processing operation. In addition, it must be of limited of duration. Thus, once the COVID-19 crisis is over, proximity-tracing activity should not remain in use, and as a general rule, the data collected should be erased or anonymised[27].

In addition, "a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases (mobile applications and servers)[28]".

(3) Data minimization

Personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[29]". Thus, only data that are relevant to fulfill the purpose of the processing activity can be collected. "Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimization. In addition, doing so would create major security and privacy risks[30]". Thus, location tracking of individual users should be avoided.

"The application should not collect unrelated or unneeded information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.[31]".

(4) Accuracy

In comparison with manual proximity-tracing, automatic proximity-tracing will increase the accuracy of data collected. Indeed, in manual proximity tracing, an individual is likely to either forget people he had been in contact with or not being able to identify whom he met.

[26] GDPR, art. 5(1)(b)
[27] EDPB, Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, *loc. cit.*
[28] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit.*
[29] GDPR, art. 5(1)(c)
[30] EDPB, Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, *loc. cit.*
[31] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit.*

"A mechanism should ensure that whenever a person is declared as COVID19-positive, the information entered in the app is correct, since this may trigger notifications to other people concerning the fact that they have been exposed. Such mechanism could be based, for instance, on a one-time code that can be scanned by the person when the result of a test is given to him/her".

(5) Storage limitation

Data collected must not be kept for longer than necessary. In the context of proximity- tracing, the retention period corresponds to COVID-19 maximal incubation period to which is added the necessary time for testing (1 month). After this delay, proximity- tracing data must be erased or anonymised[32].

(6) Integrity and confidentiality

Personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures[33]".

(7) Accountability

"To ensure accountability, the controller of any contact tracing application should be clearly defined[34]".

The GDPR provision on accountability focuses on two main elements: the need for a controller to take appropriate and effective measures to implement data protection principles; and the need to demonstrate upon request that appropriate and effective measures have been taken. It means that the controller is able to provide evidence of appropriateness and effectiveness of measures implemented.

Because contact-tracing applications put individual's privacy at risk, "the general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19". Therefore, "the stages of deployment of the application must make it possible to progressively

[32] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit*.
[33] GDPR, art. 5(1)(f)
[34] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit*.

validate its effectiveness from a public health point of view. An evaluation protocol, specifying indicators allowing to measure the effectiveness of the application, must be defined upstream for this purpose[35]".

In addition to compliance with data protection principles described above, it is necessary to guarantee individual rights. Under the GDPR provisions, individuals have the following rights: the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to object to processing, the right to data portability, the right to not be subject to automated decision making and profiling.

The rights available to individuals depend on the lawful nature of the basis of the processing. If the legal basis is that of public interest[36], then the right to data portability is not available.

Due to the COVID-19 outbreak context, some restriction to the right of rectification can also be derogated[37].

It is interesting to observe that, in its *Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, the European Data Protection Board stressed that if someone is informed of his/her proximity with a positive infected individual, the functional requirement that consists in "providing advice on next steps" should not be fully automated. "It is advisable that a call-back mechanism is put in place where the person is given a telephone number or a contact channel to get more information from a human agent. Also, in order to avoid stigmatization, no potential identifying element of any other data subject should be part of this "advice", nor should the use of the app, or part of it (like dashboards, configuration settings etc.), allow the re-identification of any other persons, infected by COVID-19 or not[38]".

Finally, a data protection impact assessment (DPIA) must be carried out "before implementing such tool as the processing is considered likely

[35] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit*.
[36] GDPR, art. 5(1)(e)
[37] It is to be noted that none of the national legal provisions explicitly refer to such issue.
[38] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit*.

high risk"[39] (art. 35 (1) GDPR[40]). Health data pertains to data types termed "special categories of data" (GDPR, art. 9) and is processed, within the frame of tracing applications, with the use of a new technological solution. This undoubtedly augments the risk of misuse. Therefore, the EDPB strongly recommended the publication of DPIAs if digital tracing systems were to be implemented by member states.

2.1.2. *Specificities of Data Processed by Tracing Applications*

Special categories of personal data were established to allow for a specific protection regarding "sensitive data". "The history of Europe in the twentieth century shows that the misuse of sensitive data […] can facilitate human rights abuses on a large scale. Misuse of sensitive data can also have serious consequences for individuals, such as unfair discrimination"[41]. Data concerning health are categorized as sensitive data. Consequently, and according to article 9 (1), their processing is prohibited unless its objective falls in one of the categories explicitly mentioned by its paragraph 2. In the specific case of tracing applications, such processing can be performed on the basis of article 9 (2) (i) "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy". As we shall see, where some Member States chose to ground the national legal framework of the app on article 9 (2) (i) GDPR[42], in Germany instead, in the absence of a specific statute regarding the tracing application, a discussion took place as to whether the only possible legal basis for the

[39] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, *loc. cit*.

[40] "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

[41] L. Georgevia, Ch. Kuner, "Article 9. Processing of special categories of personal data" *in the EU General Data Protection Regulation (GDPR). A Commentary.*; Ch. Kuner, Lee A. Bygrave, Ch. Docksey (ed.) pp. 375-383, at p. 369.

[42] Reference to this article is explicitly made in the French legislation regarding the tracing application, see *infra* "*National Report: France*".

implementation of digital tracing was the obtention of the user's consent[43]. Such approach does not seem to be in line with the various statements of the EU institutions and more specifically the letter issued by the EDPB. Taking into consideration its recommendations, both France and Italy, whose legislations clearly refer to article 9 (2) (i), established a framework that designs safeguards based on the purposes of processing underlying the GDPR as described in section 1.2.1.1.

[43] See *infra* "*National Report: Germany*".

2.2. *Overview of some national legal frameworks*

2.2.1. *Belgium*

Tracing application

Name

CoronAlert

Launch date

The application was launched on September 30th, 2020. It was developed by two Belgian companies (Devside and Ixor). The CoronAlert application is based on the German Corona-Warn application.

The app is available in four languages: English, French, German and Dutch.

The app was developed pursuant to an initiative from the Belgian Government and federated entities.

Independent specialists were involved in the design of the app from the start, including ICT, security, privacy and legal protection. The software also underwent an extensive security audit by an external party (NVISO). An impact assessment was conducted by the Belgian Data Protection Office and Sciencesano, a public institution with legal personality established by the law of 25 February 2018 authorising Sciensano to perform public and animal health assignments.

The assessment is available online:

https://coronalert.be/wp-content/uploads/2020/09/20200915-DPIA_contactopsporingsapplicatie-Belgie-V.5_final_FR.pdf

As per law (Cooperation agreement of 25 August 2020 between the Federal State, the Flemish Community, the Walloon Region, the German-speaking Community and the Joint Community Commission, concerning the joint processing of data by Sciensano and the contact centres, health inspections and mobile teams designated by the competent federated

entities or by the competent agencies within the framework of a contact investigation of persons (presumed) to be infected with the coronavirus COVID-19 on the basis of a database at Sciensano, art. 5) a specific website where users can find any information regarding the application was created: https://coronalert.be

Modifications

There are no modifications (be they technical or of legislative nature) to be reported.

Technical characteristics and development

- Protocol and Data security

CoronAlert's system architecture runs on IOS and Android and relies on Bluetooth Low Energy to gather data by proximity detection. CoronAlert has decentralised data management and processing. It uses the Apple/ Google APIs and deletes any data collected after 14 days.

Data storage

Data storage is operated by Sciensano.

Source code

The source code is available online : https://github.com/covid-be-app

- Functionalities

CoronAlert's functions are aligned with the German tracing application (Corona-Warn).

Like Corona-Warn, CoronAlert has two main functions. The first is the exposure notification function. In particular, the app shows each user his/ her risk status depending on contacts recorded by the system and the specific characteristics of the encounters with persons that have tested positive to the virus. There are three types of status information: a) low risk (no encounter with infected persons, such encounters not exceeding the defined threshold value); b) increased risk (the person encountered at least one person in the last 14 days who has been diagnosed with COVID-19); c) unknown risk (the app has not been activated for long enough by the person, then no risk of infection can be calculated).

The app has also another important (optional) function, namely it enables users to retrieve Covid-19 test results electronically. If the testing laboratory supports the electronic process, tested users can use the QR code they receive during the test to retrieve their results on the app.

- Data use[44]

CoronAlert records and uses a combination of anonymous data and minimal personal data.

Personal data is mainly stored on the user's phone and only limited information is sent to the central server if the user decides to send it (the decentralised approach).

Data is uploaded by a central server. This central server is hosted by Sciensano in the European Union.

- Retention period

The personal data stored on each user's phone and on the central server are automatically removed after 14 days.

The CoronAlert app will be deactivated at the date determined by the applicable Belgian law.

- Expression of consent:

User consent is required to download the application to the phone.

Health entitie(s) related to the application

Regional Heath administrations and Sciensano.

Legal Framework

Supranational legal framework

General Data Protection Regulation Article. No specific article of the GDPR is referred to in the national Act.

National legal framework

Accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté ermanophone et la Commission

[44] The information related to data use and retention period was retrieved from the official French website of the "tousanticovid" application https://bonjour.tousanticovid.gouv.fr/privacy-en.html

communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspections d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID–19 se fondant sur une base de données auprès de Sciensano (Cooperation agreement of 25 August 2020 between the Federal State, the Flemish Community, the Walloon Region, the German-speaking Community and the Joint Community Commission, concerning the joint processing of data by Sciensano and the contact centres, health inspections and mobile teams designated by the competent federated entities or by the competent agencies within the framework of a contact investigation of persons (presumed) to be infected with the coronavirus COVID-19 on the basis of a database at Sciensano), confirmed by Loi portant assentiment à l'accord de coopération du 25 août 2020 entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspection d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 se fondant sur une base de données auprès de Sciensano (Act confirming the Cooperation agreement of 25 August 2020).

The Cooperation agreement of 25 August 2020 provides for a general legal framework for the tracing application that was later implemented through another "cooperation agreement" of 30 October 2020 (Accord de coopération d'exécution entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980 - Cooperation agreement of 30 October 2020 between the Federal State, the Flemish Community, the Walloon Region, the German-speaking Community and the Joint Community Commission, concerning tracing applications).

This agreement deals more specifically with the tracing application in its Chapter VIII, providing a technical description of the technology used for the application and guaranteeing the temporary and voluntary nature of the system (art. 14 § 2, 8: voluntary activation of the app; art. 14 § 2,

9; voluntary sending to the server of a positive screening result; art. 14 § 5 activation and deactivation of the app). It also strictly limits the use of the tracing as well as that of the data processed through it to the purposes set down in article 14, § 1 (sending a warning to a person who has been in close contact with someone who tested positive for the coronavirus).

It is to be noted that while the cooperation agreement authorised the implementation of "regional tracing applications", the choice was made to implement a single application at the national level, with its functioning and legal framework described in a further cooperation agreement of 13 October 2020.

The agreement of 13 October 2020 presents in a detailed manner the functionalities of the application and requires, *inter alia*, that the system implemented rely on Bluetooth Low Energy to gather data by proximity detection. It also requires that clear and comprehensible information regarding its functioning as well as how data is to be processed be provided to users. This information will be made available when installing the application but should also be accessible on the website related to the application (https://coronalert.be). Under article 6 of the cooperation agreement a regular evaluation of the functioning of the application as well as of its necessity must be conducted by the "Comité interfédéral de testing et tracing" (Interfederal committee of testing and tracing)

An opinion of the Belgian Conseil d'Etat was made regarding a draft bill regarding tracing applications (Avis 67.424/3du 26 mai 2020 sur une proposition de loi 'relative à l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population' – Doc. Parl., Chambre, 2019-20, n°55-1251/001).

The opinion is available online: http://www.raadvst-consetat.be/dbx/avis/67424.pdf#search=tra%C3%A7age

The draft bill was finally not adopted.

However, since the regulation eventually took the form of a cooperation agreement, no opinion of the Conseil d'Etat was required.

Processing and retention of data:

Processing of data is done in accordance with articles 5 and 25 of the General Regulation on Data Protection (art. 14, § 4).

However, it has to be noted that "Sciensano will only be able to respond to requests from users where it will be able to link the data processed in the context of the Contact Tracing App to the specific user. To be able to link the data to the user, Sciensano would need to obtain additional data. As the Contact Tracing App is built on technology aiming at protecting the privacy of the users as much as possible, it is not desirable that Sciensano processes additional data merely to identify the user. Pursuant to article 11 GDPR, Sciensano cannot be obliged to process such additional data to identify the user for the sole purpose of complying with the data subject rights under the GDPR. This means that in practice, users will not be able to exercise their data subject rights unless additional information is provided to Sciensano."

The retention period of data cannot exceed a period of three weeks.

This applies for personal data stored on each user's phone and on the central server (art. 14 § 6).

Data related to the voluntary communication of a confirmed COVID-19 coronavirus infection as well as the data used for the authentication of the infected person must be immediately erased (art. 14 § 6).

Political discussion

No political discussion is to be reported, however a public consultation on the app was open to the public. Conclusions drawn from this consultation are available online (English):

https://www.esat.kuleuven.be/cosic/sites/corona-app/wp-content/uploads/sites/8/2020/09/Public_consultation_v1_0_sep25_2020-1.pdf

Questions regarding different issues (transparency of use, security of data) are answered in the "Conclusions" published after the consultation was closed. Some suggestions made by participants were taken into account (e.g. including a FAQ in the app and on the website: https://www.coronalert.be in order to render the app more inclusive).

Media and Human Rights associations report discussions regarding the issue of data protection (see Ligue des Droits Humains https://www.liguedh.be/applications-de-tracing-pour-la-ligue-des-droits-humains-la-vigilance-reste-de-mise/).

Opinion of national committees

Avis relatif à un projet d'arrêté royal portant exécution de l'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes

ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano et d'un projet d'accord de coopération d'exécution conclu entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980 (CO-A-2020-099)

Avis n°79/2020 du 7septembre 2021
Available at :
https://www.autoriteprotectiondonnees.be/publications/avis-n-79-2020.pdf

According to this opinion, the implementation of "CoronAlert" was considered possible, provided that some clarifications are made to the text presented. It was stressed that responsibility for compliance with the GDPR should be vested in public controllers and that users should be clearly informed on the functionalities of the application and the processing of their data when downloading the application.

Rapport en réponse à une possible atteinte de la vie privée par Google GAEN
Comité interfédéral de testing et tracing, 27 avril 2021
Available at:
https://www.corona-tracking.info/presse/?lang=fr

A possible breach of privacy due to the stocking of data in logs or diaries (for the Android system) was reported to the committee. Other applications than the tracing app could have access to this data and correlate it with other data. Google was alerted of this risk and indicated to have remedied it by developing a special update for the Android system.

- Critical appraisal
Mutatis mutandis, the critical appraisal as to the system put in place in Germany applies to the Belgian Legal framework (see *supra* the Report on Germany).

The main criticism to be addressed is the lack of transparency regarding the control that will be put in place to assess the compliance of the system with data protection regulations and the unclear role of the committees to whom such control has been assigned by the agreement of 13 October 2020 and more precisely its article 6 ("Le fonctionnement et la nécessité de l'appli sont régulièrement contrôlés, évalués et rectifiés sous l'impulsion du Comité interfédéral de testing et tracing qui se compose de représentants d'entités fédérées, de Sciensano, de la Plate-forme eHealth et de deux experts scientifiques. Ce comité peut être soutenu par un groupe de travail interdisciplinaire d'experts scientifiques. L'appli fera également l'objet d'un audit de la sécurité de l'information par une instance indépendante de celle qui a développé l'appli, qui permettra notamment de vérifier si cette appli satisfait aux conditions en matière de sécurité de l'information et est conforme à la réglementation en vigueur").

The efficiency of the tracing app was publicly queried in several questions addressed by Member of Parliaments to the Federal government:

La Chambre des Représentants - Question et réponse écrite n° 55-16 : Application Coronalert, available on line:
https://www-stradalex-com.proxy.bnl.lu/fr/sl_src_publ_div_be_chambre/document/QRcrb_55-b032-1196-0016-2020202106324

Social acceptance and efficacy
Please note that the numbers below were retrieved from an article published in Le Soir, no information being publicly available at the time of the closing of the research project[45].

Numbers are now available on the website of the Interfederal Committee of Testing and Tracing
https://www.corona-tracking.info/appli/coronalert-counter/?lang=fr

Number of users (as of February 3, 2021)
Around 2 000 000 users (15% of the Belgian population equipped with a mobile compatible with the application).

Number of cases reported (as of February 3, 2021)

[45] https://plus.lesoir.be/338717/article/2020-11-19/lapplication-coronalert-atteint-largement-le-seuil-dadhesion

Around 100 000.

The article published in Le Soir stresses that the Dutch speaking population was keener on downloading the application. However, after an investigation conducted by the consumer organization "Test Achat" leading to the publication of an article, the Walloon population was reported to feel more confident with the protection of privacy and the processing of the personal data and was said to be ready to install the app.

Bibliographical references

Websites:

Website of the application:
https://coronalert.be

Website of the Comité interfédéral de testing et tracing
https://www.corona-tracking.info

Opinions:

Avis n°79/2020 du 7septembre 2021 relatif à un projet d'arrêté royal portant exécution de l'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano et d'un projet d'accord de coopération d'exécution conclu entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant la ou les applications numériques de traçage des contacts, conformément à l'article 92bis, § 1er, alinéa 3, de la loi spéciale de réformes institutionnelles du 8 août 1980 (CO-A-2020-099)

https://www.autoriteprotectiondonnees.be/publications/avis-n-79-2020.pdf

Rapport en réponse à une possible atteinte de la vie privée par Google GAEN

Comité interfédéral de testing et tracing, 27 avril 2021
Available at:
https://www.corona-tracking.info/presse/?lang=fr

Other:

La Chambre des Représentants - Question et réponse écrite n° 55-16 : Application Coronalert, available on line:
https://www-stradalex-com.proxy.bnl.lu/fr/sl_src_publ_div_be_chambre/document/QRcrb_55-b032-1196-0016-2020202106324

2.2.2. *France*

Tracing application

Name

StopCovid (launched on 02-06-2020 and dismissed after the CNIL announcement on 04/09/2020/)
TousAntiCoviD (launched on 22-10-2020 and currently in use).

The latest version of the application (TousAntiCoviD), with its development overseen by INRIA (Institut National de Recherche en Science et Technologie du Numérique), is under the responsibility of the General Health Directorate of the Ministry for Social Affairs and Health (Direction de la Santé du Ministère des Affaires Sociales et de la Santé).

Launch date
StopCovid was first launched on June 2nd, 2020.

Its impact was disappointing with only 2.4 million downloads after two months, from a population of about 70 million of which 77% are smartphone users (95% between the ages of 19 and 39)[46]. According to a government report, dated October 2020 and covered by several newspapers among which Le Monde[47], with 7969 reported positive cases, the application managed to send only 472 notifications. According to Data Publica, a public observatory, despite 59% of the population being favourable to StopCovid,

[46] Comité de Contrôle et de Liaison – COVID-19, Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie, Avis du 15 septembre 2020 available at: https://solidarites-sante.gouv.fr/IMG/pdf/avis_du_ccl-covid_du_15_09_20._pour_un_systeme_d_information_au_service_d_une_politique_coherente_de_lutte_contre_l_epidemie.pdf
[47] https://www.lemonde.fr/pixels/article/2020/10/14/emmanuel-macron-acte-l-echec-de-l-application-stopcovid-qui-sera-renommee-tous-anti-covid_6056049_4408996.html

54% of them did not trust the government's usage of their data[48].

According to a recommendation by the CNIL[49], the application was found to be non compliant with good data protection practices ("Des mauvaises pratiques ont également été relevées"). Reasons for this assessment included incomplete information, ambiguities in protecting the rights of users, security issues regarding data sharing within certain organisations, and some insufficient guarantees that data would be preserved only for specific time periods. In part, the failure of the app was as a result of poor advertising and guidelines ("[la CNIL] s'interroge sur la cohérence de la politique poursuivie et appelle le gouvernement à faire preuve de cohérence. Un premier pas consisterait à lancer une campagne d'information sur l'application")[50].

Modifications

On October 26th, 2020, France decided to launch the second version of the application, known as "TousAntiCovid", with better functionality, but the same system architecture, and a better advertisement plan. The new version also benefits from security recommendations gathered by public and private entities such as INRIA (Institut National de Recherche en Science et Technologie du Numérique), ANSSI (Agence Nationale de la Sécurité des Systèmes d'Infromation), Orange and Dassault. TousAntiCovid performance is definitely better than its predecessor's: by the end of March 2021 it reached a total number of downloads and activations of 14,190,640 with 140,490 notifications sent out of 229,570 positive users.

Technical characteristics and development

- Protocol and Data security

[48] COVID-19 L'OBSERVATOIRE Questions spécifiques : perceptions de l'application STOPCOVID et regards sur l'enjeu du partage des données personnelles Rapport de résultats – Mai 2020 available at https://harris-interactive.fr/opinion_polls/perceptions-de-lapplication-stopcovid-et-regards-sur-lenjeu-du-partage-des-donnees-personnelles/

[49] Délibération n° 2020-087 du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d›information développés aux fins de lutter contre la propagation de l›épidémie de COVID-19 (mai à août 2020) (demande d'avis n° 20014534), available at https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_10_septembre_2020_sur_la_mise_en_oeuvre_des_systemes_dinformation_contre_la_propagation_de_covid-19.pdf

[50] CCL – COVID-19, Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie, Avis du 15 septembre 2020, *loc. cit.*

TousAntiCovid, like its predecessor StopCovid, relies on ROBERT (ROBust and privacy-presERving proximity Tracing) protocol and uses a centralised architecture.

This choice may surprise, but ROBERT's authors have clarified that the terms "decentralise" and "centralise" are often misunderstood[51], and argued that the "centralised choice is the most respectful of privacy. It is worth taking a moment to understand this argument.

"A 'fully decentralised' approach is not realistic for proximity tracing," they say, "because only relying on data exchanges between applications to inform who is at risk or not [..] would depend on the current proximity between people leading to slow and incomplete information delivery"[52]. There must also be a back-end system to share information with applications. The matter is, therefore, "how to distribute the data between the server and devices (and here "only data allowing to establish proximity contacts of individuals diagnosed positive are sent"), and where the status of the user (at risk or not) is verified"[53]. We talk of a "decentralised system", when "this verification is performed on the device of the user"; we talk of a "centralised system" when the verification is done by the central server. The authors of ROBERT clarify that opting for a "decentralised system" would imply that all applications must receive information about the users diagnosed positive, with an evident risk for those vulnerable individuals' privacy; it makes it easier for malicious users to detect that a person has been diagnosed positive"[54].

[51] INRIA, Proximity Tracing Applications: The misleading debate about centralised versus decentralised approaches. April 2020 (available at https://raw.githubusercontent.com/ROBERT-proximity-tracing/documents/master/Proximity-tracing-discussion-EN.pdf)
[52] *Ibid.*
[53] *Ibid.*
[54] *Ibid.*

Data storage:
Health Data Hub hosted by Microsoft
Source code
Publicly available on the INRIA website
https://gitlab.inria.fr/stopcovid19/accueil

- Functionalities

The TousAntiCovid app informs application users that they have been in proximity to at least one other user who has since tested positive for COVID-19 and who may have been infected. It provides information on the epidemiological situation in France with a filtering option by place of interest (figures are provided at national, regional and sometimes local level); number of positive cases and patients admitted in resuscitation units; virus reproduction number; rate of occupation of resuscitation units; incidence rate and positivity rate. It provides an updated map of screening centres as well as customised advice, such as guiding at-risk contacts towards competent healthcare professionals for treatment and testing and for self-isolation.

- Data use[55]

Data will be used in order to inform users who have been in proximity to at least one other user who has since tested positive for COVID-19; guide at-risk contacts towards competent healthcare professionals for treatment and testing, as the case may be; compile anonymous statistics for the purposes of improving the performance of the health model used by the application; generate travel exemption forms.

A randomly generated QR code with non identifying information will be fixed to the test results sent to individuals who have tested positive for COVID-19. Individuals who have tested positive for COVID-19 will be able to use this QR code in order to identify themselves on the app.

Information related to searches done on the phone regarding "places of interest" or guidance on self-isolation will not be processed by the Ministry for Social Affairs and Health and only be stored on users' mobile phones. The same rule applies to information related to travel where storage on mobile phones allows for a quicker completion of exemption forms.

[55] The information related to data use and retention period was retrieved from the official French website of the "tousanticovid" application https://bonjour.tousanticovid.gouv.fr/privacy-en.html

- Retention period

As for the notification of users who have been in proximity to another user that tested positive for COVID-19, data will be processed in the time period of six months from the declaration of the end of the state of emergency. "Proximity history" data will be retained for no longer than two weeks after being shared. Regarding travel exemption forms, the retention period will be of 24 hours starting from the validity date. The postcodes used to seek information related to a place of interest will only be stored on the mobile device. Data storage will last until the information is deleted by users or if a request using a new postcode is made.

The data used for guidance provided in the event that self-isolation is required will only be stored in the application and will not be shared with the central server. It will be retained until its deletion by the user.

All data stored on the device can be deleted at any time. Uninstalling the application will lead to the deletion of all data stored on the server.

- Expression of consent:

User consent is required to download the application to the phone, to download travel exemption forms as well as for to send the virological or serological status of the user to the server.

Health entitie(s) related to the application

Ministry for Social Affairs and Health

Several entities related to the National Health Agency (Agence Nationale de Santé Publique).

Legal Framework

Supranational legal framework

General Data Protection Regulation Article 6.1.e

National legal framework

The French legal framework was established by an Act allowing for the adoption of delegate legislation (decrees established under State Council decrees). This is a rather common procedure in the field of personal data (see art. 26 of the "loi n° 78-17 du 6 janvier 1978 relative à l'informatique,

aux fichiers et aux libertés" Act on Data Protection allowing for such procedure).

1/Loi n° 2020-546, 11 mai 2020, prorogeant l'état d'urgence sanitaire et complétant ses dispositions, (art. 11) JORF n° 0116, 12 May 2020 (Act of 11 May 2020 proroguing national health emergency), last amendment by loi n° 2021-160 du 15 février 2021 prorogeant l'état d'urgence sanitaire (Act of 15 February 2021 proroguing national health emergency).

Act of 15 February 2021 extended the National health emergency until 31 December 2021.

2/ Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions

3/ Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid », JORF n° 0131, 30 May 2020 (Decree of 29 May 2020 pertaining to the processing of data entitled "StopCovid" (since renamed TousAntiCovid) introduced after consultation with the Commission Nationale Informatique et Liberté (CNIL, the French Data Protection Authority).

4/ Décret n° 2021-157 du 12 février 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » (Decree of 12 February 2021 modifying Decree of 29 May 2020 pertaining to the processing of data entitled "StopCovid").

1/ Act of May 11 (art. 11) delegated to the French government the power to process and share personal data concerning health "when necessary" in the framework of an "information system" established under a State Council decree and implemented by the Ministry in charge of Health which led to the enactment of the Decree of 29 May 2020 pertaining to the processing of data entitled "StopCovid". The tracing application itself is not mentioned by the Act, which also fails to provide for a definition of "information systems". The Act expressly indicates the type of data that may be collected through such systems as well as the duration of their storage period.

In its section related to the administration of data concerning health that refers to information systems, it can be inferred from the French Public

Health Code (Code de la santé publique[56]), that they correspond to systems whose objective is to make data, more precisely data concerning health, available to public services and institutions.

2/ This was further confirmed by the Decree of 29 May 2020 concerning information systems cited in article 11 of the Act of 11 May 2020 (Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions), which adapted the existing information system managed by the National Health Insurance Fund to the sanitary context. This information system, centralised by design, is very broad in its scope as it covers the whole national territory and makes data accessible to a wide range of actors (besides medical staff, several public institutions as well as subcontractors and pharmacists may have access to data)[57]. This system, established in an emergency context, is two-fold. It consists in a prevention and screening system (Si-DEP – Système d'information ou de dépistage) and in a contact tracing system, that can be both manual and digital.

Moreover, paragraph II, 2°) of article 11 refers in a general manner to systems aiming to identify "people at risk of infection, by collecting information on contacts of infected people and, if necessary, by carrying out health surveys, in particular in the presence of grouped cases"[58], which is the objective of tracing applications.

It must be stressed that paragraph II, 4°) of article 11 refers to the development of a digital application for contact tracing, distinguishing this "information system" from all those mentioned by the Act. Nevertheless, the prevention and screening system (Si-DEP) has proved in practice to be the system used to send alerts to users of the application[59].

Data collected, processed and shared through information systems is personal data related to "the virological or serological status of the person"

[56] https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072665/
[57] N. Metallinos, Quel encadrement pour les outils numérique du dépistage Covid-19?, Communication Commerce Electronique, 2020, n°7, pp. 42-47.
[58] ("II. Les systèmes d'information mentionnés au I ont pour finalités : (…) l'identification des personnes présentant un risque d'infection, par la collecte des informations relatives aux contacts des personnes infectées et, le cas échéant, par la réalisation d'enquêtes sanitaires, en présence notamment de cas groupés"
[59] N. Metallinos, *op. cit.,* n°10.

and to "evidence of clinical diagnosis and medical imaging" (art. 11 I Act of 11 May 2020).

The retention period of the data processed varies from three months after data collection until the end of the national health emergency for some data that facilitates epidemiological surveillance. The extension of the storage duration period for these specific data must be authorised by means of a decree by the State Council, adopted once the opinion of the CNIL and a "Covid-19 Special Liaison Committee" (le Comité de Contrôle et de Liaison Covid-19[60]), in charge of involving Parliament and Civil Society in governmental responses to the pandemic through contact tracing as well as the deployment of the information systems provided for this purpose (art. 11 I Act of 11 May 2020), has been delivered.

Tracing application: It must be noted that according to the Act of 11 May 2020 (art. 11 I), the Ministry in charge of Health, as well as several entities related to the National Health Agency (Agence Nationale de Santé Publique[61]), may adapt, for the same purposes and during the same timeframe, the existing information systems and may provide for the sharing of data under the same conditions. The 11 May 2020 Act was therefore designed to allow the implementation of a tracing application at a later stage. Such system was established by the Decree of 29 May 2020 pertaining to the processing of data labelled "StopCovid".

3/ Decree of 29 May 2020 details the processing of personal data in the framework of the mobile contact tracing application called "StopCovid" (later renamed TousAnticovid), allowing its users to be informed when they have been near at least one other user covid-19 diagnosed or positively screened user. The tracing system is based on the conservation of the proximity history of pseudonyms issued via Bluetooth technology. For a detailed presentation of the functioning of the application, see supra, 1. 4.

The decree refers to GDPR (Regulation (EU) of April 27, 2016) and more precisely to article 6 § 1 e), the processing of the data collected by the application being deemed "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" and article 9 § 2 i), the processing of the data collected by the application being deemed "necessary for reasons of public interest in the

[60] https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/etat-des-lieux-et-actualites/article/le-comite-de-controle-et-de-liaison-covid-19-ccl-covid
[61] http://fr.ap-hm.fr/site/corevih-poc/actu/agence-nationale-de-sante-publique-ansp

area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."

The decree determines the purposes of the processing of personal data implemented, as well as the categories of data recorded (art. 2 I), the recipients of this data, their retention period and the terms and conditions of exercise, by the persons concerned, of the rights which they are entitled to under Regulation (EU) 2016/679 of April 27, 2016 (RGPD). Article 2 II of the decree prohibits the collecting and recording of data allowing the identification of the mobile phone. Furthermore, art. 3 II regulates the roles of subcontractors according to article 28 of Regulation (EU) 2016/679 of April 27, 2016 guaranteeing that processors acting on behalf of the controller are the recipients of data or have access to it only if it is strictly necessary for the exercise of their missions.

Processing and retention of data:

Data processing cannot exceed a period of six months after the end of the state of health emergency. This period slightly exceeds the retention period allowed by the Act of May 11 (finishing with the ending of the State of emergency). This retention period was established by the French Data Protection Authority (CNIL) in its data controller opinion (see *infra*).

The shared authentication key and the permanent random identifier are stored until the user uninstalls the StopCovid application, and at the latest for the period mentioned in the first paragraph of art. 2).

The proximity history data recorded by the application on the mobile phone is retained for fifteen days from their recording by this application (art. 2).

Proximity history data of contacts at risk of contamination that has been shared with the central server are stored for a period of fifteen days from their recording by the application of the mobile phone of the person screened or diagnosed positive (art. 2)

The date of onset of symptoms as well as the randomly generated QR code in case of positive test will not be stored. This data is only processed in order for the server to authorise the user of the application to share his or her proximity history (art. 2).

Actions related to the processing of the data are recorded and stored

for a maximum period of six months from the end of the state of health emergency onwards. This recording includes the identification of the data controller, the traceability data, in particular the date, time and nature of the intervention in the treatment (art. 3).

In line with article 23 of the GDPR, the rights of access, rectification and the right to limitation cannot be exercised with the data controller (art. 4).

4/ Décret n° 2021-157 du 12 février 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » (Decree of 12 February 2021 modifying Decree of 29 May 2020 pertaining to the processing of data entitled "StopCovid").

The decree modifies the name of the StopCovid application renamed "TousAntiCovid". Users are now able to report their status as "contacts at risk of contamination" in order to benefit from a test for covid-19. Additional information on the health situation is provided. The text also allows the collection of the date of the last contact with a person diagnosed or screened positive for the covid-19 virus and extends the duration of the implementation of the application until December 31, 2021.

Political discussion

The "TousAntiCovid application" was established by a State Council decree and therefore did not allow for a specific discussion as to its content. That said, the application was presented to the Parliament on 27 May 2020, after a positive opinion on the project was expressed by the French Data Protection Authority (see *infra*). The vote took place on the government's declaration "relating to digital innovations in the fight against the Covid-19 epidemic". 338 votes for, versus 215 votes against. 21 abstained.

Some reactions:

Cedric Villani (La République en Marche - Mouvement dissident) "Digital tracing is not tracking, and everyone does it."

J.-L. Mélenchon (La France insoumise): "I'm one of those people who doesn't want anyone to know with whom I was within a meter distance for more than a quarter of an hour. This is time for a kiss. That's none of your business."

D. Abad: (Les Républicains): "Either the application is voluntary, and it is ineffective, or it is compulsory, and it is a threat to freedom. StopCovid is a stillborn project, which arrives too late, a bit like the cavalry which always

arrives after the battle in the Lucky Luke comics."

(Sources: website of the Assemblée Nationale).

Opinion of national committees

1/ A first opinion was expressed on April 24th, 2020 regarding the possibility of a tracing application (CNIL, Délibération n° 2020-046 portant avis sur un projet d'application mobile dénommée «StopCovid» (French Data Protection Autority, Opinion of April 24th 2020).

2/ A second opinion was delivered on May 25th, 2020 related to the draft decree concerning the tracing application (CNIL, Délibération n°2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid »).

3/A third opinion was issued on December 20th, 2020 on a Draft Decree amending Decree of 29 May 2020 (CNIL, Délibération n° 2020-135 du 17 décembre 2020 portant avis sur un projet de décret modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid »).

1/ Opinion of 24 April 2020

According to this opinion, the implementation of "StopCovid" was considered possible, provided that it is useful for the deconfinement strategy and that it is designed to protect privacy. In its first and very detailed opinion, CNIL also acknowledged compliance with the General Data Protection Regulation, the French Data Protection Act, the European Convention on Human Rights, the Charter on Fundamental Rights and the Declaration of the Right of Man and Citizen, provided that responsibility would be vested in public controllers, an impact assessment would be conducted and accuracy of data as well as security (integrity and confidentiality) would strictly be guaranteed.

The French Authority requested that:

- the controller be the ministry in charge of health policy;
- the choice to not use the application would not lead to any kind of legal consequences;
- certain technical security measures be implemented.

2/ Opinion of 25 May 2020

According to this opinion, the use of pseudonymised data by the application and the fact that it does not establish a file of infected persons guarantees the respect of privacy. It also observed that a requested impacts

assessment was carried out, recommendations made in its previous opinion had been taken into account and that the temporary and voluntary nature of the system allowed its implementation.

The CNIL, acting as independent supervisory authority, carried out several investigations (9, 25 and 26 June 2020) as to the functioning of the application and its conformity with the GDPR and the Data protection Act. In a communication of 20 July 2020[62] the Authority noted that the functioning of the application complied for the most part with these two regulations but issued a warning on three issues:

- The user's contact history is now filtered to keep only the proximity history (app users who have been in contact within one meter for at least 15 minutes). However, in the first version of the application still in use, this filtering is done at the level of the central server instead of being done at the level of the user's phone, contrary to what the decree provides. This issue has been resolved in the second version of the application, which was released on June 26th.

The CNIL requested through an injunction that the use of this new version be generalised among users.

- The information provided to the application users should be completed with regard to the recipients of this data, the operations for reading the information present on the terminal equipment (carried out via recaptcha) and the right to refuse such operations.
- The subcontract concluded between the Ministry and INRIA (the developer of the application, Institut National de Recherche en Science et Technologie du Numérique) contains a large amount of information required by the GDPR but still needs to be completed, in particular with regard to the subcontractor's obligations.
- An impact analysis relating to data protection has indeed been carried out by the Ministry but is incomplete with regard to data processing carried out for security purposes (anti-DDOS solution collecting the IP address and recaptcha).

The French Data Protection Authority therefore requested the General Health Directorate of the Ministry for Social Affairs and Health to remedy the problems identified in order to comply both with the GDPR and the Data Protection Act. The response provided by the Ministry (not published)

[62] https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles

in August was considered satisfactory by the CNIL[63].

3/ Opinion of 20 December 2020

Two main issues were pointed out. The first one regarded the possibility, then ruled out, to use the application to record visits to public places in order to facilitate alerting those who have frequented them while some people then tested or diagnoses positive for Covid-19 were present.

The second one concerned the priority given to people alerted by the "TousAntiCovid" application to be contact cases for a screening test.

The recording of visits in public spaces (such as restaurants, fitness clubs etc.) envisaged by the Draft Decree with a view to the reopening of such places was considered as part of the functionality of the application and deemed as a complement to it.

It was also observed that such complementary functionality does not use geolocation technology and does not track users of the application; that there is no unique identifier generated for the "contact locations" reported by users screened or diagnosed positive for covid-19 or for those transmitted to the central server for a query; the data reported is separated from that processed within the framework of the ROBERT protocol.

That said, CNIL also reported to be lacking crucial points (the precise list of entities concerned, compulsory or optional nature of such system for these entities, obligation for the persons concerned to record their visits so that they can be alerted in the event of a risk of contamination) in order to assess the proportionality of this complementary function in relation to its purposes. The opinion also stressed that such tracing system be applied only in public spaces presenting a high risk of contamination and that it should, in any event, not be imposed for the visit of places where frequentation is likely to expose the data subject to special protection (places of worship, union meeting places, etc.).

As mentioned, such system was not implemented by the government after all.

As to the priority given to people identified as close contacts, CNIL stated that priority access to screening tests will not be reserved for users of the application, but will be open to all close contact cases, and will therefore

[63] https://www.lexbase.fr/encyclopedie-juridique/58318337-etude-l-application-tousanticovid-anciennement-stopcovid-mise-a-jour-le-16-02-2021

not jeopardise the "voluntary" nature of the application.

Critical appraisal

The legal framework of the French tracing application may be criticised for its complexity and sometimes lack of readability. The counterpart of the system's rigidity is however a strict compliance with GDPR rules as well as a good balance of individual rights and public interests, given the voluntary nature of the application, allowing for the respect of individual freedom, with the consequence, on the other hand, of a low number of downloads.

The requirement of a CNIL opinion before any legislative action counterbalances the delegated nature of the regulation. It is also to be noted that the French government voluntarily presented the application project to Parliament for discussion, asking for an acceptance vote. The opinions of CNIL proved to play their role of "privacy watchdogs". CNIL also carried out investigations that led to an injunction made to the government to improve the right to privacy of users.

There were very few academic debates in France around the legal framework of the tracing application. Most articles were published before the decrees were passed and most of them were expressing concerns as to privacy issues that were raised by CNIL in its opinions and taken into account. As it was observed by some scholars, it is more a matter of "state of mind" than anything else[64], some people being opposed to the application having an "absolute" vision of freedom and not tolerating any intrusion in the private sphere, even as a mere possibility, since the downloading of the application is not compulsory. Most of the time, criticisms are based on very general assumptions. The opinion of the "Commission Nationale Consultative des Droits de l'Homme" (National Consultative Committee on Human Rights) is illustrative of such approach. In its very short opinion on tracing applications[65], issued on its own motion and delivered before the tracing application was implemented, the Committee points out "risks of transversal infringements of fundamental rights and freedoms". The Committee observes that compliance with regulations regarding the protection of personal data "does not guarantee the respect of fundamental rights and freedoms" without providing further explanation. According to the opinion, the request for a free and informed consent being required

[64] A. Bensamoun, N. Martial-Braz, StopCovid : sortir des postures ! Point de vue sur l'avis de la CNIL, Revue Dalloz IP/IT, 2020, n°5 p. 280.

[65] Avis sur le suivi numérique des personnes (Communiqué de presse du 24 avril): https://www.cncdh.fr/sites/default/files/200424_cp_avis_suivi_numerique.pdf

both by the GDPR but also by article 8 of the Human Rights Convention will be difficult to implement. Social pressure to act as reasonable citizens and professional context fear of stigma could alter individuals' consent. The Committee also raises doubts as to the effectiveness of tracing applications technology with regard to the objective of protecting public health. From a socio-economic and technical standpoint, weaknesses of the Bluetooth technology are a threat. Besides, the digital divide could lead to the exclusion of vulnerable people from such system, with the consequence that they could be even more vulnerable to disease. If these two last arguments certainly merit consideration, they are not specific to tracing applications. They certainly call for a global reflection as to the impact of digitalization on people's life. It would however be reductive to present them as obstacle for tracing applications. The conclusive remark of the Committee may be presented as particularly representative of the viewpoint of many opponents to tracing applications. The Committee expresses its fears "that, through a "ratchet effect", the recourse to a follow-up measure, today legitimised by the protection of public health, may in the future encourage the use of this same type of technology for other purposes."

The most critical point lies in the hosting by Microsoft of the French Health Data Hub, especially after the decision of the Court of Justice of the European Union in the *Schrems II* case (CJEU, 16 July 2020, Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18) on the Privacy shield. By an order of 13 October 2020, the Council of State acknowledged the existence of a risk of data transfer from the Health Data Hub to the United States and requests additional safeguards (Conseil d'Etat, ordonnance n°444937 du 13 octobre 2020, *Association le Conseil National du Logiciel Libre et autres*)[66]. In a statement of February 9, 2021 (Communiqué Communiqué du 19 février 2021 relatif à la plateforme des données de santé[67]) issued on its website, CNIL approved the interim measures announced by the Ministry in charge of health consisting in a technical solution avoiding exposure of the data stored on the Health Data Hub for a period not exceeding 2 years. At the expiration of this period, the CNIL calls for the hosting of the hub by entities under the exclusive jurisdiction of EU law. This is however a distinct issue indirectly related to the tracing application and its legal framework[68].

[66] https://www.conseil-etat.fr/actualites/actualites/health-data-hub-et-protection-de-donnees-personnelles-des-precautions-doivent-etre-prises-dans-l-attente-d-une-solution-perenne

[67] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

[68] On this specific issue see N. Metallinos, op. cit., n°3.

Social acceptance and efficacy

Number of users (as of March 31 2021)
14 190 640

From 2 600 000 users by mid-October 2020, the number of users who activated the application rose to 14 190 640 by the 31st of March 2021.

The application has been installed by 21,6% of the French population (67 063 703 people as reported by the Institut National de la Statistique et des Etudes Economiques (on the 1st of January 2020).

Such an increase (only 3,88% had installed it when the decision was taken to modify the application and rename it) may be due to its new functionalities. This is however a mere assumption and further investigation would be needed to understand the reasons for it.

Number of cases reported (as of March 31 2021)
140 490

Bibliographical references

Websites:

https://bonjour.tousanticovid.gouv.fr/privacy-en.html

https://www.lexbase.fr/encyclopedie-juridique/58318337-etude-l-application-tousanticovid-anciennement-stopcovid-mise-a-jour-le-16-02-2021

Opinions:

Comité National Pilote d'Ethique du numérique, Réponse à la saisine du Ministre de la Santé et des Solidarités et du Secrétaire d'Etat chargé du Numérique, Enjeux d'éthique concernant des outils numériques pour le déconfinement (14 May 2020),
https://www.ccne-ethique.fr/sites/default/files/a_la_une/cnpen-ethique-numerique-deconfinement-2020-05-14.pdf

CNIL, Délibération n° 2020-046 portant avis sur un projet d'application mobile dénommée « StopCovid »,
https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_

avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf

Commission Nationale Consultative des Droits de l'Homme, Avis sur le suivi numérique des personnes

https://www.cncdh.fr/sites/default/files/200424_cp_avis_suivi_numerique.pdf

CNIL, Délibération n°2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », JORF n°0131 du 30 mai 2020

Comité de Contrôle et de Liaison – COVID-19, Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie, Avis du 15 septembre 2020

https://solidarites-sante.gouv.fr/IMG/pdf/avis_du_ccl-covid_du_15_09_20._pour_un_systeme_d_information_au_service_d_une_politique_coherente_de_lutte_contre_l_epidemie.pdf

CNIL, Délibération n° 2020-135 du 17 décembre 2020 portant avis sur un projet de décret modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid »), JORF n°0039 du 14 février 2021

CNIL, Communiqué du 19 février 2021 relatif à la plateforme des données de santé (Health Data Hub)

https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

Polls:

COVID-19 L'OBSERVATOIRE Questions spécifiques : perceptions de l'application STOPCOVID et regards sur l'enjeu du partage des données personnelles Rapport de résultats – Mai 2020

https://harris-interactive.fr/opinion_polls/perceptions-de-lapplication-stopcovid-et-regards-sur-lenjeu-du-partage-des-donnees-personnelles/

Articles:

A. Bensamoun, N. Martial-Braz, StopCovid : sortir des postures ! Point de vue sur l'avis de la CNIL, Revue Dalloz IP/IT, 2020, n°5 p. 280.

N. Metallinos, Quel encadrement pour les outils numériques du dépistage Covid-19 ?, *Communication, Commerce électronique*, n° 7-8 2020, n°59.

L. Pailler, StopCovid: la santé publique aux prix de nos libertés ? Point de vue, *Recueil Dalloz* 2020, p. 935.

2.2.3. *Germany*

Tracing application

Name

"Cor*ona-Warn*".

Launch date

The Federal Government and the Federal Commissioner for Data Protection and Freedom of Information officially announced the launch of the "Corona-Warn-App" on June 16, 2020.

Plans concerning the use of digital technologies in the fight against the pandemic date back at least to early March 2020. At that time, the Minister of Health published a bill aimed at allowing the processing of traffic data held by telecommunication providers to identify clusters and persons at-risk. However, the proposal was met with strong criticism for the risks of surveillance[69].

In April 2020, the public health institution the Robert Koch Institute (RKI) developed a first Covid-19 application, the "Corona Datenspende App", which was made immediately available to German citizens for download[70]. The design and rationale of this app were completely different from the later Corona-Warn. It was not conceived of as a proximity tracing application. The main purpose of the "Corona Datenspende App" was to make a specific set of clinical and socio-demographic data available to the RKI for epidemiological research. The app made it possible for users, on a strictly voluntary basis, to share with the Robert Koch Institute personal data recorded by wearable devices specifically associated with the app, such as a smartwatch or fitness tracker, and concerning health conditions (such

[69] T. Voland – M. Kümmel, *Mit Technologie gegen das Virus Rechtliche Fragen im Zusammenhang mit der Corona-Warn-App,* in *PharmR,* 2021, 189.
[70] J. Kühling – R. Schildbach, *Corona-Apps. Daten- und Grundrechtsschutz in Krisenzeiten, NJW,* 2020, 1545, at 1546.

as pulse, heart rate variability, blood pressure, temperature and weight) and activities (sleeping hours and quality, sport activity, etc.)[71]. Such data could be analysed in order to detect possible symptoms of infection, identify local clusters, and understand the patterns of pandemic diffusion[72]. The app established an interesting model of data altruism for the sake of the fight against the pandemic and was downloaded in the first weeks by more than 500.000 citizens. From the perspective of data protection, it processed only anonymised data and relied on the legal basis of the data subject's free and specific consent (which could be tailored to individual preferences once the app was installed) according to arts. 6.1.*a* and 9.2.*a* GDPR[73].

The spread of the pandemic and the examples of other apps adopted by foreign countries pushed the Federal Government to start considering the introduction of a tracing application. Initial plans were oriented towards the centralised model advocated by the European PEPP-PT consortium, of which the Fraunhofer HHI research institute was one of the most prominent members. However, this plan encountered the opposition of several scientists, who feared the risk of "unprecedented surveillance", and above all collided with the stance taken by major providers, such as Apple [74].

At the end of April, the Federal Government changed course over the model of tracing application to be followed. In particular, on April 26, 2020, Chancellery Minister Helge Braun (Special Tasks) and Minister Jens Spahn (Health) jointly announced that Germany had abandoned the centralised protocol in favour of the decentralised DP-3T model.

Behind such a sudden reversal of Germany's policy was, among other factors, the Google and Apple joint initiative and Apple's refusal to unlock the iPhone's operating system to any app exchanging data with the government. This would have almost certainly meant failure of the experiment, given the impossibility to let the app work in the background on iPhones. As a result, the Government assigned the companies SAP and Deutsche Telekom the task to develop a solution pursuant to the decentralised model and based on the application programming interface of Google and Apple. After about 50 days, and a transparent development process (the source

[71] See https://corona-datenspende.de (last visited May 1, 2021).
[72] B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung*, Beck, Munich, 3rd ed. 2021, *Einleitung*, par. 45.
[73] *Ibidem.*
[74] D. Busvine – A. Rinke, Germany flips to Apple-Google approach on smartphone contact tracing, Reuters, April 26, 2020, available at https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN22807J (last visited May 1, 2021).

code was published step by step on the open repository GitHub)[75] the app was available to download on Google Play and Apple Store. The process was closely monitored by the Federal Office for Information Security, with respect to data security issues, and by the Federal Commissioner for Data Protection and Freedom of Information (BfDi), which confirmed the app's compliance with data protection principles.

Modifications

As is the case with many other apps, and tracing applications in particular, the initial version of the app has been continuously reworked to eliminate defects and add improvements.

With version 1.13, users have been given the possibility to voluntarily donate data to help improve the app and fill out a scientific survey conducted by the Robert Koch Institute. According to the official description available on the Corona-Warn website,

> if users activate the data donation, the app transmits whether there is a red or a green tile, i.e. a low or increased risk. This allows the RKI's experts to see how many people were exposed to which risk in each case. Users also have the option of specifying their state, county, and age so that the experts can make a possible connection between warnings and local incidence rates. They can also see, for example, whether there are more red or green tiles in certain age groups than in others. The voluntarily provided data can help experts evaluate the effectiveness of the app and further improve it[76].

SAP and Deutsche Telekom have recently released version 2.0 of the Corona-Warn-App, which adds a new function. With the update, the app has a new event registration feature. This allows users to check in via a QR code at stores, restaurants, events (like concerts or exhibitions) or private meetings. The check-in is saved on the personal device and automatically deleted after two weeks. The purpose of this new function is to immediately detect potential clusters and break dangerous chains of infection via the app's alerts.

[75] Source code is available at https://github.com/corona-warn-app (last visited May 1, 2021).
[76] https://www.coronawarn.app/en/blog/2021-03-04-corona-warn-app-version-1-13/ (last visited May 1, 2021).

Technical characteristics and development

The German application is an open-source proximity tracing application[77]. It follows the Google/Apple decentralised exposure notification framework. It makes use of Bluetooth Low Energy technology and keeps proximity contact data within the local device, without transferring them to the backend server. It collects and stores only proximity contact data which fit with the criteria established by the Robert Koch Institute and does not resort to GPS technologies and related location data.

Corona-Warn has two main functions.

The first is the exposure notification function. In particular, the app shows each user her risk status depending on contacts recorded by the system and the specific characteristics of the encounters with persons that have tested positive to the virus. There are three types of status information: a) low risk (no encounter with infected persons, such encounters not exceeding the defined threshold value); b) increased risk (the person encountered at least one person in the last 14 days who has been diagnosed with COVID-19); c) unknown risk (the app has not been activated for long enough by the person, then no risk of infection can be calculated).

The app has also another important (optional) function, namely it enables users to retrieve Covid-19 test results electronically. If the testing laboratory supports the electronic process, tested users can use the QR code they received during the test to retrieve their results on the app.

Following the software update published on 19 October 2020, the app has become interoperable with contact tracing apps adopted from other European countries, among them Ireland, Belgium, Austria, Croatia and Italy[78].

It can be downloaded by anyone aged 16 or older and is available in six languages: German, English, Romanian, Bulgarian, Polish and Turkish.

It was developed by the German software corporation SAP and the Deutsche Telekom subsidiary T-Systems on the basis of a project commissioned by the German Federal Government. Advice and support were also provided by the Fraunhofer-Gesellschaft and the Helmholtz Center for Information Security (CISPA). As regards the data protection and IT security aspects, the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information (BfDi) were also involved in the design and supervision of the technological infrastructure[79]. The backend of the app is operated by Deutsche Telekom.

[77]

[78] See https://www.coronawarn.app/de/faq/#interoperability_countries (last visited May 1, 2021).

[79] See https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-

Health entities related to the application

The public entity more specifically involved in the supervision of the app is the "Robert Koch Institute", the government's central scientific institution in the field of biomedicine. The Institute has a major role in the Corona-Warn-App. On the one hand it provides specialist expertise for the development of the app, its improvement and the adjustment of epidemiological criteria used by the algorithm to identify contact risk. On the other hand, as data controller it is also responsible for carefully checking the requirements for data protection and data security.

Legal Framework

Supranational legal framework

Art. 6.1.*a* and art. 9.2.*a* EU Regulation 2016/679.

National legal framework

No existing specific legislation authorizing the processing of proximity contacts data

Political discussion

Two major issues have been debated in Germany. The first is the alternative between a centralised and a de-centralised protocol for the tracing application (*supra,* par. 1.3.1.). The second is the legal basis of data processing. Whereas the Federal Government denied the need for a specific statutory basis, various associations, privacy activists and the German Bar Association voiced some concerns over the absence of a defined and transparent legislative framework[80]. The most contentious issue was represented by the lack of specific legislation authorizing the processing of proximity contacts data on a mass scale[81]. The same stance was taken by some political parties. The Green Party (Bündnis 90 Die Grünen), in particular, voiced concern over the possible discriminatory uses of the app within private and work relationships. To this end, it presented a Bill at the Bundestag aimed at "securing the voluntary use and earmarking of mobile electronic appli-

app-englisch/corona-warn-app-faq-1758636 (last visited May 1, 2021).

[80] Corona-Warn-App startet mit Lob und Diskussion um gesetzliche Grundlage, Becklink 2016602.

[81] M. Blaeser – C. dos Santos Firnhaber, Tracking & Tracing: Fluch oder Segen der Digitalisierung des Gesundheitsmanagements? Corona-Warn-App, RDG, 2020, 182.

cations for the tracking of infection risks" (*Entwurf eines Gesetzes zur zivil-, arbeits- und dienstrechtlichen Sicherung der Freiwilligkeit der Nutzung und zur Zweckbindung mobiler elektronischer Anwendungen zur Nachverfolgung von Infektionsrisiken*) [82].

Opinion of national committees

The Federal Commissioner for Data Protection and Freedom of Information (BfDi) supervised the development of the app since the very beginning and gave specific advice to make it compatible with European and German data protection law. This is reported also in its official *Tätigkeichtsbericht 2020* transmitted to Parliament[83]. Recently, the Federal Commissioner for Data Protection and Freedom of Information approved version 2.0. of the app, with the related new event tracking function (see above, 1.4) [84].

National legal framework

It is worth recalling than in Germany data protection is considered a fundamental right, at least since the first *Microcensus* decision of the Federal Constitutional Tribunal. As a result, any interference with such right requires a legal basis, must pursue legitimate aims and should be proportional to the goals pursued. More specifically, art. 6 and art. 9 of EU Regulation 2016/679 make data processing conditional on one of the listed legal bases. In the case of a tracing application, the two alternative legal bases that are conceivable are the processing necessary for the performance of a task carried out in the public interest (art. 6.1.*e*; art. 9.2.*g*) and the data subject's consent (art. 6.1.*a*; art. 9.2.*a*). It goes without saying that the fight against the pandemic and the protection of the health of persons-at-risk, which are two of the main goals of any contact tracing application, count as purposes of relevant public interest[85]. Therefore, in theory they could be resorted to as a proper legal basis for data processing. However, art. 6.3 of the EU Regulation 2016/679 makes it clear that processing for goals of

[82] https://www.gruene-bundestag.de/themen/datenschutz/datenschutzkonforme-pandemiebekaempfung (last visited May 1, 2021).

[83] The report can be downloaded free of charge at the address: https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/29TB_20.html?nn=5217212 (last visited May 1, 2021).

[84] See https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2021/08_Möglichkeiten-Corona-Warn-App-nutzen.html;jsessionid=94622263993FCEEF6A1CFC11353FC8C2.2_cid507 (last visited May 1, 2021).

[85] B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung, Einleitung,* par. 49.

public interest should also be assisted by a specific normative basis under European or national law. As a matter of fact, Germany has not legislated on the issue, and the existing normative schemes, such as the general law on infectious diseases (*Infektionsschutzgesetz*), do not specifically authorise the massive collection of personal data related to risk exposure by means of digital technologies.

As a result, the only available legal basis is represented by the consent of the data subject. Indeed, the Federal Government backed this solution, which is considered more transparent and in line with the decentralised architecture of the app. More specifically, the voluntariness of data processing should be ensured at a double level: *a*) the free decision to download and use the application; *b*) the free decision to contact health authorities in the event of a risk exposure alert. However, this solution has been met with criticism by several legal scholars and privacy activists[86]. The main arguments raised against the lack of a specific legislative basis are the following:

a) absence of a clear definition of the limits – in terms of scope and duration – of data processing;

b) social pressure weakening the character of a truly "free" consent to data processing[87].

Whereas the latter argument echoes a general theme in the European law of data protection, which hinges on the idea of the inadequacy of the American model of notice and consent, the former one is specific to the situation at hand. Indeed, tracing apps have been conceived as an emergency instrument, which should be abandoned as soon as the pandemic is over. However, it is feared by many that in the absence of a clear legislative provision defining the exact duration of data processing, this may be extended much longer than needed, with the obvious risks in terms of mass surveillance. Furthermore, the lack of a legal basis has another, more subtle implication, concerning the possible compulsory use of the tracing app in private relationships.

Whereas in other European countries, such as Italy, it is expressly provided that by refusing to download or use the app no individual shall suffer any prejudice of any kind[88], in Germany such a principle is not explicitly enshrined in any statutory provision. As a result, the introduction of the Corona-Warn-

[86] See generally D. Samardzic – T. Becker, *Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW*, 2020, 646.
[87] J. Kühling – R. Schildbach, *Corona-Apps. Daten- und Grundrechtsschutz in Krisenzeiten,* at 1549.
[88] See art. 6.4 of the Italian legislative decree n. 28/2020 of April 30, 2020.

App immediately sparked a debate concerning the possibility of making it compulsory in private-law relationships or as a prerequisite to access certain places or services. Whereas within G2C (government to citizens) relationships this would clearly not be acceptable, as it would deprive the consent to data processing of its free and voluntary character, the situation is less clear in the private sector.

The issue is particularly controversial as regards labour relationships. Indeed, it has been suggested that it is within the duties of the employer to protect the physical integrity of employees, and therefore the use of the app might be mandated as a specific protective device[89]. Also, it cannot be seen that several firms developed or obtained under license private apps specifically tailored to the needs of a workplace, among them distance checking, rapid exchange of information and, of course, contact tracing[90]. Differently from Italy, in Germany there seems to be no preclusion to use contact tracing applications within private relationships and in the absence of a legislative basis[91]. In any event, even if the compulsory use of an app could be justified on the basis of the employer's directive power[92], it should be specifically demonstrated that the consent to data processing is compliant with the requirements set by art. 4 and 7 GDPR, and namely that it is "free, specific and informed" [93]. To this end, it would be advisable to discuss the issue with the trade unions and agree on safeguards and limits of personal data processing[94].

Critical appraisal

As discussed in the previous paragraph, the German Corona-Warn-App is wanting of a specific statutory basis and *encadrement*. However, the exposure notification system, in spite of the anonymous character of proximity data, at various stages implies the processing of personal data: *a*) to download the app, one has to register in the app store, and this may

[89] C. Sander – S. Hilberg – S. Bings, *Arbeitsschutzrechtliche Fürsorge- und Schutzpflichten sowie Haftungsrisiken für Arbeitgeber im Zusammenhang mit COVID-19, COVur,* 2020, 347.
[90] See for instance the "Comfy-App" developed by Siemens: https://new.siemens.com/ch/de/unternehmen/news/sicher-im-buero-dank-comfy.html (last visited May 1, 2021).
[91] B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung, Einleitung,* par. 51.
[92] On this issue see C. Sander – S. Hilberg – S. Bings, *Arbeitsschutzrechtliche Fürsorge- und Schutzpflichten sowie Haftungsrisiken für Arbeitgeber im Zusammenhang mit COVID-19,* at 352-353.
[93] B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung, Einleitung,* par. 52.
[94] B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung, Einleitung,* par. 52.

be a source of personal data gathered by Google or Apple; *b*) the exchange of information between the user and the Robert Koch Institute in case of a positive test result (upload of temporary keys) implies the display of the user's IP number, and this is considered personal data; *c*) health data may be implicit in the proximity identifiers (contact data) stored in each device and may be processed at the moment of the upload and sharing of a positive test result. Consequently, the relevant actors have to abide by the EU and German data protection law.

The *data controller* is the Robert Koch Institute, the Federal Government's central institution in charge of most aspects of infectious diseases' prevention and surveillance. As already clarified above, the RKI supervised the development of the app and is responsible for its compliance with data protection law.

The *data processors*, on behalf of RKI, are T-Systems International Gmbh and SAP Deutschland SE & Co. KG.

Prior to the launch of the app, the RKI carried out a data protection impact assessment according to art. 35 GDPR. This document is freely accessible on the web and disclosed all technical details of the app[95]. It makes clear that the legal basis of the processing of user's personal data, according to arts. 6 and 9 GDPR, is constituted by the data subject's consent[96]. It is therefore critical to identify the information made available to the user prior to downloading and the procedures adopted for the expression of a declaration of consent.

As soon as the app is downloaded and opened, a detailed privacy notice is shown[97]. It explains the most relevant features of the app. Namely, it makes clear that the use of the app is absolutely voluntary; the consent necessary to enable the exposure logging system, the transmission of a test result via app, as a well as to share test results may be withdrawn at any time; the age requirement is set at 16 years; the period of conservation of contact data (14 or 21 days depending on the test results) and anonymised test results; the geographical scope of data processing and the absence of any transfer outside of the EU.

As regards the declaration of consent, this is divided into three main stages, which are conceived of as mutually independent.

First, consent of the individual is needed for the gathering of proximity

[95] https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf (last visited May 1, 2021).
[96] *Ibid.,* par. 7.2.2.2, at 95.
[97] A sample is available at this address: https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf (last visited May 1, 2021).

contact data (core functionality of the app). Therefore, for the proper working of the app, the data subject should express his or her free and informed consent by tapping on the "Enable Exposure Logging" button the first time the app is opened. As said, the age requirement is set at 16 years (n. 4 of the privacy notice).

A separate consent is needed with regard to data processing performed for registering a COVID test in the app by scanning the QR code provided by doctors and test facilities. If this authorization is given, test results will be shown directly in the app.

Finally, consent is also needed for sharing test results in order to warn other users. It is important to note that the refusal to authorise data processing related to test registering and sharing does not impede the proper functioning of the core functionalities of the app related to the risk exposure notification.

As regards the data protection rights granted by arts. 15-21 GDPR, the data subject may enforce them vis-à-vis the data controller; the competent supervisory authority is the Federal Data Protection Authority.

Social acceptance and efficacy

Germany is the European country with the highest rate in terms of downloads of a tracing application. According to the author of this report, one of the reasons why the Corona-Warn-App has become so popular among Germans is that it was strongly backed by the Government at its highest levels. Not only the Minister of Health, but also the Chancellor Merkel spent much effort in convincing the citizenry about the security and usefulness of the application as one of the most important tools available to fight the pandemic[98]. Also, it should be underlined that the app is very much "user friendly" and that the official website is full of detailed and clear information concerning the technical features and the legal framework of the app, as well as constantly updated figures and statistics concerning its use.

Number of users[99]

As of April 30, 2021, 27.4 Million citizens had downloaded Corona-Warn. This amounts to 33% of the German population.

For the sake of comparison, on August 11, 2020, 16,9 Million citizens had downloaded the app (20,36% of the German population).

[98] See Chancellor Merkel's podcast available at https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch (last visited May 1, 2020).

[99] Official figures available at https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/WarnApp_KennzahlenTab.html.

Number of cases reported

As of April 30, 2021 708,435 calls to the hotline had been recorded and 424,067 positive test results had been uploaded into the system. Compared to the 3,381,597 total number of infected persons since the pandemic outbreak, this amounts to 12.54 % (the figure is striking compared to the Italian percentage of 0.45 %).

For the sake of comparison, on August 11, 2020 more than 206,000 calls to the hotline had been recorded; 1320 verification codes for sharing of test results had been issued.

Bibliographical references

Useful links:

https://github.com/corona-warn-app

https://www.coronawarn.app/en/

https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch

Official figures and statistics:
https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/WarnApp_KennzahlenTab.html

Articles:

M. Blaeser – C. dos Santos Firnhaber, *Tracking & Tracing: Fluch oder Segen der Digitalisierung des Gesundheitsmanagements? Corona-Warn-App*, *RDG*, 2020, 182

J. Kühling – R. Schildbach, *Corona-Apps. Daten- und Grundrechtsschutz in Krisenzeiten, NJW,* 2020, 1545

B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung*, Beck, Munich, 3rd ed. 2021, *Einleitung,* par. 45

D. Samardzic – T. Becker, *Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW*, 2020, 646

C. Sander – S. Hilberg – S. Bings, *Arbeitsschutzrechtliche Fürsorge- und Schutzpflichten sowie Haftungsrisiken für Arbeitgeber im Zusammenhang mit COVID-19, COVur,* 2020, 347

T. Voland – M. Kümmel, *Mit Technologie gegen das Virus Rechtliche Fragen im Zusammenhang mit der Corona-Warn-App,* in *PharmR,* 2021, 189

2.2.4. *Italy*

Tracing application

Name

Immuni

Technical characteristics and development

The Italian application is an open-source proximity tracing application realised by the Special Commissioner for the COVID-19 emergency (on behalf of the Presidency of the Council of Ministers), in collaboration with the Ministry of Health and the Ministry for Technological Innovation and Digitalisation. The software, graphics, text and documentation were originally developed by Bending Spoons S.p.A., which granted the Italian government a perpetual and irrevocable license. The source code was released under a GNU Affero General Public License version 3. Immuni is managed by the public company Sogei S.p.A. and makes use of public infrastructures located within the national borders.

Immuni features an exposure notification system, based on Bluetooth Low Energy technology, and follows the Google/Apple framework. It keeps track of close contact instances (less than 2 meters, for at least 15 minutes) and alerts persons at-risk of carrying the virus in real time. Immuni is a decentralised tracing app, as it keeps proximity contact data within the local device, without transferring them to the backend server. It collects and stores only anonymous contact data and no geolocation data of any kind, including GPS data.

Immuni is available to download to all users from age 14. Once a person tests positive to the Covid-19 virus, she may upload her data, with the effect that the app will automatically notify people who have been in close contact any time from 2 days before the symptoms began (or the test was taken) and up to a maximum of 14 days after. To this end, three alternative procedures are currently available: 1) the infected person asks for the support of the healthcare professional who communicated the result of the Covid-19 test; 2) she contacts a call centre operator, providing the CUN (*Codice Univoco*

Nazionale) code associated to the test results; 3) she uploads the CUN code directly in the app, using a dedicated function.

Immuni is exclusively a contact tracing application and does not possess other functionalities, such as symptom checking or telemedicine.

It is interoperable with several European apps, such as those adopted in Spain, Germany, Austria, Croatia, Slovenia, Belgium, Netherlands[100].

Launch date

Immuni was first piloted in the regions of Marche, Liguria, Puglia, and Abruzzo starting on June 8, 2020. It was launched nationwide on June 15, 2020.

History and launch

The Italian Government started considering data-driven strategies at the very peak of the emergency, in March 2020, when the sanitary system of Northern Italy was near collapse, and general lockdown measures were first ordered. The Special Commissioner for the COVID-19 emergency (on behalf of the Presidency of the Council of Ministers) opened a streamlined call for contributions on March 23, 2020 (with the deadline of March 26, 2020), aimed at promoting the best solutions in the field of digital contact tracing[101]. 318 proposals were received. On March 31 2020, the Ministry of Innovation appointed a task force of 73 experts of various disciplines (epidemiologists, engineers, lawyers, experts of data protection and cybersecurity, etc.) with the goal of supporting the Ministry in performing the selection.

The app "Immuni", developed by Bending Spoons S.p.A., was eventually selected and presented on April 10 to Prime Minister Giuseppe Conte. On April 16, the Commissioner for the Covid Emergency signed a contract with the developers of Immuni and completed the public procurement. However, the app was made available for download only in June, and the reason for the delay was mainly related to the fact that in the meantime Apple and Google announced their common policy concerning the standardised interface. As happened also in Germany, the synergy of

[100] For further details, see https://www.immuni.italia.it/dashboard.html (last visited April 30, 2020).

[101] C. Colapietro – A. Iannuzzi, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in Dirittifondamentali.it, n. 2/2020, 772; G. Della Morte, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, in *Diritti umani dir. int.*, 2020, 303, p. 305.

various factors – among them the support obtained by cybersecurity and privacy experts, the technical advantage of using the app in the background, the increased interoperability – played in favour of the abandonment of the centralised model, which was originally favoured by the government. As a result, the developers of Immuni spent time in adapting to the decentralised model, namely in making it compatible with the Google/Apple API. As a result, the app could not be offered for download before the middle of June. As in Germany, the source code was published on GitHub[102], and the whole process was closely supervised by the Data Protection Authority.

Modifications

The major modification is related to the mechanism adopted for the notification of a confirmed case of Covid-19. Originally, the intervention of the healthcare professional who communicated the result of the Covid-19 test was necessary to unlock the system. This however was a source of major delays and difficulties. Starting from December 21, 2020 the user was also given the option to contact a call centre and simply communicate by phone the CUN code associated to the test result. Since April 2021, version 2.4.0 of the app for Android and iOS grants the user the possibility to directly upload this code on the app[103].

Health entities related to the application

The Ministry of Health is the *data controller* with regard to the processing of personal data involved in the workings of the exposure notification system. In this capacity, the Ministry of Health filed for the first time on May 28, 2020 the impact assessment on the basis of art. 35 GDPR (the document was most recently updated on February 10, 2021) and was authorised by the Italian Data Protection Authority to start processing on June 1, 2020[104].

Data processors are the corporation Sogei S.p.A. and the Ministry of the Economy and Finance, which run the backend server.

[102] https://github.com/immuni-app.

[103] See https://www.ansa.it/sito/notizie/tecnologia/hitech/2021/04/09/covid-app-immuni-utenti-possono-caricare-codice-positivita_bc711256-5475-436f-b287-2174afa6290b.html (last visited April 30, 2021).

[104] On this G. Della Morte, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, p. 321.

Legal Framework

Supranational legal framework

The most relevant text is EU Regulation 2016/679 on data protection (art. 6.1.e); art. 9.2.g). See also Directive 2002/58/EC.

As regards resolutions and guidelines, see European Parliament, *Resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP))*; EU Commission, *Recommendation 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*, 8-4-2020, C (2020/2296 final,); EU Commission, *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection,* 17-4-2020, 2020/C 124 I/01; EDPB, *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,* 21-4-2020; *Guidance n. 3/2020 on the processing of health data for the purpose of scientific research in the context of the Covid-19 outbreak.*

Opinion of national committees

The Italian Data Protection Authority has been involved since the beginning in the process of defining an appropriate legal framework for the proximity tracing application.

On April 8, 2020, Antonello Soro, President of the Authority, was heard by the Italian deputies and senators in respect of the project of the introduction of a proximity tracing application.

On April 29, 2020, the Authority expressed its consent to the draft legislation authorizing the introduction of the app.

On June 1, 2020, it authorised the Italian Ministry of Health to start the processing of contact data.

Lastly, on February 25, 2021, the Authority gave the green light to a modification in the technical design of the app (as explained in a new impact assessment released by the Ministry of Health on February 10, 2021) by means of which a person tested positive may autonomously unlock the device and activate the notification function without the direct involvement of health authorities.

National legal framework

Since the declaration of the state of emergency (which started on January 31, 2020), the Italian legal system was interested by a massive flow of regulation aimed at preventing the spread of the pandemic and providing economic relief for sectors of the economy most affected by the crisis. An important part of this regulation concerned the relationship between the protection of health and data privacy[105].

The first important provisions were introduced by an emergency order issued by the chief officer of the civil protection department on February 3, 2020. This order, submitted for prior consultation to the Data Protection Authority[106], was later transposed, without substantial modifications, into art. 14 of the law-decree of March 14, 2020. Art. 5 of the order authorised the collection, processing and sharing of health-related data by the civil protection department, as well as by the National Institute of Health and other selected public authorities for purposes of countering the pandemic. Furthermore, it relaxed the information duties set by data protection law, by expressly allowing simplified and oral privacy notices for processing related to the management of the sanitary crisis. When the first plans concerning the introduction of a contact tracing app were disclosed, an important issue was immediately raised, concerning the legal basis of the processing of contact data and other health related data[107]. Whereas it was suggested by some scholars that consent of the individual could be considered an adequate legal basis according to arts. 6 and 9 GDPR, the Data Protection Authority suggested that the most appropriate basis was that of processing data for the performance of tasks of relevant public interest under art. 6, al. 1, let. *e*), and art. 9, al. 2, under *g)* GDPR.

The processing for public interest, however, requires under art. 6, al. 3, let. *b* GDPR and under arts. 2 *ter* and 2 *sexies* Italian Data Protection Code, a legal provision defining the conditions and limits of interference with the personal sphere. It was discussed whether art. 14 of the law decree 14/2020

[105] G. Resta, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, in *Giustizia Civile.com*, *Editoriale,* May 5, 2020.

[106] DPA, *Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili,* provv. 2-2-2020, n. 15 (doc web n. 9265883).

[107] See generally D. Poletti, *Commento all'art. 6 GDPR,* in R. D'Orazio – G. Finocchiaro – O. Pollicino - G. Resta, *Il nuovo sistema della protezione dei dati personali, Le fonti del diritto italiano*, Milan, Giuffré, in press.

could be sufficient to this purpose. Some scholars argued that it could[108], but the opposite opinion prevailed, as the decree did not expressly authorise a tool of digital mass surveillance such as the tracing app[109]. Therefore, the Government opted for the introduction of a specific legislative scheme, with the aim of clarifying the basic rules and principles to be complied with by any tracing application. It closely followed the guidelines issued by the European Data Protection Board (*Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,* 21-4-2020).

Art. 6 of legislative decree n. 28/2020 of April 30, 2020 (later modified by art. 2, let. *a* and *b* of d.l. 7-10-2020, n. 125) specifically deals with the planned "exposure notification system" [110]. The cornerstone of the whole system is represented by its voluntary character. Not only the law provides, consistently with the EDPB *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak* (par. 1.8), that there is no obligation whatsoever to download or use the tracing app. It is also clearly stated, in art. 6.4, that the refusal to download or to use the app shall not produce any "prejudicial effect" on the individual and shall not impact on the right to equal treatment.

The main function of the system is contact tracing. It is noteworthy, however, that according to art. 6.3 of the decree 28/2020, data may be reused anonymously or in aggregate form for public health purposes, prophylaxis, statistical purposes or scientific research.

The system is entirely managed by public entities (Ministry of Health and public corporations) and pays great attention to the value of transparency, as it implies that the source code should be left open and publicly disclosed. The app will be in operation until December 31, 2021 (according to art. 2, d.l. 7-10-2020, n. 125).

According to art. 2, d.l. 7-10-2020, n. 125, the interoperability with similar apps developed by other EU member states is allowed.

[108] F.P. Micozzi, *Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito,* in *BioLaw Journal,* 2020, p. 6.
[109] C. Colapietro – A. Iannuzzi, *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali,* p. 782.
[110] For a detailed analysis see D. Poletti, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza,* in *Persona e mercato,* n. 2/2020, p. 31.

Data protection issues

According to art. 6 law decree 28/2020, the data controller is the Ministry of Health. This is the public authority in charge of the data protection impact assessment (art. 35 GDPR), which has to be constantly updated and submitted for prior consultation (under art. 36 GDPR) to the Italian Data Protection Authority. In its capacity as data controller, the Ministry of Health is responsible for the adoption of the technical measures aimed at ensuring an appropriate level of security, in consideration of the risks for the fundamental rights and interests involved in the processing.

Art. 6 expressly provides, furthermore, that the Ministry of Health:

- shall make available to all users, prior to download, a privacy notice containing all information required by the GDPR and related to the purposes and conditions of the processing, as well as to the period of conservation of personal data;
- shall ensure compliance with the privacy by design principle, limiting the collection and processing only to the data strictly necessary for the proper working of the risk exposure notification system;
- shall guarantee that the app collects only anonymous (or at least pseudonimised) proximity contact data, with the exclusion of any location data;
- shall limit the processing to the period strictly necessary for the achievement of the purposes of risk exposure notification (*data retention* period);
- shall make the exercise of data protection rights (arts. 15-22 GDPR) possible also in a simplified manner.

Art. 6, al. 3, allows for a slight deviation from the rigid logic of the DP-3T protocol. On the one hand it confirms that proximity contact data shall be processed only for the purposes of risk exposure notification; on the other hand, it authorises the processing of "aggregated data or anonymous data" for purposes of public health, statistics or scientific research".

It is also provided that the use of the app and the processing of resulting data shall be terminated once the state of emergency is over, and in any event not later than December 31, 2021 (art. 2, d.l. 7-10-2020, n. 125).

As regards the technical infrastructure, it is specified that the backend platform shall be owned by the State and that data shall be stored in Italy and will not be transferred outside of national borders.

Social acceptance and efficacy

It cannot be said that the app *Immuni* has been a complete failure. However, it certainly cannot be described as a success story.

The figures concerning the download rate of the app are quite disappointing. In particular in the first months of use – which were the most critical both for the novelty of the app and for the impact of the pandemic – various difficulties were reported. Some of them arose out of the interaction between the digital tracing system and the traditional health surveillance system[111]. One of the main issues was the limited availability of molecular testing: Italians had to wait a long time until they could get tested and obtain the result, and this weakened the very utility of a contact tracing application (as the notification would have been sent too late to the persons-at-risk). Secondly, it has been reported that the procedure to notify the positive result of a test was too cumbersome, as health authorities had insufficient information and digital skills (the option to contact a call centre was added only at the end of 2020, as detailed above, see 1.4.) and therefore were not always able (or willing?) to upload the code[112]. Indeed, the Italian Government had to introduce a specific provision in the decree of the President of Council of Ministers of December 3, 2020 (art. 5, let. *b,* d.p.c.m. 3-12-2020), obliging the Department of Prevention of local health authorities to upload the code and start the notification process in case of positive result of the molecular test[113]. Thirdly, persons possessing older smartphones experienced various technical difficulties with the installation and/or functioning of the app[114].

The not so brilliant results of the app can be explained on the basis of various factors[115].

Among them are the following: *a*) lack of a coherent and effective communication strategy by the Government; *b*) the launch of the app only once the peak of the first wave was long over; *c*) the existence of other Covid-19 apps in operation at regional level, leading to a certain confusion among the public[116]; *d)* ageing population; *e*) insufficient digital skills.

[111] D. Poletti, *Contact tracing e app immuni: atto secondo,* in *Persona e mercato,* 2021, 92, p. 97.
[112] https://www.huffingtonpost.it/entry/immuni-i-punti-dolenti-la-giungla-del-meccanismo-offline_it_5f8460bec5b6e6d033a59420 ((last visited April 30, 2021).
[113] D. Poletti, Contact tracing e app immuni: atto secondo, p. 94.
[114] https://www.adnkronos.com/app-immuni-non-funziona-codacons-da-utenti-segnalazioni-disservizi-e-problemi_6UwIYio4Ole2Dt91OcdfU2 (last visited April 30, 2021).
[115] See D. Poletti, Contact tracing e app immuni: atto secondo, 97-98; G. Della Morte, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, p. 331.
[116] Some examples are: "AllertaLom" in Lombardia (https://www.regione.lombardia.it/wps/portal/istituzionale/HP/DettaglioRedazionale/servizi-e-informazioni/cittadi-

From the latter point of view, it may be useful to point out that the Regions scoring the lowest rates of download are Campania, Calabria and Sicilia, all located in the South, some of the poorest parts of the country and with the worst scores in terms of unemployment and education (see the graph reproduced below).

Number of users[117]

As of April 30, 2021, 10.443.641 persons (17,30% of the Italian population) had downloaded the application. However, this number is of a very limited value and risks being misleading, since it does not differentiate the number of *active users* of the application[118]. It is well known, indeed, that many people who downloaded the application uninstalled it after a few days, or simply did not activate it (for lack of trust in the system, fear of being quarantined just after an exposure notification or problems with the battery of the smartphone).

It is worth noting, however, that the number of downloads surged in the second and the third waves of the pandemic. Indeed, on August 9, 2020, only 4,6 million downloads had been recorded (less than 8% of the population), and this low number is striking in comparison with the current figures.

It also useful to note that the distribution of the download rate is not homogenous within the whole territory of Italy. As shown by the graphs available at the official site of Immuni (https://www.immuni.italia.it/dashboard.html), the Southern Regions tend to have the lowest rates, whereas those of the Centre (at least some of them) and Northern Italy fare much better.

Number of cases reported

As of April 30, 2021 and since the launch of Immuni, 17.858 persons tested positive have unlocked their smartphone and sent the notification to the system. This is quite a low number, as it represents a mere 0.45% of the

ni/salute-e-prevenzione/coronavirus/app-coronavirus), "SardegnaSicura" in Sardegna (https://play.google.com/store/apps/details?id=it.regione.sardegna.autorizzazioni-covid19&hl=it&gl=US), and "LazioDoctor" in Lazio (https://www.salutelazio.it/lazio-doctor). They have functions different from contact-tracing. On this see G. Della Morte, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, p. 319.

[117] Official figures available at https://www.immuni.italia.it/dashboard.html.

[118] F. Cabitza, *Analizzare i dati per guardare oltre i dati dell'app*, https://www.key4biz.it/immuni-analizzare-i-dati-per-guardare-oltre-i-dati-dellapp/331930/ (Nov. 2020).

4.009.208 persons tested positive since the outbreak of the pandemic[119]. In total, 97.300 exposure notification alerts have been sent.

Bibliographical references to any official or scientific study existing

Articles

Main references on the app Immuni and its legal framework:

C. Camardi – C. Tabarrini, *Contract tracing ed emergenza sanitaria. "Ordinario" e "Straordinario" nella disciplina del diritto al controllo dei dati personali*, in *La nuova giur. civ. comm.*, 2020, 38

C. Colapietro – A. Iannuzzi, *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali,* in *Dirittifondamentali.it,* n. 2/2020, 772

G. Della Morte, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano,* in 14 *Diritti umani dir. int.,* 303 (2020)

G. Finocchiaro, *Il punto sull'app Immuni: bilanciamento tra diritti*, in *Media Laws*, 9-6-2020 (http://www.medialaws.eu/il-punto-sullapp-immuni-bilanciamento-tra-diritti/)

T. Pertot, *Immuni e tracciamento digitale: la protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, in *Le nuove leggi civ. comm.*, 2010, 1149

D. Poletti, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza,* in *Persona e mercato,* 2020, 31

D. Poletti, *Contact tracing e app immuni: atto secondo,* in *Persona e mercato,* 2021, 92

G. Resta, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, in *Giustizia Civile.com*, *Editoriale,* May 5, 2020

G. Resta, *La app 'Immuni': pregi e limiti del tracciamento digitale dei contatti,* in *Medialaws,* 15-6-2020 (http://www.medialaws.eu/la-app-immuni-pregi-e-limiti-del-tracciamento-digitale-dei-contatti/)

G. Resta, *Tracciamento digitale dei contatti*, in C. Petrini, ed., *Tutela della salute individuale e collettiva: temi etico-giuridici e opportunità per la sanità pubblica dopo COVID-19* , Rapporti ISTISAN 20/30, Istituto superiore di

[119] Official figures provided by the Department of Civil Protection/Ministry of Health, available at https://opendatadpc.maps.arcgis.com/apps/dashboards/b0c68bce2cce478eaac82fe38d4138b1 (last visited April 30, 2021).

sanità, Rome, 2020, 79-88

V. Zeno-Zencovich, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *MediaLaws* 26-5-2020 (http://www.medialaws.eu/i-limiti-delle-discussioni-sulle-app-di-tracciamento-anti-covid-e-il-futuro-della-medicina-digitale/)

Useful links and official figures

https://www.immuni.italia.it/dashboard.html

https://dati-covid.italia.it

https://www.garanteprivacy.it/temi/coronavirus

2.2.5. *Australia*

Tracing application

Name

CovidSafe

Technical characteristics and development

- Protocol and data security

The latest releases of the app use the Bluetooth Herald Protocol.

Download is voluntary. Health officials can only access app information if someone tests positive and agrees to the information in their phone being uploaded. The health officials can only use the app information to help alert those who may need to quarantine or get tested.

- Functionalities

CovidSafe is based on the Apple and Google model and is downloadable from the Android Play Store or Apple's App Store. In order to download it, the user must provide their name, their age range and their post code and mobile number.

Bluetooth technology records when two mobile phones come within 1,5 metres of each other for 15 minutes.

The Australian "CovidSafe" app is a partially centralised model in which the data collected is managed (in an encrypted form) by the federal Health Department. When the user of one of the mobile devices running the app is tested positive, the user is asked to allow the Health Department to upload the diagnostic and the set of above defined contacts on the national data repository.

Only when this permission is given, the contact data are decrypted and the third parties contacted.

Each contact event is stored on the app for 21 days and then deleted. Therefore, only those who have been in contract in that three-week period

are traced and warned.

The app is therefore partially decentralised, in the sense that contact events are held exclusively on mobile phones for 21 days and then automatically deleted. Only when authorization to contact third parties is given is the management of the system centralised.

The CovidSafe app can be uninstalled at any time. This will automatically delete all information stored on the device and stop other users from collecting the contact data.

The app further provides users with up-to-date official information and advice to help stop the spread and stay healthy. It also provides a brief summary of the latest developments of the pandemic (the latest data on new cases, total confirmed cases and deaths, as well provides a concise self-care guide on the relevant symptoms and the contact information together with push notifications of urgent information and updates.

Launch date

At the end of April, 2020 the Australian federal government issued an "Emergency Determination" which authorised the launch of the "CovidSafe" app. The app was immediately released to the public on April 26, 2020 and in a few weeks was downloaded by over 5 million handsets (Australia's population is 25 million, 3 million of which is under 10 years old). Presently official data indicates 7 million downloads.

Modifications

Like all the similar applications, the CovidSafe app also required that battery optimization modes of the mobile phone be disactivated. Subsequently the Digital Transformation Agency (DTA) has issued (February 2021) guidelines for improved battery usage. The latest Android release contains an update that conserves energy by searching for connections only when required. Further the Herald Bluetooth Protocol is aimed at ensuring an increase in Bluetooth performance while in the background leading to more encounters captured between devices; the new protocol is aimed at providing better accuracy identifying close contacts during a 15-minute window for both iOS and Android and a low battery usage – 1% to 2% per hour on average, depending on the age of the phone and its battery capacity.

Health entities related to the application

Federal Health Department and the Digital Transformation Agency

Legal Framework

Supranational legal framework
None

Political discussion report
Nothing to be reported

Opinion of national committees
There does not appear to be a specific and official recommendation by the OAIC or by the Digital Transformation Agency, although the related webpages contain lots of practical information on the most common privacy concerns (what kind of data is collected, how it is stored and how and when will it be deleted).

The general management of the pandemic – including the CovidSafe app – has been subject to the scrutiny of a parliamentary committee (see below).

National legal framework
After launching the app, the Australian government presented to Parliament a "Covid Safe Bill", which was enacted as soon as mid-May 2020. The official title of the Bill is "Privacy Amendment (Public Health Contact Information) Bill 2020". The adoption of the tracing app was open to wide and public – not only Parliamentary – debate.

- Data protection issues
The Australian government commissioned, before launching the app, a Privacy Impact Assessment (PIA) provided by a law firm. However, there was no prior assessment by the federal Privacy Commissioner.

The Covid Safe Act expressly states that violations of its provisions fall under the Privacy Act enabling individuals to bring a complaint to the Privacy Commissioner and ask for the relevant remedies. This means that the Data Protection agency is in charge of ensuring the correct implementation of the app.

In June and in December 2020 the Australian Parliament introduced a lengthy "Privacy Amendment (Public Health Contact Information) Act n. 44-2020 (in the Appendix) which amended the Privacy Act 1988. The Act introduces several serious offences relating to COVID app data and

COVIDSafe. They deal with nonpermitted collection, use or disclosure relating to COVID app data; uploading COVID app data without consent; retaining or disclosing uploaded data outside Australia; decrypting encrypted COVID app data and requiring participation in relation to COVIDSafe.

The Act also introduces specific obligations related to deletion of data and what is to happen after the COVIDSafe data period has ended.

The general privacy law is extended, in particular by ensuring that COVID app data is taken to be personal information and breaches of the Amendment are interferences with privacy, enhancing the Commissioner's role in dealing with eligible data breaches, making assessments and conducting investigations.

One must however point out that, despite such wide legislative interventions, the OAIC website does not report decisions with the outcome of complaints. It is therefore not possible to verify if there have been complaints concerning the CovidSafe app and the effectiveness of compliance procedures. One should add that the OAIC expressly states that it acts as a mediator between the data subject and the data controller and aims at finding a settlement between the parties. Only in extreme cases does it take a formal decision. The OAIC website does not record them.

The Australian OAIC (Office of the Australian Information Commissioner) has issued an information sheet on "The COVIDSafe app and my privacy rights" describing how the Privacy Act 1988 (Privacy Act) applies to the Australian Government's COVIDSafe app. One should however consider the very soft approach – if compared with EU data protection authorities – the OAIC appears to have in regard to the enforcement of the Privacy Act.

- Critical appraisal

Academic writings (Greenleaf, Kemp I & II) have immediately pointed out that apart from technological and legal issues (transparency in the technology used, individual freedom to download, data minimisation, remedies) – all very important – the main problem with tracing apps is that of trust by citizens in the storage and use of the data collected. The authors point out that "For a significant portion of the public, the federal government's track record of serial breaches of public trust in relation to privacy is an obstacle to trust in the COVIDSafe system. A new contributor to this lack of trust is the government's failures to be transparent in

relation to the COVIDSafe app." Furthermore, "[i]ndividual decisions about whether to install and run this app are best made after obtaining as much information as can reasonably be obtained and put in the balance. This should not require a binary choice between health and privacy" forcing Australians in having "to make complex choices based on limited information."

More critical, and performance based, comments have been made by the Australian Senate Committee on Covid-19 in an interim Report that was released in December 2020. According to the Report – which took into account all the various aspects related to the pandemic – "[t]he government is yet to make a compelling case for the value that the app has actually delivered. The government has spent a considerable amount of public money and adopted a very optimistic stance on the benefits of the app." The interim finding was therefore that the "$5,24 million COVIDSafe app has significantly under-delivered on the Prime Minister's promise that the app would enable an opening up of the economy in a COVID safe manner. The app was launched with significant performance issues and has only been of limited effectiveness in its primary function of contact-tracing".

Social acceptance and efficacy

Number of users

The app was released to the public on April 26, 2020 and in a few weeks was downloaded by over 5 million handsets (Australia's population is 25 million, 3 of which under 10 years old).

Number of cases reported

The official CovidSafe website [https://covidsafe.gov.au/] reports that there have been 7 million downloads and that "In one case, NSW Health used COVIDSafe App data to identify a previously unrecognised exposure date from a known venue. This resulted in the identification of an additional 544 contacts. From this group, 2 people tested positive". Apparently, there is no more statistical information on the efficacy of the app (*e.g.* number of activations), apart from what is referred to in the Senate interim report.

Bibliographical references

References to official or scientific studies

Australia – Senate – Select Committee on Covid-19 – First interim report (December 2020), https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/COVID-19/COVID19/Interim_Report

Australia – Office of the Australian Information Commissioner (OAIC), The COVIDSafe app and my privacy rights, https://www.oaic.gov.au/privacy/covid-19/the-covidsafe-app-and-my-privacy-rights/

Australia – Department of Health - Maddoks, The CovidSafe Application. Privacy Impact assessment (24 April 2020), https://www.covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf (health.gov.au)

Australia – Digital Transformation Agency (DTA), COVIDSafe includes COVID-19 restrictions & improved battery usage, https://www.COVIDSafe includes COVID-19 restrictions & improved battery usage | Digital Transformation Agency (dta.gov.au)

Articles, Comments, Reports

Australian Human Rights Institute, Comments on the Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020 (Cth) Privacy Amendment (Public Health Contact Information) Bill 2020 (exposure draft),
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3595109

Greenleaf, Kemp (I), Australia's 'COVIDSafe App': An experiment in surveillance, trust and law,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589317

Greenleaf, Kemp (II), Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3601730

Greenleaf, Australia: A Poor Model for QR Data 'Attendance Tracking'

Jonhson, Ahn, Regulating Medical Devices in the "Internet of Things", https://pursuit.unimelb.edu.au/articles/regulating-medical-devices-in-the-internet-of-things

Lodders, Paterson, Scrutinising COVIDSafe: Frameworks for Evaluating Digital Contact Tracing Technologies,

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3752582

Rae et al., Concerns and Misconceptions About the Australian Government's COVIDSafe App: Cross-Sectional Survey Study, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7644267/

Sun et al., An Empirical Assessment of Global COVID-19 Contact Tracing Applications, https://arxiv.org/pdf/2006.10933.pdf

University of Melbourne Law School, Law in the time of Covid 19, https://law.unimelb.edu.au/covid-19

2.2.6. *United Kingdom*

Tracing application

Name

NHS Covid-19 app
(in Scotland "*Test & Protect Scotland*", in Northern Ireland "*StopCovid NI*")

Technical characteristics and development

Based on the Apple and Google model downloadable from Android's Play Store or Apple's App Store. Mobile phones must have:

- Android 6.0 (released in 2015) or iOS 13.5 (released in 2020)
- Bluetooth 4.0 or higher

- Protocol and data security

As it is built on the Apple/Google model, data are held on the user's mobile phone and are released only voluntarily if and when the user either receives a positive test or is the recipient of a message informing her that she has been in the proximity of a Covid-19 infected person.

According to the NHS, "Specialists from the National Cyber Security Centre are involved to make sure it is safe and secure to use".

- Functionalities

Beyond proximity and positive test alerts, presently the app is used to inform users in a generic way on the risk level of the area they live in, on health services in their area and other up-to-date information on the pandemic. In a more specific way, users may use the app to book a test if they feel they have Convid-19 symptoms.

Data use

The majority of data collected by the Apple/Google API is always (and only) held on the app user's phone. Some metadata is held by the producer of the mobile phone. De-identified and aggregated data is held by the NHS.

Retention period

Diagnosis keys are kept for 14 days (the incubation period of the virus). The keys are retained on Department of Health and Social Care (DHSC) secure computing infrastructure for a further 14 days. The same rationale applies to any diagnosis keys received from partner health service apps. QR codes are kept for 21 days.

Launch date

Launch date

The UK, like most other European countries, started looking at COVID-19 tracing applications at the beginning of March 2020, following the example of Far East countries – such as South Korea and Singapore – which had been hit earlier by the pandemic and where, apparently, tracing apps had been successful in countering the spread of the virus.

One should note, however, that contrary to other countries – and notwithstanding the advice of the Joint Parliamentary Committee on Human Rights – the UK has not enacted any primary legislation in this field, nor is there any secondary legislation.

Originally the model was a centralised one, with data flowing into a centralised database managed by the National Health Service (NHS). Proximity was to be detected through a Bluetooth connection.

However, in April came the Google and Apple announcement that they were developing a system that would help proximity detection through Bluetooth. The two companies made it clear that the system would operate on a decentralised basis, therefore cutting out the NHS model. In those initial phases a critical issue that was raised was that a centralised system would not have been compatible with proprietary handsets such as Apple which "go to sleep" when they are not used and therefore do not activate the Bluetooth connection. Whatever the merits of the argument, it was subsequently effective in setting aside the centralised model.

In May, the UK app was tested on the Isle of Wight, with more than half of its residents downloading it.

Nevertheless, while apparently the app was being improved, on June 18 the UK Government suddenly announced that it was abandoning the centralised model and moving to a technology based on the decentralised Google/Apple model. One of the reasons was that – as in other countries – the Isle of Wight test had shown that the centralised app had failed to detect 96% of iPhone contacts[120].

Once the new app was made available, in July, other critical issues emerged. First of all, apparently, it did not work with less modern smartphones (therefore excluding many elderly and low-income individuals). Secondly, tests showed that contacts were detected only when the app was in the foreground, which is not always the case.

The NHS therefore developed a new version which also allows users to scan QR codes in order to trace movements.

Modifications

The version presently downloadable was only made available in September 2020.

There have been several further releases and updates of the app (the latest in March 2021) providing users with a wider range of notifications, the functionality of booking and cancelling hospital appointments and the possibility to have access to certain medical records uploaded by their general practitioner.

Health entities related to the application

National Health Service - UK Department of Health and Social Care (DHSC)

Legal Framework

Supranational legal framework

Although the UK is no longer a member of the EU, its data protection legislation (Data Protection ACT 2018) is an implementation of the GDPR.

Political discussion report

The Joint Committee on Human Rights set out a long list of flaws on

[120] https://www.wired.co.uk/article/nhs-tracing-app-scrapped-apple-google-uk

how the whole legal response to the pandemic was enacted and, in particular, pointed out significant legal uncertainties and unclear and/or inconsistent public communications; heavy-handed policing in the enforcement of such rules; and the lack of parliamentary scrutiny summarised as "the most draconian restrictions on civil liberties since the Second World War, seriously impinging on a range of rights albeit for the legitimate purpose of protecting public health. These extensive restrictions have received very little parliamentary time to date especially given that they represent such a significant incursion into the civil liberties of everyone in the country". These criticisms concern, indirectly, also the whole track & trace procedure.

Opinion of national committees

The UK ICO (Information Commissioner's Office), contrary to most Data Protection authorities, has not issued any formal document or decision on tracing/tracking apps. In a very short statement in April 2020 it released an obvious statement on the Apple/Google apps: "Organisations designing contact tracing apps are responsible for ensuring the app complies with data protection law where it processes personal data and the organisations are the controllers for that data", adding on its website that "[t]he ICO has been supporting businesses and government to ensure that data protection and privacy is built into these new measures from the start." This approach is confirmed by further quite generic statements all referring to possible future action: e.g., in September 2020 "We will continue to monitor the situation. We understand that organisations are trying to operate during uncertain and challenging times, and we will adjust our regulatory approach, accordingly, taking into account the context the organisations we regulate are operating in, and acknowledging the important role that people's information rights continue to have, both around privacy protections and transparency of decision making by public bodies".

National legal framework

None

- Presentation of the legal framework

As mentioned, the UK tracking and tracing app does not have a primary legislative basis, In general, one can refer to the Data Protection Act 2018, which implemented the GDPR and is still in force.

- Data protection issues

The NHS has run a "Data Protection Impact Assessment" (DPIA) published by the Department of Health and Social Care (see the list of references).

- Critical appraisal

It is necessary to point out that the UK followed the path of concentrating all decisions in Government, substantially excluding other institutions and bodies. The Joint Committee on Human Rights pointed out, already in May 2020, the lack of Parliamentary scrutiny over the various decisions of the Government, which at that time did not yet include tracing apps. To this, one can add the significant lack of guidance and supervision by the ICO.

The adoption and the results of the app have been subject to various studies published in the last year. Apart from the doubts already raised in the early days of the app development process on the efficacity of tracing apps (Chidambaram et al., June 2020), and the difficulty to balance potential benefits against implementation costs and ethical and equity concerns (Braithwaite et al., August 2020), it was soon pointed out that there was significant difficulty of accurately measuring distance between individuals (Jacob, Lawarée, November 2020), Further, the minimum threshold of population (between 50 and 60% of the population) was never reached; and among the age groups most absent were the elderly, who were the most vulnerable to the virus.

According to Privacy International (May 2020) the NSHX app at that time had no mechanism to opt-in or opt-out of third-party trackers which are included with the app; it appeared that the app would only work when operating in the foreground, particularly on iOS devices, making its efficacy questionable; and that the app was incompatible with a range of older Android devices, potentially putting the most vulnerable, such as the elderly or those on low incomes, at risk.

However, a more recent study by the Turing Institute (Briers et al., February 2021) states that by applying a sequential Bayesian inference algorithm using a continuous flow of updated data it would appear that "the app is having a positive effect on reducing the impact of the virus. We estimated that for every 1% increase in app users, the number of

infections can be reduced by 0.8% (from modelling) or 2.3% (from statistical analysis)." And that "evidence supports the need for the continued promotion, adherence, and greater adoption of the NHS COVID-19 app (and other similar contact tracing apps around the world), to work alongside other non-pharmaceutical interventions, in order to help control the virus".

This opinion is countered by the House of Commons Public Accounts Committee which in a March 2021 Report severely criticised the "Test and Trace" system, of which the "NHS Covid-19" application is a part. According to the Report, the NHS Test and Trace service in England failed to deliver its central promise to avoid a second national lockdown and there is no clear evidence its "unimaginable" costs have been justified. In early February 2021 it was still employing around 2500 consultants at an average daily rate of £ 1000 (€.1167; $1388) with some paid £ 6624 a day. The Committee chair, stated that "Despite the unimaginable resources thrown at this project, NHS Test and Trace cannot point to a measurable difference to the progress of the pandemic, and the promise on which this huge expense was justified—avoiding another lockdown—has been broken, twice." In particular, the Report pointed out that "the target to turn around all tests in face-to-face settings in 24 hours was never met."

Social acceptance and efficacy

Number of users

According to the UK government by September 27, 2020 there had been over 10 million downloads in England and Wales. More recent data (February 2021) indicate the figure of 21 million. However, it is not known how many of those downloads are still active. Incidentally, the BBC has reported [https://www.bbc.com/news/technology-56713017] that an April 2021 update by the NHS of the Covid-19 app has been blocked because it was not compliant with the Apple and Google terms of agreement. The NHS wanted to ask users to upload logs of venue check-ins (via QR scans) if they tested positive to the virus.

Number of cases reported

The UK government issues weekly statistics on the NHS Test and Trace system. Although there is a section devoted to contact tracing it is not clear to what extent this tracing is done through the Covid-19 app.

Reference to official or scientific studies

Official documents

ICO, Apple and Google joint initiative on COVID-19 contact tracing technology,
https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

UK Department of Health and Social Care, 23 March 2021]
https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment

UK House of Commons - Joint Committee on Human Rights, Chair's Second Briefing Paper on the Lockdown Regulations,
https://committees.parliament.uk/writtenevidence/5454/pdf/

UK House of Commons - Public Accounts Committee. Covid-19: Test, track, and trace (part 1). 10 March 2021.
https://committees.parliament.uk/committee/127/public-accounts-committee/publications/reports.

Articles, comments and reports

Altmann et al., Acceptability of app-based contact tracing for COVID-19: Cross-country survey evidence,
https://www.medrxiv.org/content/10.1101/2020.05.05.20091587v1

Braithwaite et al., Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19
https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30184-9/fulltext

Briers, Holmes, Fraser, Demonstrating the impact of the NHS COVID-19 app,
https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app

Chidambaram et al., Observational study of UK mobile health apps for COVID-19,
https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30144-8/fulltext

Horvath, Banducci, James, Citizens' Attitudes to Contact Tracing Apps, https://www.cambridge.org/core/journals/journal-of-experimental-political-science/article/citizens-attitudes-to-contact-tracing-apps/

F9B8B8CFE051E6D89C3C9ADD6DF76019

Jacob, Lawarée, The adoption of contact tracing applications of COVID-19 by European governments,
https://www.tandfonline.com/doi/full/10.1080/25741292.2020.1850404

Privacy International, UK government Covid tracking app: what we found:
https://privacyinternational.org/long-read/3752/coronavirus-tracking-uk-what-we-know-so-far

Savona, The Saga of the Covid-19 Contact Tracing Apps: Lessons for Data Governance,
https://ideas.repec.org/p/sru/ssewps/2020-10.html

Williams et al., Public attitudes towards COVID-19 contact tracing apps: A UK based focus group study,
https://onlinelibrary.wiley.com/doi/10.1111/hex.13179

2.2.7. *Concluding remarks*

Six legal frameworks for tracing application systems were reviewed in this study. From this review it first can be observed that the legal framework is highly impacted by the type of architecture chosen for the application (centralised; partly centralised or decentralised). France is the only country which resorted to a centralised architecture for the tracing application. Such choice implied the adoption of a quite complex legal framework. As assessed in the report on the French application (see *supra,* 2.2.2.), the authors of the ROBERT protocol used for the application consider it more realistic in terms of efficiency "because only relying on data exchanges between applications to inform who is at risk or not [..] would depend on the current proximity between people leading to slow and incomplete information delivery" (see *supra* 2.2.5). Whether one should agree or not with such statement is left to the readers. In any case, the French system requires a stricter legal framework than those relying on a decentralised architecture. Because personal health data is shared with a public entity (the French Ministry of Health and Social Affairs), more security is required from a technical standpoint requiring regular opinions and controls by the national agency acting as a controller (the *Commission Nationale Informatique et Liberté*). That said, it does not seem that the choice of a centralised architecture had an impact on the social acceptance of the application.

With the exception of Germany, where a lively debate on the possible infringements of privacy that a centralised application would cause took place, it seems that in all the other countries the discussion focused on the risk of having people geolocated (see *supra* the National reports for Belgium – 1.2.2.1. – France – 1.2.2.2. – and the UK – 1.2.2.5), based on a misunderstanding of the functioning of the applications' system (on such misunderstanding see more specifically *supra* the report for France). In the latter, the numbers of activations of the application significantly rose after its reshaping, allowing for more functionalities available to users and transforming the application into a digital system that informs users and does not only trace them. A sociological study would be needed to scientifically corroborate that the increase of activations is mostly due to the reshaping of the application. Nevertheless, a correlation between this reshaping and the increase of activations can reasonably be envisaged. Therefore, the LEGAFIGHT experts proposes the adoption of a multifunctional application for Luxembourg (see *infra* 2.3. A Tracing application for Luxembourg? Position paper of the LEGAFIGHT experts' group). It also

emerges from our study that new functionalities were developed for all the reviewed applications. The most recent one, the Belgian application, was designed as a multifunctional system. In fact, possibilities offered by the applications to upload different types of documents (from the result of a PCR test to a future digital certificate of vaccination) should prompt individuals to download them. Given these new functionalities, the experts group considered it necessary to assess whether consumer law applies to tracing applications (see *infra* 2.3. A Tracing application for Luxembourg? Position paper of the LEGAFIGHT experts' group).

A second important point is the choice of the legislative instrument framing the use of the application. The German legislature chose a minimalist approach grounding its choice on the fact that data protection is considered a fundamental right, at least since the first *Microcensus* decision of the Federal Constitutional Tribunal. Domestic law was therefore considered as guaranteeing the respect of data protection. Moreover, the existence of a statute on infectious diseases that did not authorise the massive collection of personal data related to risk exposure by means of digital technologies was perceived as an obstacle to the passing of a legislation authorising such collection. Consequently, the implementation of the tracing system was based solely on the consent of users. Given the status of fundamental right of data protection, the protection granted was considered sufficient. Thus, the adoption of a specific legal framework was not regarded as necessary. The United Kingdom's approach was similar, being however stressed that the constitutional system of this country notably differs from that of Germany and that it could be argued that data protection is a fundamental right grounded in the UK constitution. As stated in the National Report on UK (see *supra* 1.2.2.5.), the legal basis can only be the Data Protection Act 2018, which implemented the GDPR and is still in force. The lack of a clear legal framework was clearly criticised at a more general level, with regard to the whole legal response to the pandemic. The Joint Committee on Human Rights depicted it as "the most draconian restrictions on civil liberties since the Second World War, seriously impinging on a range of rights albeit for the legitimate purpose of protecting public health". That said, neither in Germany nor in the UK were infringements of data protection related to the implementation of tracing applications reported.

Nevertheless, the experts' group is of the opinion that it is hardly arguable that article article 6.1.(e) of the GDPR is the most appropriate

legal basis for the legal framing of tracing applications. The fact that the processing of data for objectives of public interest should also be assisted by a specific normative basis under European or national law should not be considered as a superfluous legal requirement but, on the contrary, as an opportunity to clearly define the limits of the use of data (notably the retention period) as well as the entities that will act as the controller as per the GDPR requirements. The existence of a specific act (be it of regulatory nature or not) also guarantees transparency of the system and represents a strong signal coming from the legislature as to the importance granted to the respect of citizen's fundamental rights. Consequently, the experts' group advocates for the adoption of a specific legal framework if a sanitary application was to be implemented in the Grand-Duchy of Luxembourg (see *infra,* 2. A Tracing application for Luxembourg? Position paper of the LEGAFIGHT experts' group). The Belgian, French, Italian and Australian legislations can be a source of inspiration (the latest has even established a list of several serious offences relating to the infringement of the tracing app related bill see *infra* 1.2.2.6.).

Last but not least, the experts' group would like to emphasise that any developments regarding digital tracing or e-health devices should be backed by an in-depth sociological study allowing to understand how to improve social acceptance of such systems. If there is something that this project achieved in demonstrating, it is that all the legal frameworks that were scrutinised showed that the legal instruments adopted successfully protected the rights of users (though they can certainly be improved for some aspects). Nevertheless, the discussion of the efficiency of tracing applications in combatting the pandemic, at least in legal systems like those studied, where the legal framework is highly respectful of citizens' fundamental rights, is still open (see more specifically the polls quoted in the National Report on UK, *infra* 1.2.2.5.).

2.3. *Beyond Data Protection: Tracing applications and Consumer Law* (L'application du droit de la consommation aux applications traceuses)

Les applications traceuses étudiées dans le projet LEGAFIGHT peuvent poser des problèmes qui dépassent le cadre du traitement des données personnelles. Dans la mesure où ces applications sont exploitées par des entités publiques, les utilisateurs se trouvent dans une situation d'infériorité vis-à-vis de celles-ci. Cette infériorité n'est pas sans rappeler le déséquilibre entre les consommateurs et les professionnels, tel qu'envisagé par le droit de la consommation. Cela conduit à s'interroger sur une éventuelle application de la protection spécifique qu'il prévoit[121]. Il faut également noter que les problématiques posées par la protection des données personnelles et le droit de la consommation tendent à se recouper. On songe par exemple au déséquilibre informationnel subi par l'utilisateur et le consommateur[122]. Ainsi, si l'entité publique qui met en place une application traceuse « anti-Covid » pouvait être qualifiée de « *professionnel* », et l'utilisateur de « *consommateur* » au sens du droit de la consommation, leur relation relèverait à la fois des dispositions liées à la protection des données et à la protection des consommateurs.

Avant d'entrer dans le cœur de notre étude, quelques précisions sont nécessaires afin d'en circonscrire le champ. Dans de nombreux États, des applications traceuses ont été mises en place par les pouvoirs publics

[121] On sait par ailleurs, comme le relèvent de nombreux auteurs, que les frontières de ce droit sont particulièrement difficiles à tracer. Sur cette question, V. E. Poillot, « Droit européen de la consommation », Dalloz Action, 2021-2021, pp. 57-61 ; E. Poillot et V. Zeno-Zencovich, « Définir le droit de la consommation : mission impossible ? » in Mélanges en l'honneur de Pascal Ancel, 1ère éd., Collection de la Faculté de Droit, d'Économie et de Finance de l'Université du Luxembourg, Larcier, 2021, pp. 187-198 ; J. Julien, « La consumérialité » in Études en la mémoire de Philippe Neau-Leduc, LGDJ, 2018, p. 537 ; G. Paisant, Défense et illustration du droit de la consommation, Lexisnexis, 2015, pp. 75 et s. ;

[122] Le Règlement Général sur la Protection des Données (RGPD) prévoit à son article 13 une information de l'utilisateur portant, entre autres, sur l'identité du responsable de traitement et les finalités du traitement des données. Une telle obligation rappelle l'obligation d'information de la directive 2011/83 à destination du consommateur avant la conclusion de tout contrat à distance. Par exemple, l'obligation d'information mise en place par l'article 6, a) de la directive 2011/83 précise que le professionnel doit informer le consommateur des « *principales caractéristiques du bien ou du service* ». Du fait de l'étendue de l'expression « *caractéristiques principales* », il ne serait pas douteux de considérer que l'information due à l'usager au titre du RGPD puisse également l'être au titre de la directive 2011/83 susmentionnée.

afin de faciliter la gestion des effets de la pandémie de la Covid-19. Leur fonctionnement présente généralement deux aspects. Premièrement, ces applications offrent la possibilité à leurs utilisateurs d'être alertés lorsqu'ils ont été en contact avec une personne testée positive à la maladie en « retraçant » les contacts entre les téléphones de leurs utilisateurs. Deuxièmement, elles peuvent prévoir diverses autres fonctionnalités destinées à faciliter les démarches de l'utilisateur vis-à-vis des autorités sanitaires[123]. Les entités étatiques qui mettent en place et gèrent ces applications sont diverses mais ont en commun leur nature d'administration publique[124]. Les utilisateurs sont les personnes physiques qui installent et utilisent ces applications traceuses. Nos développements se concentreront sur la relation juridique entre ces entités publiques et les utilisateurs des applications qu'elles proposent[125].

Enfin, une dernière précision s'avère nécessaire pour délimiter le champ de notre recherche. Le droit de la consommation suppose l'existence d'un cadre contractuel pour la grande majorité des règles qui le composent[126].

[123] Par exemple, l'application française « TousAntiCovid » permet, en cas de notification de contact avec une personne infectée, de se faire tester de manière prioritaire, de recevoir des informations et des recommandations et de conserver les résultats de ses tests afin de faciliter leur présentation. Elle propose aussi la possibilité de stocker certaines données personnelles sur l'application afin de faciliter l'émission des justificatifs requis par les autorités nationales. V. article 1er, II, 5°, 6°, 7° et 8° du décret n°2020-65 du 29 mai 2020 relatif au traitement de données dénommé « TousAntiCovid » ;

[124] Entre autres : En Allemagne, l'application « Corona Warn App » est mise en place par le Robert Roch Institute, l'agence de santé publique allemande (V. https://www.rki.de/EN/Content/Institute/institute_node.html ; dernière consultation le 30 juin 2021) ; En Belgique, l'application « Coronalert » est mise en place par Sciensano, un établissement publique fédéral chargé de la santé publique (V. https://coronalert.be/fr/conditions-dutilisation/ ; dernière consultation le 30 juin 2021) ; En France, l'application « TousAntiCovid » » est gérée directement par le Ministère ayant la santé dans ses attributions (V. Article 1er, I, du décret n°2020-65 du 29 mai 2020, préc.) ;

[125] Nous rappellerons que l'utilisation des applications traceuses « anti-Covid » est une relation tripartite. En effet, lors du téléchargement de l'application, l'usager est non seulement en relation avec l'entité publique qui met l'application à disposition, mais également avec la plate-forme par le biais de laquelle il la télécharge. Le droit de la consommation trouvera bien entendu à s'appliquer à la relation entre l'utilisateur et l'entreprise qui gère la plate-forme de téléchargement des applications : Apple pour l'Appstore, ou Google pour le Google Play store.

[126] C'est le cas de la directive 2011/83 qui établit des obligations d'information précontractuelles à la charge des professionnels pour les contrats avec les consommateurs, ou encore de la directive 93/13 qui met en place un régime de protection des consommateurs contre les clauses abusives insérés dans les contrats conclus avec les professionnelles. La directive 2005/29 relative à la lutte contre les pratiques commerciales déloyales fait alors office d'exception, car elle peut trouver application en l'absence de tout contrat. V. par ex.

Cependant, les dispositions régissant l'utilisation des applications traceuses sont de nature variable selon les États. En Allemagne, les règles applicables à l'application « Corona Warn App » sont d'ordre essentiellement contractuel[127] et l'application du droit de la consommation ne fait aucun doute[128]. Dans d'autres États comme Belgique ou de la France, la relation entre l'utilisateur et l'entité publique n'est pas directement identifiée comme étant de nature contractuelle. L'utilisateur se trouve-t-il alors dans une situation légale ou réglementaire, ou bien dans une situation contractuelle vis-à-vis de l'entité publique ? Dans le premier cas, l'absence de contrat conclu entre cet utilisateur et l'entité publique le priverait du plein bénéfice de la protection du droit de la consommation[129]. Dans le second en revanche, l'utilisateur pourrait éventuellement bénéficier de la protection du droit de la consommation au titre du contrat conclu, et notamment de la protection contre les clauses abusives[130].

La réponse à cette question peut dépendre des caractéristiques du système juridique de l'État membre, si celui-ci prévoit des règles particulières applicables aux entités publiques. Elle peut aussi dépendre des modalités prévues par les lois et règlements adoptés spécifiquement au regard des applications traceuses « anti-Covid », ou encore, de leurs conditions générales d'utilisation le cas échéant. Pour ces raisons, il serait difficile de donner une réponse générale, valant pour toutes les applications proposées par les États membres de l'Union. Une telle recherche nécessiterait une étude individuelle dans chacun des 27 systèmes juridiques nationaux, qui dépasserait très largement le cadre de notre propos. Nous pouvons

CJUE, 20 juillet 2017, *Gelvora*, C-357/16, point 20 ;

[127] Le gouvernement allemand précise sur le site internet de l'application qu'aucune législation n'est nécessaire, dans la mesure où l'application est librement installée et utilisée par les utilisateurs. (V. « *L'utilisation de la Corona Warn App est-elle obligatoire ?* » https://www.bundesregierung.de/breg-fr/dossier/corona-warn-app-faq-1761438#:~:text=L›utilisation%20de%20la%20Corona,au%20bon%20vouloir%20de%20chacun) ; Dernière date de consultation : 3 juin 2021 ;

[128] La clause n°13 des conditions d'utilisation de l'application allemande qualifie d'ailleurs l'utilisateur de consommateur, lorsqu'elle traite du droit applicable : « *This does not affect the statutory provisions on restriction of the choice of law and on the applicability of mandatory provisions, including those in the country in which you as a consumer are resident.* » ;

[129] Cela ne signifierait pas pour autant que l'utilisateur se retrouverait démuni face à l'entité publique. Premièrement, le RGPD trouverait malgré tout à s'appliquer. Ensuite, l'utilisateur bénéficierait éventuellement de la possibilité de contester la validité de l'acte législatif ou réglementaire fixant les conditions d'utilisation de l'application.

[130] Cf. point sur l'insertion de la clause d'exonération de responsabilité dans les conditions d'utilisations de l'application allemande « Corona Warn App », sous note 4 ;

cependant donner une illustration avec le cas français et l'application « TousAntiCovid ». Dans le système français, la fourniture d'une application « anti-Covid » peut être qualifiée de service public[131]. Savoir si l'usager se trouve dans une relation contractuelle ou non avec une entité publique dépend du type de service public fourni[132]. Alors que les services publics industriels et commerciaux supposent l'application des règles du droit privé dans la relation avec les usagers, les services publics administratifs supposent que l'usager se trouve dans une situation légale et réglementaire. Dans une telle situation, l'application des règles du droit privé est en principe exclue[133]. Au vu des caractéristiques et des objectifs de l'application « TousAntiCovid », sa qualification de service public administratif fait peu de doute[134]. Par conséquent, ses usagers se trouveraient dans une situation légale et réglementaire excluant l'application du droit de la consommation.

[131] Qui se définit localement comme activité d'intérêt général assurée ou assumée par une personne publique, et régie au moins partiellement par des règles de droit public. Dans la mesure où elle est gérée par le Ministère ayant la santé dans ses attributions, une partie au moins du régime de l'application sera organiquement soumis aux règles du droit public.

[132] Le droit administratif français connait deux types de service public. Les services publics administratifs et les services publics industriels et commerciaux. (Tribunal des conflits français, 22 janvier 1921, Bac d'Eloka, n°00706, Rec. Lebon p. 91). Les premiers sont exclusivement soumis au droit public alors que les seconds se voient appliquer les règles du droit privé dans leurs relations avec les usagers.

[133] B. Delaunay, Synthèse – Service publics, JurisClasseur Administratif, LexisNexis, 2017, n°34 et 35 ; P. Terneyre, Grève dans les services publics, Répertoire de droit du travail, Dalloz, 2017, n°452

[134] Rappelons que la qualification de service public administratif ou de service public industriel et commercial dépend de trois critères cumulatifs (Conseil d'État français, 16 novembre 1956, Union syndicale des industries aéronautiques, Rec. CE 1956, p. 434) : l'objet du service, le mode de financement du service, les modalités de fonctionnement du service. S'agissant de l'objet du service, il ne peut être de nature industrielle et commerciale que s'il ressemble à un service assuré par une personne privée. L'application « TousAntiCovid » ayant pour objet d'améliorer la gestion de la pandémie et de ses conséquences, elle relève de la santé publique. Par analogie, l'établissement français du sang avait été considéré comme un service public administratif au regard de son objet (Conseil d'État français, 20 octobre 2000, n° 222672, Mme T., AJDA 2001, p. 394). S'agissant du mode de financement du service, le service public est industriel et commercial lorsque le coût est assuré pour l'essentiel par l'usager. Il est administratif lorsqu'il est gratuit ou que le coût demandé à l'usager ne correspond pas au coût réel du service (Tribunal des conflits français, 25 avril 1994, Syndicat mixte d'équipement de Marseille, n°02917). S'agissant du mode de fonctionnement du service, le service public est industriel et commercial lorsqu'il est géré d'une manière similaire à une gestion commerciale. Dans le cas de l'application « TousAntiCovid », tant la gratuité que son lien avec la santé publique tendent à démontrer sa nature de service public administratif. L'usager serait selon toute vraisemblance dans une situation légale et réglementaire à l'égard de l'entité qui la met en place.

Cet argument est toutefois à relativiser car la distinction entre service public administratif et service public industriel et commercial relève du droit interne. Or, la Cour de Justice a déjà eu l'occasion d'affirmer que le statut juridique et les caractéristiques d'un organisme public au titre du droit national étaient dépourvus de pertinence vis-à-vis de l'interprétation des règles du droit européen de la consommation[135]. La présence d'une situation purement légale ou réglementaire ne semble donc pas de nature à faire obstacle à l'application du droit européen[136]. Notre propos se concentrera donc essentiellement sur l'étude de ce droit, étant donné qu'il s'applique dans le territoire des États membres sans tenir compte des qualifications nationales des entités publiques mettant en place les applications traceuses.

Comme brièvement indiqué plus haut, ce droit peut trouver une utilité pour l'utilisateur des applications traceuses, dont l'utilisation n'est pas sans risque pour les usagers. Ces derniers peuvent rencontrer diverses difficultés liées au fonctionnement des applications, auxquelles la protection instaurée par les directives en matière de protection des consommateurs peut apporter une réponse. Quelques exemples peuvent être d'ores et déjà relevés, notamment au sujet de la conformité de l'application, ou des éventuelles clauses abusives pouvant se retrouver dans leurs conditions générales d'utilisation lorsque celles-ci sont de nature contractuelle. En tant qu'applications numériques installées sur le téléphone de l'usager, elles peuvent être qualifiées de service numérique au sens de la directive 2019/770[137]. Imaginons qu'à la suite d'un dysfonctionnement, l'utilisateur

[135] CJUE, 3 octobre 2013, *Zentrale zur Bekämpfung unlauteren Wettbewerbs*, C-59/12, point 26 ; Nous reviendrons plus en détail sur l'apport de cette décision dans le cadre de nos développements à propos de la soumission des personnes publiques au droit de la consommation.

[136] Bien entendu, l'absence de relation contractuelle exercera nécessairement une influence sur l'étendue de la protection de l'usager par le droit européen de la consommation. L'absence de contrat conclu entre l'utilisateur et l'entité publique empêche, de facto, le recours à la protection contre les clauses abusives, ou l'existence d'une quelconque obligation d'information. Elle n'empêche pas en revanche la caractérisation d'une pratique commerciale déloyale. Nous reviendrons sur cette question à l'occasion de notre partie sur le champ matériel des directives du droit de la consommation.

[137] Le service numérique est défini par la directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques comme : (a) « *un service permettant au consommateur de créer, de traiter ou de stocker des données sous forme numérique, ou d'y accéder* » ou (b) « *un service permettant le partage ou toute autre interaction avec des données sous forme numérique qui sont téléversées ou créées par le consommateur ou d'autres utilisateurs de ce service* » ;

voie ses données effacées et ne puisse finalement bénéficier des fonctionnalités de l'application. La question de sa conformité vis-à-vis des règles posées par la directive susmentionnée pourrait être soulevée.

S'agissant de la présence éventuelle de clauses abusives, il est possible de prendre en exemple les conditions générales de l'application allemande « Corona Warn App ». Elles prévoient une clause d'exonération de responsabilité de l'autorité qui trouve à s'appliquer en cas d'erreur ou de piratage des données personnelles[138]. Dans cette hypothèse, la question du caractère abusif d'une telle exclusion pourrait se poser à l'aune de la protection instaurée par la directive 93/13 relative à la lutte contre les clauses abusives.

Cet apport est d'autant plus important que l'utilisation d'applications traceuses risque de devenir incontournable pour les citoyens européens. Certes, leur installation et leur utilisation sont facultatives pour les usagers[139]. L'évolution de leurs fonctionnalités pourrait néanmoins avoir un impact non négligeable sur le choix des utilisateurs de les installer sur leurs téléphones portables. Certains pays européens ont en effet instauré des restrictions drastiques de la liberté de circulation des personnes[140] en soumettant les arrivées sur leur territoire à l'obligation de présenter un test PCR négatif de moins de 72h[141], voire 48h dans certains cas[142]. Les tests étant faits sur

[138] La clause n°11 des conditions générales de l'application « Corona Warn App » stipulant que le RKI (le fournisseur de l'application), ne garantit pas l'utilisation de l'application sans erreur ni interruption, ni que l'application ne subira aucune : perte, corruption, attaques informatiques, virus, interférences, piratage ou tout autre problème de sécurité.

[139] Par exemple en France, V. Article 1er, III du Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « TousAntiCovid ». Il est intéressant de noter cependant que l'installation de l'application et son utilisation ne sont pas basées sur le volontariat dans certains États. C'est par exemple le cas à Singapour. V. https://www.technologyreview.com/2020/11/23/1012491/contact-tracing-mandatory-singapore-covid-pandemic/

[140] C'est le cas notamment de la Belgique, du Danemark, de la Tchéquie ou encore de la Finlande.

[141] Par exemple en France : Article 6 du Décret n° 2020-1310 du 29 octobre 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de la Covid-19 dans le cadre de l'état d'urgence sanitaire ; Également en Belgique : Article 3 de l'arrêté ministériel du 28 octobre 2020 portant des mesures d'urgence pour limiter la propagation de la Covid-19 ;

[142] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Transport/Archiv_Tests/Test_06042021_en.pdf?__blob=publicationFile

prise de rendez-vous et les délais de communication des résultats des tests PCR allant parfois eux-mêmes jusqu'à 72h, avoir en sa possession le résultat des tests effectués au moment de l'entrée sur le territoire d'un autre État membre pourrait s'avérer difficile. Certaines applications permettent de bénéficier d'un test prioritaire en cas de croisement avec une personne testée positive. Il est alors envisageable qu'un citoyen européen devant se rendre dans un autre État pour une urgence installe l'application pour maximiser ses chances d'obtenir le résultat du test le plus rapidement possible. Il est également intéressant de noter que la Commission européenne envisage actuellement la création d'un *Digital Green Certificate* attestant d'une part, du statut vaccinal des citoyens européens, d'autre part de leur soumission à un test revenu négatif et enfin, de leur rémission d'une contamination antérieure[143]. Dans la droite ligne de ce projet, l'application française va d'ailleurs bientôt présenter une nouvelle fonctionnalité appelée « Carnet de test », permettant aux utilisateurs de stocker les résultats de leurs tests afin d'en faciliter la présentation aux autorités nationales[144]. Ce type d'évolution pourrait remettre en question le caractère facultatif de l'installation et de l'utilisation des application traceuses « anti-Covid ». La protection de l'utilisateur apparaîtrait, dès lors, d'autant plus importante que le « libre choix » de l'utilisateur risque de se transformer à plus ou moins long terme en « non-choix ».

Si l'on admet que la protection du droit de la consommation pourrait être utile aux usagers des applications traceuses en complément des droits garantis par le droit des données personnelles, une question demeure : le droit de la consommation est-il applicable au regard des spécificités des applications traceuses et de la relation entre les usagers et les entités publiques qui les mettent en place ?

La question de l'applicabilité matérielle du droit de la consommation implique de surmonter plusieurs difficultés tenant au contexte de la fourniture de telles applications. Cela suppose de traiter du problème de l'application du droit de la consommation aux relations entre les entités publiques et les usagers d'une part, et du champ d'application matériel de chacune des directives du droit de la consommation. Certaines prévoient en

[143] Communication from the Commission to the European Parliament, The European Council and the Council, A common path to safe and sustained re-opening, COM (2021) 129 final.

[144] https://tousanticovid.stonly.com/kb/guide/fr/informations-generales-4WLNKEHmTL/Steps/321015

effet des exclusions pouvant influer sur l'applicabilité des régimes qu'elles mettent en place[145]. D'autres ne ciblent, pour leur part, qu'un type de contrat déterminé[146].

Pour ces raisons, notre étude se focalisera sur ceux deux difficultés. Il s'agira en premier lieu de s'interroger sur l'influence du caractère public des entités qui mettent en place applications traceuses « anti-Covid » sur l'applicabilité du droit de la consommation. Nous rappellerons à ce titre que le droit européen de la consommation trouve à s'appliquer en principe aux relations entre les entités publiques et les usagers (I). En second lieu, il s'agira de traiter la question de savoir si la fourniture d'applications traceuses entre matériellement dans le champ des directives du droit de la consommation compte tenu de leurs spécificités (II).

2.3.1. *Le principe de la soumission des entités publiques au droit de la consommation*

Le droit de la consommation nécessite pour son application la réunion de plusieurs critères. Le premier est la présence d'une relation entre un consommateur et un professionnel. Le consommateur est généralement défini comme une personne physique agissant à des fins n'entrant pas dans le cadre de son activité professionnelle[147]. La qualification de consommateur de l'utilisateur d'applications traceuses ne soulève pas de difficulté. La question de la qualification de « *professionnel* » des autorités nationales qui mettent en place et gèrent ces applications est en revanche plus délicate. Pour qu'une telle qualification soit possible, il est nécessaire d'établir tout d'abord que la qualité de personne morale de droit public n'exclut pas la qualification de professionnel (i) et que la nature publique d'une activité n'exclut sa qualification d'activité professionnelle (ii).

(i) La soumission des personnes morales de droit public au droit de la consommation

Le droit européen de la consommation n'est pas insensible à la difficulté soulevée par son application aux personnes morales de droit public. La prise

[145] On songe par exemple à la directive 2011/83 relative aux droits des consommateurs qui exclut notamment son application aux services sociaux, aux jeux d'argent, aux services financiers, etc.
[146] On songe ici à la directive 2019/771 relative à certains aspects concernant les contrats de vente de biens, dont l'application se limite, logiquement, aux contrats de vente.
[147] Ou « *activité commerciale, industrielle, artisanale ou libérale* », selon les directives en droit européen de la consommation.

en compte de leurs particularismes a par ailleurs très tôt été relevée et en partie résolue dans les directives européennes. De même, la Cour de Justice a maintes fois réaffirmé la soumission de la personne publique au droit de la consommation, la situation factuelle de l'usager face à l'administration publique présentant le germe de l'asymétrie contre laquelle la protection européenne des consommateurs tend à lutter.

Quatre directives retiendront notre attention dans le cadre de cette étude, dans la mesure où leurs dispositions intéressent la protection des utilisateurs. Il s'agit de la directive 93/13/CE relative à la protection contre les clauses abusives, de la directive 2005/29/CE relative à la protection contre les pratiques commerciales déloyales, de la directive 2011/83/UE relative aux droits des consommateurs ainsi que de la directive 2019/770/UE relative à la conformité des contenus et services numériques.

Les directives 2011/83 et 2019/770 proposent une définition identique et particulièrement large du professionnel : « *toute personne physique ou morale, qu'elle soit publique ou privée […]* ». Dans la mesure où les personnes morales de droit public sont inclues au sein même de la définition qu'elles donnent, ces deux directives n'appellent pas davantage de commentaire sur la possibilité de leur application aux entités publiques pourvues de la personnalité morale. Tel n'est pas le cas pour les directives 2005/29 et 93/13, qui méritent un examen plus approfondi.

La directive 2005/29 ne mentionne pas directement la possibilité pour une personne morale de droit public d'être qualifiée de « *professionnel* » au titre de la protection contre les pratiques commerciales déloyales[148]. La prudence de la formulation semble s'expliquer par la proximité du régime imposé par la directive avec celui du droit européen de la concurrence qui admet des exceptions à la soumission des personnes publiques[149]. En dépit de similitudes marquées avec la réglementation du droit de la

[148] Directive 2005/29, article 2, b) : « *professionnel* » : *toute personne physique ou morale qui, pour les pratiques commerciales relevant de la présente directive, agit à des fins qui entrent dans le cadre de son activité, commerciale, industrielle, artisanale ou libérale, et toute personne agissant au nom ou pour le compte d'un professionnel.*

[149] C'est le cas des personnes morales de droit public qui exercent une activité économique, lorsque l'application des règles du droit de la concurrence empêcherait la réalisation de la mission d'intérêt économique général (V. article 106 du TFUE). Idem pour les personnes morales de droit public n'exerçant pas d'activité économique qui doivent assurer l'effet utile de réglementation du droit de la concurrence, sans pour autant y être assujetties (CJUE, 16 novembre 1977, *Inno*, C-13/77).

concurrence, la directive 2005/29 participe tout de même de la politique de protection des consommateurs. À ce titre, la Cour de Justice a déjà eu l'occasion de reconnaître son application à des personnes morales de droit public lorsque ces dernières se trouvaient face à un consommateur en raison de l'interprétation autonome du droit de l'Union[150], les qualifications juridiques nationales étant dépourvues de pertinence pour l'application du droit européen lorsque les directives n'y font pas un renvoi exprès[151].

Aux termes de l'article 2 de la directive 93/13, il faut entendre par « *professionnel* » : « *toute personne physique ou morale qui, dans les contrats relevant de la présente directive agit dans le cadre de son activité professionnelle, qu'elle soit publique ou privée* ». Les termes « *publique ou privée* » ne sont pas ici à comprendre comme étant relatifs à la personne mais à l'activité qu'elle exerce, ainsi que l'explique la directive dans ses considérants[152]. La précision est importante car l'activité de nature publique et la personne publique ne sont pas systématiquement liées. Une activité de nature publique peut être exercée tant par une personne morale de droit public que par une personne morale de droit privé chargée d'une mission d'intérêt général. La définition du professionnel de la directive 93/13 ne donne pas de réponse tranchée, faute de précision textuelle sur la nature publique ou privée de la personne morale. La Cour de Justice a cependant eu l'occasion de préciser que seule une interprétation large de la notion de professionnel est de nature à permettre l'efficacité de la protection des consommateurs contre les clauses abusives[153]. Elle a par ailleurs affirmé dans un arrêt *Karel de Grote* que la directive 93/13 n'excluait pas de son champ d'application « *les entités poursuivant une mission d'intérêt général ni celles qui revêtent un statut de droit public*[154] ».

Quelle que soit donc la directive concernée, le statut de personne morale de droit public ne semble pas faire obstacle à la qualification de professionnel, soit en raison de l'inclusion directe dans leurs définitions

[150] CJUE, 3 octobre 2013, *Zentrale zur Bekämpfung unlauteren Wettbewerbs*, préc., point 32, dans lequel la Cour estime qu'une personne morale, fût-elle de droit public, exerçant une activité rémunérée doit être considérée comme un professionnel au sens de la directive 2005/29.
[151] CJUE, 19 septembre 2000, *Linster*, C-287/98, point 43 ; CJUE, 11 mars 2003, *Ansul*, C-40/01, point 26 ; CJUE, 30 juin 2011, *VEWA*, C-271/10, point 25 ;
[152] Directive 93/13/CE, considérant 14 ;
[153] CJUE, 21 mars 2019, *Pouvin et Dijoux*, C-590/17, point 42 et CJUE, 31 mai 2018, *Sziber*, C-483/16, point 32 ;
[154] CJUE, 17 mai 2018, *Karel de Grote*, C-147/16, point 51 ;

du professionnel, soit en raison de l'interprétation large de cette notion commandée par l'effet utile des directives, lorsque l'usager se trouve dans une situation de déséquilibre face à une personne morale de droit public.

Refuser de soumettre ces dernières au droit de la consommation dans leurs rapports avec les usagers reviendrait à établir une différence dans le niveau de protection des consommateurs, basée sur un critère organique que la Cour de Justice a jugé dénué de pertinence au regard du droit de l'Union[155]. D'un point de vue pragmatique, cette différence serait d'autant moins acceptable que la situation d'infériorité de l'usager se trouve renforcée par les prérogatives exorbitantes dont sont pourvues les personnes morales de droit public pour l'accomplissement de leur mission. On peinerait alors à comprendre pourquoi les consommateurs seraient davantage protégés face à des personnes morales de droit privé que face à des personnes morales de droit public.

Sur le plan du droit européen, il n'y a donc aucune difficulté à admettre la possibilité de qualifier les administrations nationales « *responsables*[156] » des applications comme des professionnels dans leurs rapports avec les utilisateurs.

Le critère personnel n'est qu'une partie de l'opération de qualification du professionnel. Physique ou morale, publique ou privée, la personne du professionnel doit agir à des fins entrant dans le cadre de son activité professionnelle afin d'être qualifiée comme tel. La question se pose donc de savoir si l'activité d'une personne morale de droit public peut être considérée comme une activité professionnelle au sens du droit de la consommation.

(ii) La soumission des activités de nature publique au droit de la consommation

Afin de savoir si la mise à disposition d'une application traceuse entre dans le champ d'application du droit de la consommation, il est nécessaire de s'interroger sur le fait de savoir si l'activité de la personne publique qui la propose peut être qualifiée d'activité professionnelle. Dans

[155] CJUE, 3 octobre 2013, *Zentrale,* préc., point 26 ;

[156] Le sens du terme est à comprendre conformément au RGPD, c'est-à-dire : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

cette optique, il convient de relever tout d'abord une difficulté d'ordre terminologique au sein des directives considérées.

On note une divergence de formulation dans les directives mentionnées relativement à l'activité aux fins desquelles la personne du professionnel doit agir. Alors que la directive 93/13 mentionne une « *activité professionnelle, qu'elle soit publique ou privée* », les directives 2005/29, 2011/83 et 2019/770 font référence à une « *activité commerciale, industrielle, artisanale ou libérale* ». Sur le plan purement linguistique, le caractère *commercial, industriel, artisanal ou libéral* est inclus dans le qualificatif *professionnel*. En revanche, l'inverse n'est pas vrai. Une activité professionnelle peut n'être ni *commerciale,* ni *industrielle*, ni *artisanale*, ni *libérale*[157]. Alors que l'adjectif « *professionnel* » renvoie à une manière d'exercer une activité, les quatre autres qualificatifs renvoient à un type d'activité spécifique. Une première lecture de ces définitions conduirait à conférer à la directive relative à la protection contre les clauses abusives un champ d'application bien supérieur aux trois autres. Si le fait de proposer une application traceuse « anti-Covid » au public vient immédiatement à l'esprit comme ayant un caractère professionnel, il est douteux d'estimer qu'elle présente un caractère commercial, industriel, artisanal ou encore libéral. En conséquence, la publication d'une telle application se devrait de respecter la réglementation contre les clauses abusives de la directive 93/13, mais ne serait soumise en principe ni à la protection contre les pratiques commerciales déloyales de la directive 2005/29, ni à l'obligation d'information de la directive 2011/83, ni même l'exigence de conformité des contenus et services numériques de la directive 2019/770. Divergence réelle, ou divergence d'apparence ? L'analyse du droit de l'Union permet de pencher davantage vers la seconde option pour plusieurs raisons.

La première est d'ordre linguistique et tient au principe d'interprétation uniforme du droit de l'Union. Si les directives 2005/29, 2011/83 et 2019/770 mentionnent dans leur définition du professionnel une « *activité libérale* », tel n'est pas le cas des autres versions linguistiques des directives qui présentent pour la quasi-totalité d'entre elles l'équivalent du mot « *profession* » en français[158]. Chaque version linguistique ayant valeur

[157] On songe ici à l'activité de l'agriculteur, de l'intermittent du spectacle, ou encore, du prêtre.

[158] La version anglaise dispose que le *trader* agit à des fins entrant dans le cadre de ses « *trade, business, craft or profession* » ; la version espagnole dispose pour sa part que le *comerciante* agit à des fins entrant dans le cadre de son « *actividad económica, negocio, oficio o profesión* » ; la version allemande, que les *Gewerbetreibender* agissent à des fins entrant dans le cadre de leurs « *gewerblichen, handwerklichen oder beruflichen Tätigkeit* » ; enfin, la version portugaise

authentique[159], une version ne peut prévaloir sur une autre. En cas de divergence linguistique d'une version par rapport aux autres, il est de jurisprudence constante que la disposition divergente doit être interprétée en considération de toutes les autres, en vertu du principe d'interprétation uniforme du droit de l'Union[160]. Si la divergence porte sur une notion autonome du droit de l'Union, c'est-à-dire une notion ne faisant pas de renvoi explicite au droit des États membres, elle doit être interprétée en fonction de l'économie générale et de la finalité de la réglementation dont elle constitue un élément[161] et ce, à la lumière des versions établies dans toutes les langues et de la volonté réelle de leur auteur[162]. En droit de la consommation, la question s'était posée pour l'application de la directive 93/13 dont la version néerlandaise ne renvoyait pas au « *professionnel* » mais au « *vendeur* » (« *verkoper* »). La juridiction néerlandaise doutait alors qu'un bailleur professionnel puisse être qualifié de vendeur au sens de la directive 93/13. Dans son arrêt *Asbeek Brusse et Man Garabito*[163], la Cour de justice répondit que toutes les autres versions de la directive faisaient usage du terme « *professionnel* » et qu'il convenait d'en déduire que l'intention du législateur européen n'avait pas été de limiter le champ d'application de la directive aux seuls vendeurs, la directive 93/13 étant dès lors applicable au bailleur professionnel[164].

fait, elle, référence à une « *actividade comercial, industrial, artesanal ou profissional* ».

[159] Ce principe d'égalité linguistique est fondé sur l'actuel article 342 du TFUE, donnant compétence au Conseil pour fixer le régime linguistique par voie de règlement et sur le règlement du Conseil n°1/58.

[160] V. par exemple : CJUE, 27 octobre 1977, *Bouchereau*, C-30/77, point 14 ; CJUE, 7 décembre 1995, *Rockfon*, C-449/93, point 28 ; CJUE, 17 décembre 1998 *Codan*, C-239/97, point 26 ; CJUE, 11 décembre 2003 *Hässle*, C-127/00, point 70 ; CJUE, 29 avril 2004, *Plato Plastic Robert Frank*, C-341/01, point 64 ; CJUE, 29 avril 2010, *M e.a.*, C-340/08, point 44 ; CJUE, 15 novembre 2012, *Kurcums Metal*, C-558/11, point 48 ; CJUE, 9 avril 2014, *GSV*, C-74/13, point 27 ; CJUE, 21 juillet 2016, *EUIPO / Grau Ferrer*, C-597/14, point 24 et CJUE, 1er mars 2016, *Alo et Osso*, C-443/14 et C-444/14, point 27

[161] CJUE, 3 juin 2010, *Internetportal und Marketing*, C-569/08, point 35 ; CJUE, 9 juin 2011, *Eleftheri tileorasi et Giannikos*, C-52/10, points 23-24 ;

[162] CJUE, 29 avril 2010, *M e.a.*, C-340/08, points 44-45 et 64-65 ; La Cour de Justice étant allée jusqu'à considérer en pratique que lorsqu'une version est minoritaire par rapport aux autres, il y a lieu de faire prévaloir ces dernières, V. CJUE, 27 octobre 2011, *Commission / Pologne*, C-311/10, point 18 ;

[163] CJUE, 30 mai 2013, *Asbeek Brusse et Man Garabito*, C-488/11, point 28 ; Dans le même sens, pour l'application du principe d'interprétation uniforme à la directive 2005/29 : CJUE, 3 avril 2014, 4finance, C-515/12, points 19 et 20 ;

[164] *Ibid*, point 34 ;

La seconde raison est que ces quatre directives ont été adoptées sur le fondement de l'article 114 du TFUE relatif au rapprochement des législations nationales. Retenir une définition différente du professionnel pour les pays de langue juridique française[165] équivaudrait à créer une divergence de champ d'application entre ces trois États et les autres. Les activités exercées à titre professionnel sans pour autant être de nature commerciale, industrielle, artisanale ou libérale seraient alors exclues du champ d'application des directives dans ces trois États membres alors qu'elles ne le seraient pas dans tous les autres. Cette divergence serait manifestement incompatible avec l'objectif de rapprochement des législations de l'article 114 du TFUE. Elle créerait, du reste, une disparité dans le niveau de protection des consommateurs entre les États membres et entrerait en contradiction avec la finalité du haut niveau protection des consommateurs commun sur tout le territoire de l'Union[166]. Dès lors, plutôt que de considérer cette énumération d'activités comme limitative, il serait à notre sens plus juste d'y voir des illustrations d'une catégorie plus grande, l'activité professionnelle. Le risque d'une interprétation trop restrictive par les juridictions nationales est d'autant plus important qu'au Luxembourg, l'article L. 010-1 du code de la consommation qui pose les définitions du consommateur et du professionnel, est une transposition servile des définitions de la directive 2011/83[167].

Cette considération mène à un second questionnement, le caractère public d'une activité fait-il obstacle à sa qualification « *d'activité professionnelle* » ? Sur ce point, tant les directives de l'Union que la jurisprudence de la Cour de Justice tendent à montrer l'absence d'influence du caractère public ou privé de l'activité. Ainsi, la directive 93/13 mentionne qu'elle s'applique également aux activités à caractère public[168]. Ce constat est par ailleurs soutenu par l'interprétation de la Cour dans l'arrêt *Karel de Grote*, à l'occasion duquel la Cour estime le régime mis en place par la directive applicable à un établissement d'enseignement public qui propose des facilités de paiement

[165] En l'espèce la Belgique, la France et le Luxembourg.

[166] L'exigence de prise en compte d'un haut niveau de protection dans les actes juridiques européens est une exigence rappelée à plusieurs reprises dans le TFUE. C'est ainsi le cas de l'article 114 précité qui a servi de base juridique à l'adoption des directives examinées, ainsi qu'à l'article 169 du même traité. La Charte des droits fondamentaux de l'Union réaffirme également cette nécessité à son article 38.

[167] À la différence de la France, qui pour tenter de pallier le risque d'interprétation restrictive par les juridictions nationales, a plus ou moins maladroitement ajouté l'activité « agricole » au sein de l'article liminaire de son code de la consommation.

[168] Directive 93/13/CEE, considérant 15 ;

à ses étudiants[169]. Il en va de même pour l'activité d'avocat qui, en dépit de ses liens avec l'intérêt général, n'échappe pas non plus à la protection contre les clauses abusives dans les contrats conclus à l'occasion de cette activité[170].

Pour ce qui est de la directive 2005/29/CE, la Cour de Justice a eu l'occasion d'affirmer expressément son application aux activités à caractère public dans l'arrêt *Zentrale* précité[171].

Enfin, en ce qui concerne les directives 2011/83/UE et 2019/770/UE, ces dernières sont applicables également aux *personnes physiques ou morales, publiques ou privées*[172]. Les personnes morales de droit public n'ayant pas pour vocation première d'agir à des fins purement privées, ces textes semblent dès lors avoir vocation à s'appliquer aussi aux activités à caractère public.

Sur le plan théorique, le droit européen de la consommation ne s'oppose pas à ce qu'une personne morale de droit public soit considérée comme un professionnel lorsqu'elle interagit avec ses usagers dans le cadre de son activité. Il faut toutefois que cette interaction ait lieu à des fins entrant dans le cadre de cette activité professionnelle et que le droit de la consommation lui soit matériellement applicable.

2.3.2. *L'application du droit de la consommation aux applications traceuses*

Une personne morale de droit public qui met à disposition de ses usagers une application traceuse pourrait se voir reconnaître la qualité de professionnel. Cependant, afin que le droit de la consommation lui soit applicable, il est aussi nécessaire de tenir compte d'autre facteurs. Il faut d'une part que la mise à disposition de l'application puisse être rattachée à l'exercice de son activité professionnelle par application d'un critère finaliste (i). Il faut d'autre part tenir compte des spécificités de chacun des régimes mis en place par les directives pour leur application. Même en présence d'une relation entre consommateur et professionnel, certains éléments du régime peuvent conduire à écarter l'application des directives en question (ii).

[169] CJUE, 17 mai 2018, *Karel de Grote*, préc., point 51 et s. ;
[170] CJUE, 15 janvier 2015, *Šiba*, C-537/13, points 25 et 28 ;
[171] CJUE, 3 octobre 2013, *Zentrale zur Bekämpfung unlauteren Wettbewerbs*, préc., point 32.
[172] Article 2, 2) de la directive 2011/83 et article 2, 5) de la directive 2019/770 ;

(i) Les applications traceuses peuvent-elles être rattachées à l'activité professionnelle d'une personne morale de droit public ?

En droit européen, le caractère public ou privé de l'activité et la nature de l'activité concernée n'a que peu d'importance sur la qualification de « *professionnel* » de la personne qui exerce cette activité. L'important est que l'acte[173] considéré soit passé à des fins qui entrent dans le cadre l'activité professionnelle de cette personne. La question est alors de savoir si la fourniture d'applications traceuses aux usagers peut être rattachée à l'activité professionnelle de la personne publique responsable.

Le problème est que l'activité professionnelle largement entendue ne connaît aucune définition juridique nationale ou européenne formalisée dans un texte. Il est donc difficile de savoir quand un acte est passé à des fins entrant dans l'activité professionnelle. Certaines décisions de la Cour de Justice permettent toutefois de dresser quelques critères du rattachement : c'est le cas notamment de l'arrêt *Zentrale* déjà évoqué et de l'arrêt *Kamenova*.

Dans le premier arrêt, la Cour s'est prononcée sur l'influence d'un but lucratif sur la qualité de « *professionnel* ». Elle a notamment indiqué que la notion de professionnel, particulièrement large, vise toute personne exerçant une activité rémunérée et n'exclut pas pour autant les personnes exerçant une activité à caractère public et ne poursuivant pas un but lucratif[174]. Par conséquent, il est de peu importance qu'une personne morale de droit public, en proposant une application traceuse, agisse dans un but lucratif ou non, ce critère n'ayant dans ce cas précis aucune influence sur la possibilité de se voir qualifier de professionnel[175].

Toujours à propos de la question du rattachement d'un acte à l'activité

[173] Le terme est ici à comprendre au sens « d'agissement » et non « d'acte juridique », la protection du droit de la consommation n'exigeant pas toujours pour son application, l'existence d'un acte juridique constitué.

[174] CJUE, 3 octobre 2013, *Zentrale zur Bekämpfung unlauteren Wettbewerbs*, préc., point 32.

[175] Il est également intéressant de relever que la Cour de Justice avait adopté un raisonnement similaire par le passé, pour la directive 85/374 relative à la responsabilité du fait des produits défectueux. Cette directive prévoit à son article 7 une exonération de responsabilité lorsque le produit défectueux n'a pas été fourni dans un but économique par producteur. Dans un arrêt *Veefald*, la Cour de Justice a estimé que l'exonération ne visait pas un produit fabriqué par des hôpitaux intégralement financés par des fonds publics (CJUE, 10 mai 2001, *Veefald*, C-203/99). Par analogie, il est permis de penser également que l'absence de but économique de l'entité publique n'aurait pas réellement incidence sur sa qualification de professionnel, y compris pour l'application des quatre directives considérées dans notre étude.

professionnelle de son auteur, la Cour de Justice a eu l'occasion de donner, dans l'arrêt *Kamenova*[176], une liste de critères que les juridictions nationales doivent prendre en compte afin de déterminer si la personne en cause a agi à des « *fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale*[177] ». L'affaire portait en l'espèce sur le fait de savoir si, pour une personne physique, mettre en vente des biens par le biais d'une plate-forme en ligne pouvait être constitutif d'une activité professionnelle lui conférant la qualité de professionnel. En raison de la spécificité des faits de l'espèce, certains critères donnés par la Cour de Justice sont d'un intérêt limité par rapport à la question des applications traceuses, ces dernières n'impliquant pas l'existence d'un contrat de vente. D'autres, en revanche, peuvent être utiles en raison de leur généralité afin de vérifier que la fourniture d'une application traceuse « anti-Covid » relève de l'activité professionnelle de l'entité publique qui la met à disposition.

Tout d'abord, la Cour énonce que la juridiction de renvoi devra vérifier si l'acte a été réalisé de manière organisée. Ce critère de l'organisation semble avoir pour finalité d'exclure la personne qui passerait un acte de manière fortuite et unique. Inversement, pourrait être qualifiée de professionnel la personne qui déploierait d'importants moyens financiers, juridiques ou encore matériels, aux fins de conclure des contrats avec les consommateurs. Dans le cas des applications traceuses, leur promotion a fait l'objet de sites internet dédiés[178], de pages gouvernementales[179], d'une mise à disposition sur les boutiques en ligne d'application d'entreprises privées[180], de publicités sur les chaînes nationales de télévision, ultérieurement publiées sur des plates-formes vidéo[181]. Il est de ce fait difficilement contestable que derrière

[176] CJUE, 4 octobre 2018, *Kamenova*, C-105/17.
[177] *Ibid*, points 37-38.
[178] Par ex. en France : https://bonjour.tousanticovid.gouv.fr/ ; en Belgique : https://coronalert.be/fr/ ; en Espagne : https://radarcovid.gob.es/fr/node/2 ; au Portugal : https://stayawaycovid.pt/landing-page/ ; en Allemagne : https://www.coronawarn.app/en/ (dernières consultations le 3 juin 2021).
[179] Par ex. en France : https://www.gouvernement.fr/info-coronavirus/tousanticovid ; en Belgique : https://www.info-coronavirus.be/fr/news/coronalert/ (dernières consultations le 3 juin 2021).
[180] Par ex. pour la France : https://play.google.com/store/apps/details?id=fr.gouv.android.stopcovid&hl=en_US&gl=US ; l'Espagne : https://play.google.com/store/apps/details?id=es.gob.radarcovid&hl=en_US&gl=US ; le Portugal : https://play.google.com/store/apps/details?id=fct.inesctec.stayaway&hl=en_US&gl=US ; https://play.google.com/store/apps/details?id=be.sciensano.coronalert&hl=en_US&gl=US (dernières consultations le 3 juin 2021) ;
[181] Par ex. en France : https://www.youtube.com/watch?v=pot3wVMHt0c ; En Belgique :

chacune de ces applications se trouve une logistique importante, tendant à montrer le caractère organisé de leur diffusion.

Ensuite, l'arrêt mentionne que les juridictions nationales doivent vérifier si « *le vendeur dispose d'informations et de compétences techniques relatives aux produits qu'il propose à la vente dont le consommateur ne dispose pas nécessairement, de façon à le placer dans une position plus avantageuse par rapport audit consommateur* ». Certes, la fourniture de ces applications ne s'insère pas dans le cadre d'un contrat de vente. Le critère ne perd pas de son intérêt pour autant dans la mesure où ces applications reposent sur des protocoles informatiques complexes et de grande technicité. Pour que le consommateur comprenne le fonctionnement de ces dernières et les implications relativement à ses données personnelles, il lui faudrait connaître la différence entre le système centralisé et décentralisé[182], puis se livrer à des recherches extensives afin de déterminer si l'application proposée dans son État de résidence relève de l'un ou de l'autre.

Il est de même nécessaire de vérifier « *dans quelle mesure l'acte [la vente en ligne] est liée à l'activité commerciale ou professionnelle du vendeur* ». Le lien entre la fourniture d'une application traceuse et l'activité professionnelle des administrations publiques nationales ne soulève pas de difficulté, puisque les dispositions légales, réglementaires ou contractuelles qui s'y rapportent les désignent expressément comme en étant responsables[183].

Enfin, l'arrêt présente un intérêt important en ce qu'il précise que les critères énumérés dans la décision ne sont ni exhaustifs, ni exclusifs[184]. Selon la Cour, d'autres critères peuvent en effet être pris en compte au vu des « *circonstances pertinentes du cas d'espèce* ». Comme précédemment évoqué, les conditions générales d'utilisation des applications sont parfois fixées par

https://www.youtube.com/watch?v=berbh2Jk7HI (dernières consultations le 3 juin 2021);

[182] Coronavirus contact-tracing: World split between two types of app (disponible au lien suivant : https://www.bbc.com/news/technology-52355028) (dernière consultation le 3 juin 2021) ;

[183] En France : Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « TousAntiCovid » ; En Belgique : Arrêté royal portant exécution de l'arrêté royal n° 44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano ; En Allemagne : https://www.coronawarn.app/assets/documents/cwa-eula-1.3-en.pdf et https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf (dernière consultation le 3 juin 2021) ; En Italie : https://www.immuni.italia.it/pn.htm[l] (dernière consultation le 3 juin 2021) ;

[184] CJUE, 4 octobre 2018, *Kamenova*, préc., point 39 ;

des dispositions réglementaires, unilatéralement décidées et adoptées par les autorités publiques responsables elles-mêmes. Un dernier argument pourrait être sans nul doute l'impuissance du consommateur à influer de quelque manière que ce soit sur les conditions réglementaires d'utilisation des applications, les laissant en outre à la merci d'une éventuelle modification unilatérale des conditions par l'entité publique qui les a fixées.

La finalité des directives considérées étant d'accorder une protection au consommateur se trouvant dans un état d'infériorité vis-à-vis du professionnel, il serait contraire à celle-ci de conclure au non-rattachement de la fourniture de telles applications à l'activité professionnelle des autorités nationales en charge. Pour autant, il reste à mentionner que si le droit de la consommation pourrait et devrait s'appliquer aux applications traceuses « anti-Covid », encore faut-il que ces dernières entrent dans le champ d'application matériel des directives en la matière.

(ii) Les applications traceuses rentrent-elles dans le champ d'application matériel des directives de protection des consommateurs ?

La fourniture d'application traceuse par les autorités publiques a théoriquement vocation à entrer dans le champ d'application des directives considérées. S'appliqueront-elles réellement pour autant ? Les directives 93/13 relatives à la protection contre les clauses abusives, 2005/29 relative à la lutte contre les pratiques commerciales déloyales, 2011/83 relative aux droits des consommateurs et 2019/770 relative à la conformité des contenus et services numériques nécessitent pour leur application la présence d'un consommateur et d'un professionnel. En revanche, leurs spécificités empêcheront parfois l'utilisateur-consommateur de bénéficier pleinement de cette protection, notamment en raison de leur champ d'application matériel. Afin de mesurer l'étendue des droits des consommateurs-utilisateurs, il sera en conséquence nécessaire d'évoquer pour chacune des directives les conditions spécifiques de leur application et de les confronter avec les particularités des applications traceuses.

Premièrement, la directive 93/13 relative aux clauses abusives présente une spécificité liée à son champ d'application pouvant, dans certains États membres, conduire à ce que les utilisateurs ne bénéficient pas de la protection qu'elle met en place. L'article 1er paragraphe 1 de la directive 93/13 pose le principe de son application à tous les contrats passés entre un consommateur et un professionnel. Cependant, le paragraphe 2 admet une limite à ce principe, en ce qu'il ne soumet pas à la protection de la

directive les clauses contractuelles qui reflètent des dispositions législatives ou réglementaires impératives. Cela s'explique notamment par le fait que le législateur européen considère que les dispositions législatives ou réglementaires qui fixent les clauses de contrats avec les consommateurs ne sont pas censées comporter de clauses abusives du fait de leur origine étatique[185]. Les États doivent toutefois s'assurer que des clauses abusives n'y figurent pas, le régime mis en place par la directive devant s'appliquer également aux activités présentant un caractère public[186].

La directive étant d'harmonisation minimale, les États demeurent libres d'adopter des mesures allant plus loin dans la protection que celles contenues dans la directive. On retrouve alors des différences parfois substantielles dans les transpositions nationales de celle-ci. Alors que certains États comme la France ou la Belgique ont fait le choix de soumettre sans distinction les clauses reflétant des dispositions légales ou réglementaires à la protection contre les clauses abusives[187] d'autres, comme le Luxembourg[188], l'Allemagne[189] ou l'Italie[190] ont fait le choix de les en exclure[191].

Alors qu'en France ou en Belgique, l'application de la protection contre les clauses abusives issue de la directive 93/13 ne poserait pas de difficulté, la question serait plus délicate au Luxembourg[192] ou en Italie, en raison

[185] Directive 93/13/CEE, considérant 13 ;
[186] *Ibid*, considérant 14 ;
[187] Tant le code de la consommation français que le code de droit économique belge ne contiennent pas de disposition particulière écartant du contrôle du caractère abusif les clauses reflétant des dispositions légales ou réglementaires impératives, dans les sections dédiées aux clauses abusives.
[188] Article L. 211-5 du code de la consommation luxembourgeois : « *La présente section ne s'applique pas aux clauses contractuelles qui sont fixées directement ou indirectement par des dispositions légales ou réglementaires ainsi que par des dispositions ou des principes des conventions internationales ratifiées par le Luxembourg ou dont l'Union européenne est partie, notamment dans le domaine des transports.* »
[189] Section §307 du BGB, sous-section 3 : « *Les sous-section 1 et 2 ainsi que les sections 308 et 309 s'appliquent uniquement aux clauses standardisées sur la base desquelles des contrats dérogent aux dispositions légales ou les aménagent.* ».
[190] Article 34 § 3 du code de la consommation italien : « *Ne sont pas abusives les clauses qui reproduisent des dispositions légales ou mettent en œuvre des principes contenus dans des convention internationales auxquelles tous les États membres de l'Union européenne ou l'Union européenne elle-même.* »
[191] C'est également le cas du Royaume-Uni qui avait transposé la directive 93/13 dont les dispositions se retrouvent aujourd'hui dans le Consumer Rights Act de 2015. La section 73 exclut ainsi les clauses qui reflètent des dispositions légales, règlementaires ou encore des dispositions et principes issus de conventions internationales auxquelles le Royaume-Uni ou l'Union européenne sont parties.
[192] Si une application devait être lancée au Luxembourg, le pays ayant fait le choix de ne

de l'exclusion pure et simple des clauses issues de dispositions légales ou réglementaires de la protection contre les clauses abusives.

S'agissant de l'Allemagne, la question risque de se poser pour la déclaration de confidentialité du Robert Koch Institute relativement à l'application « Corona Warn App », qui fait une référence expresse aux dispositions du RGPD[193]. La législation allemande sur les clauses abusives ne permet le contrôle du caractère abusif de la clause que dans l'hypothèse où les aménagements contractuels s'écartent des dispositions légales impératives ou supplétives, conformément à l'exclusion de l'article 1, paragraphe 2 de la directive 93/13[194]. Dans la mesure où une clause contractuelle reprend les dispositions du RGPD, est-elle soumise au contrôle de son caractère abusif ? En dépit de son intérêt principalement théorique, la question mérite d'être posée.

L'exclusion des clauses reflétant des dispositions législatives, réglementaires ou issues d'engagements internationaux impératives ou supplétives[195] vaut également pour les législations européennes, comme le rappelle la Commission dans son document d'orientation[196]. Il importe alors de savoir si le RGPD fait partie des règles impératives ou supplétives dont traite l'article 1er de la directive 93/13. Bien que le consentement puisse écarter certaines dispositions du règlement[197], il pose pour l'essentiel des règles qui s'imposent au responsable du traitement des données sans possibilité de s'y soustraire. Il se compose donc de dispositions impératives et supplétives s'appliquant en l'absence de consentement donné par la personne qui fournit ses données. Partant, une clause reflétant les dispositions du RGPD ne devrait pas pouvoir être contrôlée au titre de la législation contre les clauses abusives. Par ailleurs, ainsi que les considérants du règlement l'indiquent

pas produire d'application traceuse « anti-Covid ».

193 V. Déclaration sur la protection des données de l'application « Corona Warn App », sections 3 et 13.

194 Communication de la Commission, Orientations relatives à l'interprétation et à l'application de la directive 93/13/CEE du Conseil concernant les clauses abusives dans les contrats conclus avec les consommateurs (2019/C 323/04), point 1.2.3 ;

195 CJUE, 3 avril 2019, *Aqua Med*, C-266/18, point 33 ; CJUE, 7 décembre 2017, *Woonhaven Antwerpen*, C-446/17, point 25 ; CJUE, 20 septembre 2017, *Andriciuc*, C-186/16, point 29 ; CJUE, 30 avril 2014, *Barclays Bank*, C-280/13, points 31 et 42 ; CJUE, 10 septembre 2014, *Kušionová*, C-34/13, point 77 et CJUE, *RWE Vertrieb*, C-92/11, point 26 ;

196 Communication de la Commission, Orientations relatives à l'interprétation et à l'application de la directive 93/13/CEE du Conseil concernant les clauses abusives dans les contrats conclus avec les consommateurs (2019/C 323/04), point 1.2.4 ;

197 V. par ex., article 9, 18 et 22 du RGPD.

eux-mêmes[198], la protection des données a valeur de droit fondamental au regard de l'article 8 de la Charte des droits fondamentaux de l'Union, ainsi que de l'article 16 du TFUE. On peut, au demeurant, douter qu'en pratique les dispositions du règlement soient susceptibles d'être à l'origine de déséquilibres significatifs ou de clauses illisibles ou ambiguës.

Cela étant et comme l'a indiqué la Cour de Justice, cette exclusion est envisageable uniquement lorsque la clause reflète exactement le contenu d'une disposition législative ou réglementaire[199]. A contrario, une clause qui se baserait sur une disposition législative, règlementaire ou issue d'un engagement international sans pour autant en reprendre exactement le principe, ne saurait être exclue du contrôle de son caractère abusif. Les sections 3 et 13 de la déclaration de confidentialité de l'application allemande renvoient cependant directement aux articles du RGPD et ne pourront pas être contrôlées.

Deuxièmement, le régime mis en place par la directive 2005/29 peut apporter une protection supplémentaire pour l'usager au regard du fonctionnement de l'application. Du fait de la promotion dont ont fait l'objet les applications par les autorités publiques nationales, certaines d'entre elles pourraient être tentées de ne pas mentionner clairement des parties du fonctionnement des applications ou en exagérer les bénéfices afin de pousser leurs usagers à les télécharger. À titre d'exemple, il est possible de citer la pratique réputée trompeuse en toute circonstance, par laquelle le professionnel décrirait faussement le produit comme étant « gratuit »[200]. Les applications fonctionnant par la communication régulière avec les serveurs centraux et nécessitant le téléchargement de textes et images, elles nécessitent pour leur bon fonctionnement un accès au réseau internet et peuvent partant occasionner des frais d'utilisation selon les modalités de l'abonnement téléphonique de l'usager. Cela n'empêche pas pour autant certaines autorités de présenter l'utilisation de l'application comme étant gratuite[201].

[198] RGPD, considérant 1 ;
[199] CJUE, 10 septembre 2014, *Kušionová,* préc. ;
[200] Annexe I, 20), directive 2005/29/UE : « *Décrire un produit comme étant « gratuit », « à titre gracieux », « sans frais » ou autres termes similaires si le consommateur doit payer quoi que ce soit d'autre que les coûts inévitables liés à la réponse à la pratique commerciale et au fait de prendre possession ou livraison de l'article.* »
[201] C'est par exemple le cas de l'application belge « Coronalert », dont la page internet dédiée mentionne la gratuité.

De même, beaucoup d'entre elles mentionnent que l'usager ne sera pas géolocalisé et que l'application ne fonctionne que par l'utilisation de la technologie Bluetooth. Cela étant, sur les Smartphones fonctionnant sous Android, certaines applications nécessitent pour leur utilisation d'activer la géolocalisation du fait de la construction même du système d'exploitation[202]. Certes l'application et ses responsables n'utilisent pas les données GPS des utilisateurs afin de fournir leur service, mais donner l'impression d'une absence totale de géolocalisation est fallacieux. À une époque où une attention particulière est donnée à la question du traçage et de la géolocalisation qui suscitent souvent la méfiance des utilisateurs, il serait légitime d'estimer que l'explication détaillée des procédés techniques employés par l'application soit qualifiée d'information substantielle à transmettre à l'usager. Le fait pour une autorité publique de ne pas se montrer totalement transparente à cet égard devrait alors pouvoir être qualifié de pratique commerciale trompeuse.

Enfin, la directive 2005/29 présente un dernier intérêt du point de vue de l'utilisateur d'une application traceuse. Dans la qualification d'une pratique commerciale déloyale, la directive permet de prendre en compte la vulnérabilité du consommateur[203]. Cette question est d'autant plus importante que les personnes âgées par exemple, constituent une catégorie vulnérable à la fois au regard de l'épidémie et de l'usage de nouvelles technologies[204]. À ce titre, la directive 2005/29 permettrait une prise en

[202] V. le guide à l'usage des développeurs d'applications Android sur la technologie Bluetooth Low Energy, en ce qui concerne les permissions (« *Because discoverable devices might reveal information about the user's location, the device discovery process requires location access* ») ; V. https://developer.android.com/guide/topics/connectivity/bluetooth-le#permissions

[203] Article 5, paragraphe 3 de la directive 2005/29 ;

[204] En France par exemple, les chiffres de l'INSEE tendent à démontrer qu'en 2019, 67,2% des personnes de plus de 75 ans sont en situation « d'illectronisme », c'est-à-dire le fait de ne pas posséder les compétences numériques de base ou de ne pas se servir d'Internet. V. S. Legleye, A. Rolland, « *Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base* », INSEE Première, n°1780, 30 oct. 2019 ; La vulnérabilité ne se limite pourtant pas aux personnes âgées. D'autres facteurs pouvant être pris en compte, ainsi que la Commission l'a rappelé dans son document d'orientation relatif à la directive 2005/29 sur les pratiques commerciales déloyales. V. Document de travail des services de la Commission - Orientations concernant la mise en œuvre / l›application de la directive 2005/29/CE relative aux pratiques commerciales déloyales, accompagnant le document: Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, une approche globale visant à stimuler le commerce électronique transfrontière pour les citoyens et les entreprises d›Europe, SWD/2016/0163 final, point 2.6 ;

compte plus large de l'influence de certaines pratiques lorsqu'elles touchent des personnes âgées, moins à-même de déterminer la nécessité et l'éventuel danger de l'utilisation d'une application traceuse.

Si l'on admet que l'usager peut être considéré comme un « *consommateur* » face à l'entité publique agissant comme professionnel, il reste toutefois à démontrer l'existence d'un « *produit* » d'une part, et d'une « *altération substantielle du comportement économique du consommateur* » relative au produit d'autre part.

Sur la question du « *produit* », l'article 2, c) de la directive 2005/29 adopte une définition particulièrement large : « *tout bien ou service, y compris les biens immobiliers, les droits et les obligations* ». Les applications traceuses « anti-Covid », en ce qu'elles donnent à l'usager de nombreuses informations sur les modes de transmission, les risques de la maladie, des chiffres officiels ou encore un droit à un test prioritaire en cas de contact avec une personne testée positive, semblent pouvoir être qualifiées de « produits » au sens de la directive 2005/29.

Il en va de même pour « *l'altération substantielle du comportement économique du consommateur* ». La directive précise que cette altération substantielle doit être comprise comme le résultat d'une pratique qui amène le consommateur à prendre une décision commerciale qu'il n'aurait pas prise autrement[205]. La gratuité du téléchargement de l'application exclurait-elle la notion de décision commerciale ? La question du lien entre décision commerciale et gratuité a déjà été posée à la Cour de Justice à l'occasion de l'affaire *Trento Sviluppo et Centrale Adriatica*[206]. Dans la décision rendue à son propos, la Cour a répondu que constitue une décision commerciale « *toute décision qui est en lien direct avec celle d'acquérir ou non un produit* » et ce, y compris le seul fait de rentrer dans un magasin[207]. Autrement dit, la notion de décision commerciale au sens de la directive 2005/29 s'éloigne du sens commun de l'expression et n'implique ni contrepartie pécuniaire, ni contrat effectivement conclu. La décision de l'usager d'installer l'application et de l'activer afin de bénéficier des services qu'elle propose pourrait en conséquence être qualifiée de « décision commerciale » au sens de la directive considérée.

[205] Directive 2005/29, article 2, e) ;
[206] CJUE, 19 décembre 2013, *Trento Sviluppo et Centrale Adriatica*, C-281/12 ;
[207] Document de travail des services de la Commission, orientations concernant la mise en œuvre et l'application de la directive 2005/29/CE relative aux pratiques commerciales déloyales, SWD/2016/0163 final, section 2.3 ;

Pour autant, bien que la fourniture d'applications traceuses proposées par les entités publiques puisse entrer dans le champ de la directive 2005/29, la question de l'effectivité de son application se pose. La directive dispose que les États demeurent libres de déterminer les sanctions applicables aux violations des règles qu'elle met en place, pourvu qu'elles soient effectives, proportionnées et dissuasives[208]. Les sanctions varient ainsi d'un État à un autre. Par exemple, au Luxembourg, l'article L. 122-8 du code de la consommation mentionne que ces pratiques sont passibles d'une amende allant de 251 à 120 000 euros. Les contrats conclus à la suite d'une pratique commerciale déloyales sont, eux, susceptibles d'être annulés au titre du même article. En France, la question des sanctions est réglée par les articles L. 132-1 à L. 132-24-2 du code de la consommation français. Ils prévoient entre autres, des peines d'emprisonnement, des amendes pouvant aller jusqu'à 10% du chiffre d'affaires du professionnel établi sur les trois dernières années et, dans certains cas, la nullité du contrat conclu à la suite de pratiques commerciales déloyales. Force est de constater l'inadaptation de ces sanctions au contexte de la fourniture d'application par les autorités nationales. On peine ainsi à imaginer la soumission de l'État à une amende ainsi qu'à des peines d'emprisonnement. La sanction de la nullité du contrat conclu n'est pas plus convaincante en pratique, dans la mesure où l'utilisation est gratuite et peut être cessée à tout moment par l'utilisateur[209].

Cela étant, les entités publiques, au même titre que les entreprises privées, demeurent soumises à l'opinion publique. Pour un État, le fait de violer ouvertement les règles de droit sur lesquelles il repose enverrait un message politique certainement nuisible à la confiance que ses citoyens lui portent. On peut donc supposer - ou du moins, espérer - que les entités

[208] Article 13 de la directive 2005/29 ;

[209] La nullité du contrat implique en principe la remise en état des parties antérieurement à la conclusion du contrat. La question des restitutions prend alors une teinte particulière en ce qu'elle porte sur des données personnelles. Cette hypothèse correspond à l'article 17 du RGPD concernant le droit à l'effacement des données. La personne ayant communiqué ses données personnelles dispose du droit à demander que ces dernières soient effacées, notamment pour assurer le respect d'une obligation légale. Il faut toutefois tempérer notre propos, étant donné que le paragraphe 2 de l'article 17 exclut un tel droit lorsque le traitement des données est nécessaire « *pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ». La lutte contre la pandémie de la Covid-19 pourrait à ce titre justifier que les données soient conservées malgré le prononcé de la nullité du contrat. Il faut noter également que même à supposer que le droit à l'effacement soit applicable en conséquence d'une nullité, il serait en toute hypothèse plus simple et plus rapide pour le consommateur de le demander directement à l'entité responsable du traitement, lorsque la base juridique du traitement est le consentement (ce qui est le cas pour l'application allemande notamment).

publiques s'astreignent d'elles-mêmes au respect des dispositions luttant contre les pratiques commerciales déloyales.

Troisièmement, l'application de la directive 2011/83/UE peut également présenter un intérêt dans le domaine des applications traceuses. Il ne s'agit pas ici du droit de rétractation, en l'espèce peu pertinent du fait de la gratuité du téléchargement et de la faculté pour l'utilisateur de cesser d'utiliser l'application à tout moment[210]. Toutefois, l'obligation d'information à la charge du professionnel peut s'avérer intéressante pour l'utilisateur-consommateur. Les applications traceuses reposent sur la communication et le traitement des données à caractère personnel des utilisateurs et demeurent soumises au RGPD. Seulement, ce règlement n'oblige le responsable à fournir que des informations relatives aux données personnelles et non sur le fonctionnement général de l'application traceuse. Pour sa part, l'obligation d'information imposée au professionnel par la directive 2011/83 apparaît bien plus complète. Certains éléments de fonctionnement de l'application peuvent également être d'intérêt pour l'utilisateur sans pour autant concerner le traitement des données. Cela peut être le cas par exemple pour la mention que des frais supplémentaires peuvent être exigibles à l'utilisation de l'application[211], notamment en ce qui concerne les frais liés à l'utilisation du réseau internet mobile. Cela peut encore être le cas pour l'interopérabilité du contenu numérique avec certains matériels ou logiciels[212], si l'installation ou le fonctionnement de l'application nécessitait une configuration minimale ou encore si son bon fonctionnement était empêché par l'utilisation simultanée d'une autre application. Ce point est par ailleurs d'autant plus important que, à la différence de l'application française, nombre d'applications proposées dans d'autres États tels que l'Allemagne ou l'Italie reposent sur le protocole *Exposure Notification Express*, publié conjointement par Apple et Google et intégré par défaut dans les systèmes d'exploitation des smartphones sous iOS et Android. L'obligation d'information de la directive 2011/83 couvre aussi les fonctionnalités du contenu numérique et les mesures de protection techniques applicables[213], ces dernières étant d'autant plus importantes pour l'utilisateur que les données personnelles en question relèvent de son état de santé.

Enfin, le système mis en place par la directive laisse la possibilité

[210] Sur la question des restitutions, V. nos développements en note 89.
[211] Article 6, e) de la directive 2011/83
[212] *Ibid*, article 6, s)
[213] *Ibid*, article 6, r)

aux juges nationaux d'interpréter largement la notion de « principales caractéristiques du bien ou du service[214] », afin de pouvoir prendre en compte une information non spécifiquement prévue dans la directive mais d'importance aux yeux du consommateur[215].

Il faut noter également que faire entrer les applications traceuses « anti-Covid » dans le champ d'application de la directive ne soulève pas de difficultés particulières. L'acte prévoit lui-même son application aux contenus numériques non fournis sur un support matériel en ce qui concerne l'obligation d'information[216] et l'exclusion des « soins de santé » de l'article 3 ne peut être appliquée aux applications traceuses, dans la mesure où elles ne sont pas fournies par un professionnel de la santé au sens de l'article 3, point a) et f) directive 2011/24/UE.

Au-delà de l'intérêt et de l'applicabilité du régime mis en place par la directive 2011/83, la question de l'effectivité risque également de se poser dans les mêmes termes que pour la directive 2005/29. Ici encore, la directive laissait libre champ aux États pour déterminer les sanctions applicables aux violations des dispositions transposées[217]. Au Luxembourg, l'article L. 222-11 du code de la consommation prévoit une amende allant de 251 à 15 000 euros ainsi qu'une éventuelle nullité du contrat à distance conclu en violation de l'obligation d'information précontractuelle. En France, l'article L. 242-10 prévoit seulement une amende administrative d'un montant allant jusqu'à 15 000 euros. Comme dans le cadre des pratiques commerciales déloyales, les sanctions prévues pour le manquement à l'obligation d'information dans les contrats à distance se révèlent difficilement applicables aux administrations nationales[218]. Il faudra à nouveau espérer que l'entité publique, soucieuse

[214] *Ibid*, article 6, a)
[215] N. Helberger, F. Zuiderveen Borgesius et A. Reyna, "The Perfect match? A closer look at the relationship between EU Consumer Law and Data Protection Law", Common Market Law Review, n°54, 2017, p. 1439
[216] *Ibid*, article 6, 2.
[217] Article 24, 1., de la directive 2011/83
[218] La question de l'effectivité peut aussi se poser sous l'angle des actions en cessation, à même de faire cesser durablement des agissements contraires aux dispositions du code de la consommation. Au Luxembourg, deux associations sont désignées comme représentant l'intérêt collectif des consommateurs, l'Union Luxembourgeoise des Consommateurs (ULC) et l'Automobile Club Luxembourg (ACL), dans le domaine automobile ; V. Communication de la Commission relative à l'article 4, paragraphe 3, de la directive 2009/22/CE du Parlement européen et du Conseil relative aux actions en cessation en matière de protection des intérêts des consommateurs (version codifiée de la directive

de son image auprès des concitoyens, se conforme d'elle-même au respect des dispositions issues de la directive 2011/83 et communique toute information nécessaire à l'utilisateur.

Enfin, on observera que les applications traceuses ne pourront pas être soumises au régime de la récente directive 2019/770/UE. Ce texte exige pour son application que la fourniture du contenu ou service numérique se fasse en contrepartie du paiement d'un prix ou bien contre la fourniture de données personnelles, mais seulement dans l'hypothèse où ces données ne sont pas traitées par le professionnel uniquement afin de fournir le service. En d'autres termes, tant que le professionnel récoltant les données personnelles ne les utilise pas dans un autre but que celui de fournir le service et qu'il en assure lui-même le traitement, la fourniture de l'application demeure en dehors du champ de la directive.

En conclusion, même si les bénéfices que les utilisateurs des applications traceuses peuvent tirer du droit de la consommation apparaissent limités, l'application de ce droit présente tout de même un intérêt à plusieurs égards. On songe notamment à la suppression d'éventuelles clauses abusives incluses dans les conditions générales d'utilisation, à l'obligation d'informer l'utilisateur à propos des services proposés au travers de l'application. On songe encore à la lutte contre d'éventuelles pratiques commerciales déloyales commises par les autorités publiques. La question de l'application du droit de la consommation aux applications traceuses pourrait d'ailleurs prendre de l'ampleur dans les mois et années à venir. Au regard des nouvelles fonctionnalités qui sont susceptibles de leur être ajoutées, elles pourraient devenir des supports numériques importants au recouvrement de la liberté d'aller et de venir. L'idée d'un passeport vaccinal (ou du moins sanitaire), timidement envisagée par les autorités nationales et européennes, vient du reste d'être formalisée dans une proposition de règlement publiée par la Commission[219], dans laquelle transparaît clairement l'intention de le

98/27/CE), concernant les entités qualifiées pour intenter une action au titre de l'article 2 de ladite directive. De manière étonnante par ailleurs, il convient de relever qu'en dépit de la Communication de la Commission précitée dans laquelle elle est citée, le droit national luxembourgeois ne permet pas à l'ULC d'introduire d'action en cessation. L'article L. 320-4 du code de la consommation dispose que les actions en cessation peuvent être introduites par les entités désignées aux articles L. 313-1 et suivants, dont l'ULC ne fait pas partie.

[219] Proposition de Règlement du Parlement Européen et du Conseil relative à un cadre pour la délivrance, la vérification et l'acceptation de certificats interopérables de vaccination, de test et de rétablissement afin de faciliter la libre circulation pendant la pandémie de COVID-19 (certificat vert numérique) ; COM (2021) 130 final

faire reposer sur des technologies numériques[220]. Tout laisse à penser que les applications « anti-Covid » ne sont en réalité que le préambule d'une gestion du risque pandémique toujours plus dépendante de l'information et du numérique.

[220] Outre l'expression de « *certificat vert numérique* » déjà suffisamment évocatrice, il est question à l'article 4 d'une « *infrastructure numérique cadre de confiance permettant la délivrance et la vérification sécurisées des certificats* » mise en place par les États membres, à l'article 8 d'une « *interopérabilité avec les normes internationales et/ou les systèmes technologiques* » et à l'article 9 de la « *protection des données à caractère personnel* ».

II

A Tracing application for Luxembourg? Position paper of the LEGAFIGHT experts' group

1. *Contexte épidémiologique et technique :*

La lutte contre le coronavirus s'inscrit dans un contexte épidémiologique nouveau confrontant nos sociétés à une pandémie faisant peser une pression de gestion des patients sur le système hospitalier ayant conduit à des décisions de confinement des citoyens.

Parmi les différentes mesures permettant à la fois une sortie d'un confinement et un endiguement des chaînes de contagion, l'un des outils communément utilisés est le traçage électronique des contacts, technique ayant fait ses preuves dans le cadre du contrôle du virus Ebola[1]. Ce pistage des contacts a démontré son efficacité même lorsqu'il est effectué manuellement. Toutefois cette forme de traçage se révèle compliquée à mettre en place dans des lieux où la circulation humaine est intense pour plusieurs raisons : elle prend du temps et mobilise du personnel et surtout elle est porteuse d'incertitudes dans la mesure où le traçage basé sur la mémoire humaine des personnes infectées n'est pas fiable. La reconstruction de la chaîne des personnes croisées est sujette à des oublis et des imprécisions. Le pistage électronique s'avère beaucoup plus fiable. Il a du reste permet à certains pays asiatiques d'endiguer la contagion par le virus COVID-19 et de ne pas recourir aux méthodes de confinement (notamment en Corée).

Le traçage électronique peut prendre des formes variées, celui d'un accord entre les opérateurs téléphoniques et les Etats afin d'identifier les clusters de contagion ou bien celui de la mise à disposition des citoyens d'une application traqueuse laquelle ouvre plusieurs options :

- téléchargement nécessaire pour être autoriser à circuler (Chine)
- téléchargement volontaire et basée sur le consentement de la personne (Singapore)

[1] Implementation and management of contact tracing for Ebola virus disease, WHO, Emergency documents, Sept. 2015 disponible sur https://www.who.int/csr/resources/publications/ebola/contact-tracing/en/

- accès aux métadonnées par les services secrets permettant de pister en temps réel les personnes infectées (Israël).

Des options plus respectueuses des libertés fondamentales des citoyens existent toutefois. Elles consistent en l'adoption d'applications dont le but n'est pas de traquer les personnes et de les soumettre éventuellement à l'application de mesures coercitives mais d'applications « traceuses » dont l'objectif est de faciliter le traçage des contacts d'une personne contaminée afin de ralentir la progression de l'épidémie.

De nombreux pays se sont orientés vers la mise en place de ce type d'application traceuse dont l'utilisation est volontaire (l'Allemagne, l'Australie, la Belgique, la France, l'l'Italie, le Royaume-Uni et la Suisse par exemple). Le contexte européen de protection des données fournit d'ores et déjà un cadre légal précis garantissant une stricte protection des droits fondamentaux des citoyens (Charte des droits fondamentaux, Convention européenne des droits de l'homme, Règlement Général sur la Protection des Données). C'est dans ce cadre qu'ont du reste été établis les collectifs de développement d'applications traqueuses : PPEP-PT (Pan-European Privacy-Preserving Proximity Tracing) ou DP-3T[2], (cadre développé par des chercheurs suisses), dont les système de collecte des données basés sur le principe de l'anonymat sont fondés sur le respect des grands principes posés par le Règlement Général sur la Protection des Données (RGPD) : licéité loyauté et transparence dans l'utilisation des données ; minimisation des données (adéquation, pertinence et limitation de leur à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées) ; garantie de leur exactitude ; droits d'accès, de rectification, de suppression et d'objection à leur conservation ; limitation dans le temps de leur conservation ; intégrité et confidentialité, garantie de la sécurité de leur traitement par la personne les traitant, laquelle porte la responsabilité de leur traitement en conformité avec les principes précédemment énoncés (article 5 du RGPD).

[2] https://github.com/DP-3T/documents

2. *Justification de la mise en place d'une application sanitaire traceuse au Grand-Duché de Luxembourg*

Par la voix de son premier ministre, Monsieur Xavier Bettel, le gouvernement luxembourgeois a plusieurs fois exprimé être peu enclin à la mise en place d'une telle application dont il estimait, en avril 2020, qu'elle était dépourvue de base légale[3]. Près d'un an plus tard et avec en toile de fond le projet de règlement relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats interopérables de vaccination, de test et de rétablissement afin de faciliter la libre circulation pendant la pandémie de COVID-19 (certificat vert numérique)[4], le gouvernement luxembourgeois semble moins réticent à la possibilité d'une application permettant de faciliter certaines démarches administratives liées notamment à la possibilité de circuler librement[5]

Le groupe de travail à l'origine du projet LEGAFIGHT prend acte de la position gouvernementale. Il souhaite toutefois souligner que l'étude menée dans le cadre de ce projet démontre que la mise en place d'application traceuses étudiées dans les systèmes juridiques, choisis pour leur similarités culturelles et/ou juridique avec le Grand-Duché, s'est faite dans un cadre respectueux des droits des citoyens. Aucun des systèmes étudiés n'a été le lieu d'atteintes ou de violations des libertés fondamentales des citoyens. Au contraire, les systèmes mis en place, dont la forme varie, tant sur le plan technique (architecture centralisée ou décentralisée) que sur celui de leur encadrement juridique, ont démontré leur capacité à encadrer l'utilisation des applications traceuses et à garantir le respect des libertés individuelles tout en protégeant l'intérêt public. Ainsi, les craintes exprimées par le Président de la Commission consultative des droits de l'Homme, M. Gilbert Pregno, craignant l'émergence d'un scandale « StopCovid Analytica » nous semblent pouvoir être écartées[6]. Depuis le début de la pandémie, que l'on peut dater du mois de février 2020, l'arrivée de « nouvelles vagues » de contamination liées en partie à l'émergence de variants du virus entraînant une plus grande contagiosité de celui-ci démontre que la pandémie ne s'est

[3] Déclaration de Monsieur le Premier Ministre Xavier Bettel lors de la conférence de presse en date du 3 avril 2020. V. https://paperjam.lu/article/app-tracking-moi-j-aime-pas

[4] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0130

[5] https://www.wort.lu/fr/luxembourg/un-pas-vers-une-appli-covid-au-luxembourg-60ac829cde135b92361c9b07

[6] https://ccdh.public.lu/fr/actualites/2020/20200427_Covid_Gilbert_Pregno_Radio_100_7.html

pas éteinte. En l'état des connaissances scientifiques, il semble du reste difficile de prédire quand et comment celle-ci prendra fin. La vaccination de la population risque de se heurter à des plafonds de verre et l'efficacité des vaccins pourrait être mise à mal par l'apparition de nouveaux variants.

L'étude menée dans le cadre du projet LEGAFIGHT met également en lumière l'évolution des fonctionnalités des applications qui, de simples applications traceuses, se sont transformées en instruments d'information sur la pandémie et en supports pour les différents documents numériques liés à la gestion de celle-ci par les Etats (autorisations spéciales de déplacement, résultats de test dits « PCR », certificats de vaccination etc.) et d'accompagnement des patients (facilitation de prise de rendez-vous médicaux liés à la contamination, orientation vers un suivi psychologique). La volonté européenne de s'orienter vers la mise en place d'un certificat numérique afin de faciliter la liberté de circulation des citoyens de l'UE au sein du territoire de l'Union mise à mal par certaines restrictions nationales destinées à limiter la propagation du virus, matérialisée au moment où ces lignes sont écrites par le projet de règlement relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats interopérables de vaccination, de test et de rétablissement afin de faciliter la libre circulation pendant la pandémie de COVID-19 (certificat vert numérique)[7] plaide du reste en ce sens. Une application traceuse aux finalités élargies permettrait le stockage du certificat. Pour toutes ces raisons, la mise en place d'une application sanitaire dont l'une des fonctions serait le traçage des personnes contaminées nous semble toujours d'actualité et pourrait correspondre aux aspirations gouvernementales de faciliter la vie des citoyens et résidents luxembourgeois dans le contexte de la pandémie.

3. *Caractéristiques de l'application sanitaire*

L'application dont nous proposons l'usage serait de type *proximity tracing* ou encore back *tracing* et s'inscrirait dans un cadre technique transparent et « open access » en matière de protection données personnelles[8]. Dans

[7] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0130

[8] Pour un aperçu exhaustif des options étudiées par les différentes Etats Membres, v. le document du Ehealth Network : Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States Version 1.0 15.04.2020

la lignée de l'approche défendue par l'Union Européenne, l'application luxembourgeoise serait basée sur une technologie « *bluetooth low-energy* ». Ces cadres techniques proposant un code open source se recommandent de bonnes pratiques communes s'agissant de la mise en œuvre des applications, dont les modèles peuvent ensuite être déclinés à l'échelle nationale selon les modalités déterminées par les différents gouvernements. Plusieurs pays asiatiques ont opté pour une approche « open-source » de leurs propres applications.

La technologie proposée s'appuierait sur l'interface de programmation d'application (API) existant déjà tant pour le système IOS que pour le système Android. Cette interface servirait de base technique. Une application de traçage fondée sur un système décentralisé ne comportant pas l'envoi de données à un serveur devrait ensuite être développée. Cette approche a été adoptée par l'Allemagne (application Corona Warn-app) et la Belgique (Coronalert). Ces technologies ont été développées dans le respect des exigences européenne en matière de protection des données et en tenant compte des nombreuses recommandations faites par les institutions européennes en la matière.

L'Union Européenne a publié plusieurs documents relatifs à l'usage des applications traqueuses, dont notamment une recommandation à destination des Etats Membres quant aux lignes de conduite à adopter et une « boîte à outil » fournissant des directives sur la mise en œuvre de telles applications. Ces documents soulignent l'importance et la nécessité de l'interopérabilité européenne des solutions, facilitée par le recours à un cadre technologique commun.

Le téléchargement de l'application choisie pour le pistage se ferait sur une base volontaire et le fait de ne pas avoir recours à l'application n'entraînerait aucune conséquence de type légal, ce qui est parfaitement conforme à la position retenue par la Commission dans sa Communication *Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection* (point 3. 3, p. 5 : "*Processing by health authority on the basis of the législation does not change the fact that the individuals remain free to install the app or not and to share data with health authorities. No advers conséquences for the users should therefore occur whenever the app is uninstalled* ").

En pratique, l'usager téléchargerait l'application sur une plateforme de mise à disposition (« store ») ou au moyen d'un QR code communiqué

par le gouvernement. Lors de la première ouverture de l'application, sa finalité ainsi que les modalités du traitement des données personnelles opéré seraient communiquées à l'usager, dont le consentement serait recueilli dans le respect des principes posés par le Règlement Général sur la Protection des Données et la Directive 2002/58. Le signalement de leur contamination par les usagers se ferait de façon volontaire par l'intermédiaire d'une fonctionnalité de l'application.

Deux options peuvent ici être envisagées s'agissant de la façon de notifier les personnes ayant été en contact avec la personne contaminée.

(1) Approche impersonnelle :

Dans le cadre de cette option, le signalement à l'application d'un test positif entraîne l'alerte des personnes ayant été en contact avec la personne contaminée par l'intermédiaire d'une notification impersonnelle envoyée par l'application « anti Covid ». Cette notification ne comporte aucune indication de l'identité de la « personne contact » (pour une description détaillée des systèmes v. *supra Technical Framework*).

(2) Approche personnalisée

Cette option offre en parallèle à l'inspection sanitaire l'accès aux numéros de téléphone de l'usager. La communication du numéro de téléphone se ferait par l'usager. Un enregistrement de ce numéro lui serait proposé au moment de l'installation de l'application, enregistrement qui une fois que l'usager l'aurait explicitement accepté. La véracité du numéro serait vérifiée subséquemment par l'envoi d'un SMS, lequel fournirait un code qui serait rentré dans l'application par l'usager afin de confirmer son identité.

Cette vérification s'inscrit dans le cadre du respect du principe de garantie de l'exactitude des données posé par le RGPD. Le numéro de téléphone serait alors associé à une identité cryptée ID de téléphone qui serait agrégée à une base de données administrée par l'inspection sanitaire. Une fois cette ID attribuée, le téléphone commencerait à enregistrer anonymement (sous forme de numéros ID aléatoires générés par le téléphone) les contacts ayant eu lieu avec d'autres téléphones. Le stockage de ces contacts se fera uniquement sur le téléphone de l'usager.

Dans le cadre de cette approche, l'usager pourrait aussi consentir au transfert des données des personnes avec lesquelles il a été en contact à des fins de décryptage par l'inspection sanitaire. L'inspection sanitaire se

mettrait alors en contact avec ces personnes dans le but de leur expliquer les mesures d'auto-isolation. Cette approche a pour but de rendre plus effective les mesures d'auto-isolation. Le consentement donné au décryptage garantit en outre la transparence du système. Une information personnelle et personnaliséeserait ainsi offerte par l'autorité sanitaire aux contacts de la personne testée positive. Cet accompagnement personnalisé permet d'exprimer les angoisses liées à une éventuelle contamination et de poser des questions relatives aux conséquences de celle-ci. Ce processus s'inscrit dans le cadre des recommandations du Comité Européen de la protection des Données et donc dans le respect du principe de minimisation des données posé par le RGPD[9].

Il convient enfin de souligner que, toujours selon ces recommandations, le stockage des contacts sur le téléphone resterait anonyme, tout comme le resteraient les notifications envoyées à l'usager. Seule l'inspection sanitaire, lorsqu'elle recevrait les contacts cryptés, aurait la possibilité de décrypter et d'accéder aux numéros de téléphone (à l'exclusion de toute autre information) des personnes ayant été en contact avec l'usager testé positif. Enfin tout usager pourrait à tout moment désinstaller l'application et faire valoir ses droits d'accès, de rectification de suppression et d'objection au traitement de ses données.

Cette option est plus intrusive que celle offerte par les modèles belges et allemands mais elle présente en contrepartie la possibilité de ne pas laisser la personne avertie de son statut de « cas contact » seule, d'autant que ce statut ne signifie pas nécessairement qu'une contamination a eu lieu.

Par comparaison avec le système de traçage manuel, ce système de traçage numérique devrait donc permettre (1) d'avoir un traçage des contacts plus exhaustif et (2) de réduire le laps de temps entre le moment où le test de l'usager est identifié comme positif et celui où ses contacts
se mettent en « auto-isolation ».

Le système proposé serait en outre en conformité avec les recommandations émises par la Commission Nationale d'Ethique qui avait indiqué « conseiller au gouvernement d'envisager positivement le traçage informatique et faire l'analyse des moyens techniques et juridiques nécessaires à cet effet »[10] dans

[9] Avis du Président du Comité Européen de la protection des données en date du 14 avril 2020, réf. OUT2020-0028

[10] Prise de position de la Commission nationale d'Ethique (C. N. E.) sur les aides infor-

une prise de position en date du 20 mai 2020 estimant que ce « traçage informatique doit être considéré comme un élément utile »[11], dans la mesure où ce traçage se fait dans le cadre d'un certain nombre de conditions techniques – auxquelles le cadre proposé correspond[12] et juridiques au nombre desquelles :

- le caractère volontaire de l'utilisation de l'application ;
- la protection de ce caractère volontaire ;
- la limitation dans le temps de la durée de vie de l'application (une désactivation automatique de celle-ci étant incorporée dans le système) ;
- la destruction des données traitées dans le cadre de ce système ;
- le traitement minimal des données en fonction de la finalité poursuivie

Le groupe de travail LEGAFIGHT préconise en outre que l'application traceuse ait un domaine opérationnel plus large que celui du seul traçage des contacts. Il serait sans doute à ce titre plus approprié de parler d'application sanitaire (ou de santé) permettant un accès du grand public aux données essentielles relatives à la pandémie. Cet intitulé plus rassurant pourrait conduire à une plus grande confiance du public dans cet outil numérique.

Sur le modèle des applications envisagées dans ce rapport, et sans doute plus spécifiquement sur le modèle de l'application française qui semble la plus complète du point de vue des usagers (v. *supra National report : France*), l'application devrait donner libre accès aux informations suivantes :

Informations relatives au contexte sanitaire :

- nombre de téléchargements de l'application
- nombre de personnes notifiées par l'application
- nombre de personnes déclarées positives
- nombre de nouveaux cas quotidiens,
- indice de reproduction du virus, taux d'incidence,

matiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2 : https://cne.public.lu/dam-assets/fr/publications/avis/Prise-de-position-tra%C3%A7age.pdf, conclusions en page finale.

[11] Prise de position de la Commission nationale d'Ethique (C. N. E.) sur les aides informatiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2 : https://cne.public.lu/dam-assets/fr/publications/avis/Prise-de-position-tra%C3%A7age.pdf

[12] V. le point 1.2. de la Prise de position de la Commission nationale d'Ethique (C. N. E.) sur les aides informatiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2.

- taux de positivité
- taux d'occupation des lits en réanimation
- nouveaux patients en réanimation
- total des personnes vaccinées

L'application devrait aussi fournir des informations relatives aux derniers développements scientifiques intéressant la lutte contre la pandémie (par ex. les vaccins reconnus par l'Agence Européenne du Médicament).

Surtout l'application devrait permettre de télécharger les certificats sanitaires tels que le certificat de vaccination que l'Union européenne entend mettre en place.

La nécessité d'une information claire et transparente des usagers sur la finalité et les modalités du traitement répond en outre aux exigences posées par le Règlement Général sur la Protection des données (et plus particulièrement son article 6 § 1 e)) ainsi que divers textes de protection des consommateurs (sur cette question, v. *supra L'application du droit de la consommation aux applications traceuses*).

Enfin, prenant acte de la proposition émise par la Commission Nationale d'Ethique qui recommande dans sa prise de position sur les aides informatiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2, le groupe de travail LEGAFIGHT propose que la mise en œuvre du traçage numérique soit accompagnée par la mise en place d'un « comité *ad hoc* externe, composé de spécialistes informatiques, de la santé, de la protection des données et d'éthique »[13]. La composition et le mode de fonctionnement de ce comité pourrait s'inspire du modèle belge et plus spécifiquement du Comité interfédéral de testing et tracing (v. *supra National report : Belgium*).

[13] V. le point 1.3. de la Prise de position de la Commission nationale d'Ethique (C. N. E.) sur les aides informatiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2.

4. *Questions juridiques*

La conformité des applications traqueuses au cadre juridique européen a déjà été examinée par la Commission européenne et par le Conseil de l'Europe. Le contrôleur européen de la protection et le Comité européen de la protection des données ont également rendu des avis sur la question.

Tous les points évoqués ci-dessous le seront à la lumière des documents suivants :

- Règlement (EU) 2016/679 (Règlement Général sur la Protection des Données)
- Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État[14]
- Working Party Act 29, Guidelines on consent under Regulation 2016/679, WP259 rev.01
- Directive (CE) 2002/58 sur la protection de la vie privée dans le secteur des communications électroniques (« Directive vie privée et communications électroniques »)
- Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, et – portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle
- - Conseil de l'Europe, Information Documents SG/Inf(2020)11, Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis A toolkit for member states, 07/04/20
- Commission recommendation on a common Union toolbox for

[14] Il est à noter que la loi ne comporte pas de dispositions spécifiques relatives au traitement des données de santé, si ce n'est son article 66 qui intéresse le traitement de données génétiques et n'a pas vocation à s'appliquer s'agissant de l'encadrement légal des applications traceuses.

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)2296 final of 8/04/20 ;
- Avis du Président du Comité Européen de la protection des données en date du 14 avril 2020, réf. OUT2020-0028
- E Health Network : Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States Version 1.0 15.04.2020
- Communication from the Commission Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection C(2020) 2523 final of 16 /04/20
- European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, 19/03/20
- Code de la consommation (art. L. 121-1 à L. 121-8 ; L. 211-2 à L 211-5 et L. 212-1 à L. 212-13)

4.1. *Cadre juridique du fonctionnement de l'application*

a) Cadre normatif

L'application retenue aura comme toute première finalité le « *proximity mapping* » permettant de retracer les contacts d'une personne testée positive. Le choix probable d'une prise de contact personnelle de l'inspection sanitaire avec les personnes ayant croisé le porteur identifié du virus conduira à un décryptage par l'inspection sanitaire des données collectées par l'application. Ces deux caractéristiques techniques doivent dont être au centre de l'analyse ici proposée. Le cadre normatif aura pour vocation de garantir une information claire et transparente relative au fonctionnement de l'application ainsi qu'aux droits des usagers (v. *infra* les recommandations du groupe de travail). La base légale du texte qui pourrait être de nature réglemenatire devrait être l'article 9 (2) (i) du RGPD.

b) Collecte des données :

Au regard de tous les documents exprimant des prises de position de l'Union Européenne et du Conseil de l'Europe, les données collectées par les applications traqueuses doivent être celles nécessaires aux finalités explicites du pistage des contacts ou d'autres usages souhaités en fonction de la politique mise en place (principe de minimisation posé par le RGDP).

Puisque la seule finalité de la collecte est un usage sanitaire permettant de

lutter contre la pandémie et autorisant une sortie de la phase de confinement des populations, le système envisagé est conforme à ces recommandations.

Dans sa Communication C(2020) 2523 final, la Commission européenne se prononce en faveur d'un traitement purement anonyme des données. Toutefois, le RGDP (art. 5) ne pose pas une telle obligation. Le choix de décrypter les données pour contacter les personnes ayant été en contact avec un usager testé positif est donc licite, à la condition que les données décryptées soient traitées selon le principe de la confidentialité (seules les personnes autorisées à y avoir accès peuvent en prendre connaissance) et que le consentement à ce transfert de données nominatives soit donné par l'usager. Cette position est également celle du garant européen des données (Avis du Président du Comité Européen de la protection des données en date du 14 avril). En outre, dans sa Communication C(2020) 2523 final, la Commission envisage le scenario d'un accès aux données par les autorités de santé. Elle ne le désapprouve pas mais privilégie un traitement anonyme du pistage

Du point de vue des droits fondamentaux, eu égard à sa licéité au regard du RGDP et de la Directive 2002/58, ainsi que du fait que le but poursuivi sert à la fois l'intérêt public (endiguement de la pandémie), et l'intérêt privé (accompagnement sanitaire et psychologique des personnes testées positives ou ayant été en contact avec un usager testé positif), le décryptage des données reflète une balance des intérêt conforme aux exigences du Conseil de l'Europe (point 3. 3 du document d'information SG/Inf(2020)11 du Conseil de l'Europe, lequel indique, plus particulièrement au regard du respect à la vie privé que : « *restriction on [it] are only permissible if they are established by law and proportionate to the legitimate aim pursued, including teh protection of health).* Le point 3. 6 de la Communication C(2020) 2523 final de la Commission européenne va également en ce sens, puisqu'il reconnaît que les Etats Membres pourront poursuivre des finalités différentes au travers des applications choisies et que de tels choix sont acceptables lorsque l'information donnée aux usagers relativement à ces dernières est claire et met suffisamment en lumière les spécificité du système qui fait l'objet d'un contrôle (« *the Commission recommends to specify further the purposes* »). Le point central est donc l'obtention d'un consentement éclairé de la part des usagers à la lumière du RGDP et de la « Directive vie privée et communications électroniques ».

c) Consentement :

Il n'est pas inutile de rappeler que l'application retenue sera d'usage volontaire et qu'aucune conséquence légale ne pourra être attachée au choix de ne pas y avoir recours.

Elle respecte donc dans son principe d'utilisation la qualité qui doit être celle du consentement au traitement des données posées par le RGPD.

La mesure du caractère éclairé du consentement se fera à la lumière de l'utilisation ultérieure des données dans le respect des finalités définies. La question de l'information fournie à l'usager est en ce sens est cruciale puisqu'elle relève du respect du principe de transparence. Les informations essentielles à communiquer sont les suivantes : qui recueille les données; comment sont-elles traitées (caractère anonyme ou non) ; qui peut y avoir accès ; combien de temps seront-elles gardées ?

Le système envisagé (collecte de données anonymes, approche personnalisée des personnes en contact avec un usager testé positif dont le nom ne sera pas communiqué) devra être clairement présenté et expliqué aux usagers (art. 12, 13 RGDP et art. 5 de la Directive 2002/58/CE).

L'obtention de leur consentement se ferait par « opting-in », c'est-à-dire acceptation positive de chaque étape du processus : collecte anonymisée et autorisation de décryptage par l'inspection sanitaire. L'usager devra cocher chaque modalité pour les accepter.

Ce processus du consentement respecte les exigences posées par les articles 4 (1), 7 et 9 du RGDP. Sa mise en œuvre concrète devra se faire à la lumière du Working Party Act 29 (éditée par le Comité Européen de la protection des données).

La Commission européenne privilégie l'obtention d'un consentement par « opting-in » (point 3.2. de la Communication C(2020) 2523 final) permet en effet une « modularisation » (granularity) du consentement.

Aucune des applications étudiées dans le cadre de ce projet ne repose sur un système d' « opting out ». Outre les problèmes d'ordre juridique soulevés par une telle option, elle pourrait conduire à susciter une méfiance des utilisateurs potentiels et être un frein à son téléchargement.

Une disposition spécifique quant à un âge minimum pour l'utilisation de l'application serait la bienvenue. Elle permettrait de ne pas laisser la question de la capacité liée à l'âge dans un flou juridique appelant une décision judiciaire (ce choix a par ailleurs été fait en Allemagne, v. *infra* «*National report : Germany*»).

d) droit d'accès, de rectification de suppression et d'objection :

Le système envisagé est licite puisqu'il donne à l'usager le pouvoir de désinstaller l'application à tout moment et celui de demander à ce que les données le concernant soient effacées de la base des données collectées (art. 15, 16, 17 et 18 du RGPD).

4.2. *Traitement et conservation des données*

4.2.1. *Traitement et stockage des données sur le téléphone de l'usager*

Dans le cadre du système envisagé, les données sont traitées de façon totalement anonyme par l'application qui génère des ID éphémères modifiés de façon périodique. Ce système garantit une sécurité contre leur piratage ainsi qu'un total anonymat vis-à-vis des usagers de l'application. Il correspond à un système « décentralisé » approuvé et recommandé par la Commission européenne (point 3. 5 de la Communication C(2020) 2523 final). Tant que l'usager de l'application n'est pas testé positif, les données sont stockées sur son seul appareil. Ce n'est que dans l'hypothèse où il est testé positif que ces dernières seront communiquées à l'inspection sanitaire qui les décryptera et les stockera au sein d'une infrastructure publique.

4.2.2. *Option d'un traitement et stockage des données par l'inspection sanitaire*

Si l'option de la communication des données de contact à l'inspection sanitaire devait être retenue, elle se ferait à l'initiative de l'usager qui a été testé positif. Il utiliserait pour ce faire une fonctionnalité de l'application lui permettant de partager ces données avec l'inspection sanitaire, ce qui, comme il a déjà été souligné auparavant, constitue une double garantie de son consentement au partage des données stockées sur son appareil. Ce système ne contredit donc pas à notre sens les recommandations émises par la Commission européenne dans sa Communication C(2020) 2523 final (point 3. 5). Elle pose toutefois la question de l'absence de consentement des « personnes contact » dont l'anonymat est levé.

Dans le système envisagé, l'inspection sanitaire garantirait toutefois que les données qu'elle recueillerait seraient traitées de façon totalement anonyme vis-à-vis des usagers. L'usager infecté n'a en effet lui-même pas accès à l'identité des personnes avec lesquelles il a été en contact, tout comme ces dernières n'ont pas connaissance de son identité. Ce type de traitement est ainsi conforme aux recommandations formulées par la Commission dans sa Communication C(2020) 2523 final (point 3. 5).

Seule l'inspection sanitaire aurait accès aux données décryptées dans le respect de la finalité de sa mission (endiguement de la pandémie et accompagnement sanitaire et psychologique des personnes testées positives ou ayant été en contact avec un usager testé positif). Ce traitement, lié à la fonctionnalité de l'application envisagée, serait conforme au principe de minimisation du RGDP. La Commission européenne ne s'oppose pas à ce type d'approche dès lors que le traitement des données correspond effectivement à la fonctionnalité choisie (point 3. 6. de la Communication C(2020) 2523 final). Une telle approche pose toutefois la question de son acceptation sociale et comporte le risque de réveiller des polémiques sachant que le thème des applications traceuses peut donner lieu à des réactions de type émotif (sur ce point v. *supra National Report : France*).

4.2.3. *Durée de la conservation des données*

La Commission européenne ainsi que diverses autorités de contrôle nationales plaident en faveur d'une conservation temporaire des données recueillies (point 10 § 3 de la recommandation de la Commission européenne, point 2. 2. du document d'information du Conseil de l'Europe ; p. 11 du Bulletin de veille du comité consultatif national d'éthique français « Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire »).

De façon plus précise, la Commission indique que les données devraient être conservées en tenant compte des exigences médicales ainsi que de la fonctionnalité de l'application choisie. Dans le cadre du système décrit ici, et s'agissant des données relatives aux contact de l'usager testé positif, une période d'un mois correspondant à la période d'incubation entendue de façon large est recommandée (point 3. 7. de la Communication C(2020) 2523 final). Les systèmes allemands et belges ont fait le choix d'une durée de rétention d'une période de 14 jours qui pourrait être reprise par la loi (V. *supra National Report : Belgium* et *National Report : Germany*).

4.2.4. *Contrôle du traitement et du stockage des données par l'inspection sanitaire*

Dans sa communication C(2020) 2523 final, la Commission recommande que le contrôle du traitement des données (contrôle de conformité – *compliance* – avec les exigences légales) soit opéré par l'autorité sanitaire (point 3. 1), et donc, au niveau national, par l'inspection sanitaire. Cette institution devrait travailler en étroite collaboration avec la Commission Nationale de Protection des Données qui devrait être étroitement associée au développement et à la mise en œuvre de l'application (point 3. 10 de la communication C(2020) 2523 final). La Commission Nationale de Protection des Données devrait par ailleurs être en charge de mener l'étude d'impact sur la protection des données relative à un tel système exigée avant sa mise en place par l'article 35 du RGPD.

4.2.5. *Mise en place d'un comité ad hoc*

La mise en place de ce comité correspondrait au souhait émis par la Commission Nationale d'Ethique dans sa prise de position sur les aides informatiques dans la lutte contre la pandémie du Coronavirus SARS-CoV-2 où elle s'exprimait en ces termes : « La mise en œuvre d'un traçage informatique devrait être accompagnée par un comité *ad hoc externe*, composé de spécialistes informatiques, de la santé, de la protection des données et d'éthique, aucune autorité existante – et a fortiori la C.N.E. – n'étant en mesure de s'exprimer sur des applications informatiques concrètes ». Ce comité pourrait soutenir utilement la Commission Nationale de Protection des Données dans les contrôles qu'elle opérerait au sujet de l'application sanitaire et dans les investigations qu'elle pourrait devoir conduire à son propos si elle était saisie de signalements la concernant.

5. *Avis et recommandations du groupe d'experts*

Eu égard à l'analyse précédemment faite, le groupe d'expert :

1/ Prend acte de l'existence de garanties légale suffisantes pour le développement initial d'une application trappeuse au Grand-Duché de Luxembourg.

2/Recommande que :

- Une application sanitaire à finalités variées dont celle du traçage numérique des personnes contaminées et ayant été en contact avec celles-ci reposant sur une architecture de type décentralisé soit mise en place.
- La Commission Nationale de Protection des Données soit en charge de mener l'étude d'impact sur la protection des données relatives à un tel système posée par l'article 35 du RGPD avant sa mise en place.

Un texte national formalisant cet encadrement et précisant certains points du dispositif légal soit proposé et débattu. Une telle approche est du reste prônée par la Commission européenne (Communication C(2020) 2523 final point 3. 3). Ce texte devrait

- Être adopté sur le fondement du Règlement Général de la Protection des Données – article 6.1(e) – et rappeler aux usagers la conformité du système mis en place avec ce texte
- Informer l'usager de l'application du fonctionnement et des finalités de l'application
- Informer l'usager de la durée de conservation des données
- Mettre en place un comité *ad hoc* veillant au bon fonctionnement de l'application
- Indiquer l'autorité en charge du contrôle de la protection des données veillant au respect de la protection de ses données personnelles dans le cadre du système de traçage et de stockage de document sanitaire mis en place et informer l'usager de l'existence d'un comité *ad hoc* veillant au bon fonctionnement de l'application.

Ce texte permettrait de compléter le cadre réglementaire national en tenant compte des questions suscitées par le contexte inédit de la crise sanitaire relative à la pandémie provoquée par le COVID-19 (Loi du 1er août 2018 portant organisation de la Commission nationale pour la

protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État). En apportant des précisions relativement à la question fondamentale de la forme du consentement et des informations et explications à communiquer aux usagers, il contribuerait à l'acceptation du recours à l'application sanitaire par la population et donc à son effectivité et son efficacité. Il garantirait enfin que le droit de la crise ne devienne pas le droit commun en prévoyant l'effacement des données après la fin des mesures d'urgence adoptée par le gouvernement (sur ce point tous les avis convergent, v. dernièrement l'avis du Président du Comité Européen de la protection des données en date du 14 avril 2020, réf. OUT2020-0028).

III

Lessons to be learnt from the crisis
The Rise and Fall (and Rise?) of Tracing Applications

1. *The complexity of legal transplants*

Since the very beginning of the European debate on tracing applications, the East-Asian experience has been taken as a reference model in a quite simplistic manner, without carefully reflecting on the peculiar institutional framework surrounding the use of tracing apps in those systems and conditioning the efficacy of a legal transplant.

First of all, it is worth noting that tracing apps were not the only and not even the most important of the digital solutions adopted in the East with the aim of countering the pandemic. Migration maps created by integrating different sources of data, last generation screening technologies (such as body temperature scans), AI models applied to health data for the purposes of diagnosis and risk prediction, electronic monitoring of home-quarantined individuals, health QR codes, virtual care platforms, robots for personal care in hospitals, all of the above are just some examples of the panoply of digital technologies effectively deployed since the very first stage of the pandemic.

Secondly, to correctly appreciate the effectiveness of East-Asian strategies, one should keep in mind that Covid-19 was just the last episode of a long wave of health crises triggered by contagious diseases experienced in recent times in that region. China, Hong Kong, South Korea were already faced with the need to restructure the whole framework of disease control first in 2002 following the outbreak of the SARS epidemic, and later in 2013 of the MERS (which hit South Korea). This led to a revision and modernization of the respective legislations on disease control, which proved extremely helpful for the fight against Covid-19. In China, the general Law on Prevention and Treatment of Infectious Diseases (1989) was deeply revised in 2004 and later amended in 2013. Together with the 2003 Law on

Emergency Response and the 2003 regulation on Contingent Public Health Emergencies, this statute provided the main legal framework for rapidly adopting a set of wide-ranging measures, such as the blockading of entire areas, cities, or regions of the country, the building of dedicated hospitals, the development of online healthcare platforms (measures rapidly put in place in the cities hit the hardest by the pandemic, such as Wuhan).

In South Korea, the *Act on Infectious Diseases Prevention and Control* was amended in 2015, with the aim of improving the responses to the possible outbreak of new contagious diseases. The new arts. 34 *bis* and 76 *bis* of the Act make massive recourse to various sources of data for tracking purposes possible. In particular, they grant public authorities the power to access a wide gamut of personal data – geolocalisation data, communications metadata, history of purchases and financial data, health data, video surveillance footage – with the aim of tracking the patterns of the disease and informing the public through detailed migration maps. As a result of this background, South Korea and China were extremely fast and efficient in adopting a wide range of measures – physical and digital – as soon as the Covid-19 epidemic erupted. Lastly, it is worth underlining that tracing applications are embedded in a legal framework whose features mark a stark contrast, from several points of view, with the European tradition. Among such features are the following: *a*) quasi-compulsory use of digital tools, as evidenced by the Chinese resort to the QR Code as a requirement to access public places; *b*) loose application of data protection principles vis-à-vis public authorities, as evidenced by the Chinese and Singaporean experience; *c*) adoption of centralised models of tracing applications and access by health authorities to proximity data (Singapore); *d)* strict surveillance and harsh enforcement of quarantine duties.

The rise of tracing applications.

Based on a naive belief that a transplant of tracing applications could work in EU Member States, digital technologies being perceived as a magic tool against the virus, governments were prone to launch digital tracing systems as a way out of the crisis, relying on the assumption that the EU data protection regulation would guarantee both the respect of EU residents' fundamental rights and the efficiency of the system. In many countries, both governments and media presented tracing applications as an important piece of an exit strategy out of the sanitary crisis. The LEGAFIGHT project also considered, when it was launched back in March 2020, tracing

applications as "key instruments in containing the spread of COVID-19 and ending the complete lockdown". The (legal) cultural gap existing between the EU approach of fundamental rights and that of the countries where tracing applications were successfully implemented was known but went probably undervalued as to its capacity to hinder an efficient use of tracing applications. The very protective approach of individual's privacy, which is the essence of the GDPR, proved to be a very efficient safeguard of citizen's fundamental rights. The consent-based approach imposed by the regulation allowed for a careful balancing between the rights of individuals and the public interest. One of the consequences of such privacy-above-all approach was the decision of the producers of the main -Covid-19 tracing app, Google and Apple, to favour a decentralised model: the data concerning the holder of the smartphone and his or her contacts remains strictly under the holder's control. With the exception of France, all the tracing applications studied in this research project were also based on this type of architecture. Only if the user decides to inform on a Covid-19 positivity does the system act by sending alerts to the positive user's contacts.

The fall of tracing applications.

The consent-based solution may not have led to the most efficient result that one would have wished for as to the capacity of tracing applications to combat the pandemic and its disastrous effects. A system relying on individual choices for the success of a public health strategy could nevertheless have worked if people had trust both of the system and the entities managing the data behind the system. Alas, millions of citizens who every second of their daily life provide thousands of personal data to any private on-line business (not only the big-tech giants, but also any provider of apps or of online services), enabling these to profile people in every aspect, raised the alarm over a revised and incumbent version of the Orwellian Big Brother. The individual right to privacy became the antagonist of public health concerns which had to surrender. The cleavage between individualist (and selfish) EU societies and community oriented (and rigidly governed) Eastern ones has become ever wider. The result is that an app that in order to be effective needed to be downloaded and kept constantly in function by at least two thirds of the adult population, in its peak reached not more than 30% of the citizens of a well-organised and disciplined country such as Germany and an average of 20% in the others.

The issue of public trust.

The overall management of the Covid-19 pandemic has raised deep concerns on the ability of government to face and counter such an unprecedented emergency. At the end of the day, the only substantive remedies were those of the past centuries against the plague and deadly fevers: lockdowns and quarantine. The transfer of all substantive powers to central government, the ancillary role of Parliaments, a widespread deference of the judiciary towards the decisions of public authorities, a substantial suspension of constitutional rights (in particular of circulation and assembly), have accompanied and augmented an already existing deteriorated public trust of decision makers. In a democratic system, promotion of public goals passes necessarily through a widespread compliance with the rules introduced. Tracing apps were outside this picture and were seen as only a further burden on an already significantly impaired way-of-life. Furthermore, it is worth reflecting on the fact, registered by many pollsters, that people had shown more confidence in the idea that proximity data were collected by Google and Apple – pursuant to the decentralised model – than by the governments, under the original centralised model. But the reasons for the fall of tracing applications lie not only in the consent-based approach and the distrust citizens show towards governments which requires, incidentally, to be further studied and understood.

Technical inadequacies.

It would appear that one of the essential features of all tracing apps was that the smartphone in a relation of proximity should have activated the Bluetooth application enabling a reciprocal connection. However, Bluetooth is an energy consuming technology which renders it not very attractive, especially for those who are in possession of old devices and are in open spaces. Furthermore, Bluetooth compared to GPS has the advantage of being a less privacy-intrusive technology, as it does not disclose the location of its user, but only the distance and duration of the exposure. Yet, tracing applications based on Bluetooth – a technology developed to make communications between two devices possible – have strong limitations in terms of precision of measurements (more so if the sensors built in the smartphones are not of the latest generation) and are prone to false positives. For instance, the presence of a wall or of a Plexiglas shield between two devices would not be recorded by the system. Lastly, BLE applications are able to detect proximity as long as the smartphone is switched on and carried by its user; if these conditions are not met, then the tracing

app would be unable to detect proximity, both active and passive. It is no wonder, therefore, that alternative solutions, such as cheap wearable devices independent from any smartphone, have been proposed and carefully considered by decision-makers.

Digital divide.

The tracing apps were developed for the current generation of smartphones. This clearly cut out all the holders of less recent devices, and in particular traditional mobile phones, not connected to the internet and very common among elderly persons, the most exposed to infection and to its dire consequences. Obviously, it also cut out all the persons that do not own a cell phone, like children and the very poor.

Organizational failures.

To be effective a tracing app requires an efficient health prevention system around it. Not only is it necessary that the person who has received a positive Covid-19 test result alert the system, but it is necessary that this rapidly detect those who have been in his/her proximity. If the alert arrives many days later the prevention effect is substantially watered down, with a chain reaction: those who have been in contact with a person who results positive will know if they have been infected only several days later, and in the meantime may have infected many others. The Italian experience is illustrative. At least during the first and the second wave of the pandemic, the Italian screening system was under pressure and, due to serious organizational deficiencies, people had to wait long hours to get tested and several days to get the results. This means that an alert were likely to be sent days after the appearance of symptoms. Furthermore, doctors and other personnel in charge of the unlocking of the app and the sending of an alert had not been properly instructed and, in several cases, proved unable to initiate the notification proceeding.

The rise of sanitary applications.

Tracing applications are dead, long live tracing applications! In the end, the only conclusion that can be drawn at this stage of the pandemic is that the pandemic is going to last and that there will be no quick exit out of it. Tracing applications may stay longer with us than originally thought. Reshaped into multifunctional applications, transformed into digital certificates supports (for PCR tests or vaccines), the newly born

sanitary applications may prove eventually useful in the eyes of the public (needless to say, to that part of the population equipped with smartphones) and perceived less intrusive. Besides, the emergence of a new state of mind, that of "pandemic-fatigue", could lead to a better social acceptance of such tracing and informing systems. Finally, tracing applications are just one of the many configurations of e-health systems.

Ever-rising applications: the future of e-health.

Europe is everyday more an ageing society: already one fifth of its population (90 million) is over 65; in a few decades over-80s will be one tenth of the population (50 million). There will be increasing costs for drugs, medical devices and hospitalisation. Citizens should learn now how to manage the health difficulties that they may encounter in older age. One of the lessons that came from tracing apps is that they dramatically increased the digital divide. This can no longer be the case. Together with trust, education on how to use e-health technologies is essential if one wishes to ensure a universal provision of medical services and maintain the excellence in public health services which is a distinctive feature of the European welfare system. This should eventually result in a much more direct relation between each citizen and his/her local health provider, for which "knowing your patient" will become an imperative. Tracing applications are not dead, we said…

Elise Poillot is Full Professor of Civil Law in the University of Luxembourg and has written extensively in the fields of Consumer law and comparative European law. She has spearheaded pan-European research on clinical legal teaching.

Gabriele Lenzini is the Head of the Interdisciplinary Research group in Sociotechnical Cybersecurity (IRiSC) at SnT, University of Luxembourg and is extensively engaged in the modelling, analysis, and design of secure and trustworthy computing systems.

Giorgio Resta is Full Professor of Comparative Law in the Roma Tre University and is the author of numerous books and articles in the field of personality rights. He has recently co-edited an ample commentary to the GDPR, published by Giuffré - Francis Lefebvre.

Vincenzo Zeno-Zencovich is Full Professor of Comparative Law in the Roma Tre University and is author or editor of over twenty volumes devoted to legal issues of ICT, data protection, and media.

Damien Negre is Doctoral researcher in the Department of Law at the University of Luxembourg and his main field of research for the Ph.D thesis is consumer protection.

Legislation

Australia, Privacy Amendment (Public Health Contact Information) Act 2020. No. 44, 2020. An Act to amend the *Privacy Act 1988*, and for related purposes [*Assented to 15 May 2020*]

Australia, Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020, 25th April 2020

Australia - Office of the Australian Information Commissioner (OAIC), Covid 19, 30th June 2020

Australia - Office of the Australian Information Commissioner (OAIC), Privacy obligations regarding COVIDSafe and COVID app data, 30th June 2020

Belgium, Service Public Federal Chancellerie Du Premier Ministre [C – 2020/10437] 25 AOUT 2020. — Accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspections d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID–19 se fondant sur une base de données auprès de Sciensano

Council of Europe, Joint Statement on Digital Contact Tracing, Strasbourg 28th April 2020

Council of Europe, Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, Strasbourg, 30 March 2020

European Union, Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic (Text with EEA relevance). C/2020/4934. *OJ L 227I , 16.7.2020, p. 1–9*

European Union, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01, C/2020/2523, *OJ C 124I , 17.4.2020, p. 1–9, 17th April 2020*

European Union, Commission Recommendation (EU) 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,

European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020

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 Adopted on 21st April 2020

Regulation (EU) 2021/953 of the European Parliament ad of the Council of 14 june 2021 - on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic

Regulation (EU) 2021/954 of the European Parliament ad of the Council of 14 june 2021 - on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third- country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic

France, décret n. 2020-650 du 29 mai 2020 relatif au traitement de donnée dénommé "StopCovid", Jorf n. 0131 du 30 mai 2020

Germany, Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an den Bundesminister für Gesundheit zur Frage, welche Zwecke einer «Corona App» einer gesetzlichen Regelung bedürfen, 13.05.2020.

Italy, Legge 25 giugno 2020 , n. 70, Conversione in legge, con modificazioni, del decreto-legge 30 aprile 2020, n. 28, recante misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché' 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. (20G00088)

Italy, Decreto Legge 30 aprile 2020, n. 28, Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché 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. (20G00046)

Luxembourg, Loi du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant : 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

Luxembourg, Commission nationale pour la protection des données, Délibération n° 13/2020 du 8 juin 2020

United Kingdom, House of Commons and House of Lords, Joint Committee on Human Rights. Human rights and the Government's Response to Covid-19: Digital Contact tracing, 7th May 2020

United Kingdom Information Commissioner's Opinion (ICO), Apple and Google joint initiative on Covid-19 contact tracing technology 2020/01, 17 April 2020

United Kingdom Information Commissioner's Opinion (ICO), COVID-19 Contact tracing: data protection expectations on app development, Statement, 4th May 2020

Australia, Privacy Amendment (Public Health Contact Information) Act 2020. No. 44, 2020. An Act to amend the *Privacy Act 1988*, and for related purposes [*Assented to 15 May 2020*]

The Parliament of Australia enacts:

1 Short title

This Act is the *Privacy Amendment (Public Health Contact Information) Act 2020*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	15 May 2020
2. Schedule 1	The day after this Act receives the Royal Assent.	16 May 2020
3. Schedule 2, item 1	The day after this Act receives the Royal Assent.	16 May 2020
4. Schedule 2, items 2 to 4	At the end of 90 days after the day determined under subsection 94Y(1) of the *Privacy Act 1988* as amended by this Act.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Amendments
Privacy Act 1988
1 Subsection 6(1)
Insert:
communication device means an item of customer equipment (within the meaning of the *Telecommunications Act 1997*).
contact tracing has the meaning given by subsection 94D(6).
COVID app data has the meaning given by subsection 94D(5).
COVIDSafe means an app that is made available or has been made available (including before the commencement of this Part), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.
COVIDSafe user, in relation to a communication device, means the person whose registration data was uploaded from the device when the user was registered through COVIDSafe.
data store administrator means:
(a) for the purposes of a provision of Part VIIIA specified in a determination under section 94Z—the agency specified in that determination (but not to the extent of any limitation in that determination); or
(b) otherwise—the Health Department.
former COVIDSafe user has the meaning given by subsection 94N(2).
Health Department means the Department administered by the Health Minister.
Health Minister means the Minister administering the *National Health Act 1953*.
in contact: a person has been ***in contact*** with another person if the operation of COVIDSafe in relation to the person indicates that the person may have been in the proximity of the other person.
National COVIDSafe Data Store means the database administered by or on behalf of the Commonwealth for the purpose of contact tracing.
registration data, of a person, means the information about the person that was uploaded from a communication device when the person was registered through COVIDSafe.
State or Territory health authority means the State or Territory authority responsible for the administration of health services in a State or Territory.
State or Territory privacy authority means a State or Territory authority that has functions to protect the privacy of individuals (whether or not the authority has other functions).
2 After Part VIII
Insert:
Part VIIIA—Public health contact information
Division 1—Preliminary
94A Simplified outline of this Part
There are several serious offences relating to COVID app data and COVIDSafe. They deal with:

- nonpermitted collection, use or disclosure relating to COVID app data; and
- uploading COVID app data without consent; and
- retaining or disclosing uploaded data outside Australia; and
- decrypting encrypted COVID app data; and
- requiring participation in relation to COVIDSafe.

Other specific obligations relate to deletion of data and what is to happen after the COVIDSafe data period has ended (as determined by the Health Minister).
The general privacy law provided by this Act is applied to the requirements of this Part, in

particular by:

- ensuring that COVID app data is taken to be personal information and breaches of this Part are interferences with privacy; and
- enhancing the Commissioner's role in dealing with eligible data breaches, making assessments and conducting investigations in relation to this Part; and
- enabling the Commissioner to refer matters to, and share information or documents with, State or Territory privacy authorities; and
- providing for this Act to apply to State or Territory health authorities in relation to COVID app data.

This Part imposes on State or Territory health authorities the Act's rules and privacy protections, and Commonwealth oversight, in relation to COVID app data, as Commonwealth property that those authorities receive.

This Part also cancels the effect of Australian laws that are inconsistent with the prohibitions in this Part.

94B Object of this Part

The object of this Part is to assist in preventing and controlling the entry, emergence, establishment or spread of the coronavirus known as COVID19 into Australia or any part of Australia by providing stronger privacy protections for COVID app data and COVIDSafe users in order to:

(a) encourage public acceptance and uptake of COVIDSafe; and

(b) enable faster and more effective contact tracing.

94C Constitutional basis of this Part

Principal constitutional basis

(1) This Part relies on the Commonwealth's legislative powers with respect to matters that are peculiarly adapted to the government of a nation and cannot otherwise be carried on for the benefit of the nation.

Additional operation of this Part

(2) In addition to subsection (1), this Part also has effect as provided by subsections (3) to (5).

(3) This Part also has effect as if a reference in this Part to COVID app data were expressly confined to a reference to COVID app data that was collected or generated for the purposes of quarantine (within the meaning of paragraph 51(ix) of the Constitution).

(4) This Part also has effect as if a reference in this Part to COVID app data were expressly confined to a reference to COVID app data that was collected or generated using a service of a kind to which paragraph 51(v) of the Constitution applies (postal, telegraphic, telephonic and other like services).

(5) This Part also has effect as if it were expressly confined to giving effect to Australia's obligations under the International Covenant on Civil and Political Rights done at New York on 16 December 1966 ([1980] ATS 23), and in particular Article 17 of the Covenant, in relation to COVID app data.

Note: The Covenant is set out in Australian Treaty Series 1980 No. 23 ([1980] ATS 23) and could in 2020 be viewed in the Australian Treaties Library on the AustLII website (www.austlii.edu.au).

Division 2—Offences relating to COVID app data and COVIDSafe

94D Collection, use or disclosure of COVID app data

(1) A person commits an offence if:

(a) the person collects, uses or discloses data; and

(b) the data is COVID app data; and

(c) the collection, use or disclosure is not permitted under this section.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(2) The collection, use or disclosure is permitted if:

(a) the person is employed by, or in the service of, a State or Territory health authority, and the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing; or

(b) the person is:

(i) an officer or employee of the data store administrator; or

(ii) a contracted service provider for a government contract with the data store administrator;

and the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(iii) enabling contact tracing by persons employed by, or in the service of, State or Territory health authorities; or

(iv) ensuring the proper functioning, integrity or security of COVIDSafe or of the National COVIDSafe Data Store; or

(c) in the case of a collection or disclosure of COVID app data—the collection or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i) transferring encrypted data between communication devices through COVIDSafe; or

(ii) transferring encrypted data, through COVIDSafe, from a communication device to the National COVIDSafe Data Store; or

(d) the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of, the Commissioner performing the functions or exercising the powers of the Commissioner under or in relation to this Part; or

(e) the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i) investigating whether this Part has been contravened; or

(ii) prosecuting a person for an offence against this Part; or

(f) in the case of a use of COVID app data by the data store administrator—the use is for the purpose of, and only to the extent required for the purpose of, producing deidentified statistical information about the total number of registrations through COVIDSafe; or

(g) in the case of a use of COVID app data that the data store administrator is required by section 94L to delete—the use consists of access by the data store administrator for the purpose of, and only to the extent required for the purpose of, confirming that the correct data is being deleted.

(3) Subsection (1) does not apply to the collection of COVID app data if:

(a) the collection of the COVID app data:

(i) occurs as part of the collection, at the same time, of data that is not COVID app data (***nonCOVID app data***); and

(ii) is incidental to the collection of the nonCOVID app data; and

(b) the collection of the nonCOVID app data is permitted under an Australian law; and

(c) the COVID app data:

(i) is deleted as soon as practicable after the person becomes aware that it had been collected; and

(ii) is not otherwise accessed, used or disclosed by the person after it was collected.

Note: A defendant bears an evidential burden in relation to the matters in this subsection: see subsection 13.3(3) of the *Criminal Code*.

(4) The admissibility of the nonCOVID app data as evidence in any proceedings is not affected by the incidental collection of the COVID app data, or by the subsequent deletion of the COVID app data as required by subparagraph (3)(c)(i).

(5) ***COVID app data*** is data relating to a person that:

(a) has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe; and

(b) either:

(i) is registration data; or

(ii) is stored, or has been stored (including before the commencement of this Part), on a communication device.

However, it does not include:

(c) information obtained, from a source other than directly from the National COVIDSafe Data Store, in the course of undertaking contact tracing by a person employed by, or in the service of, a State or Territory health authority; or

(d) deidentified statistical information about the total number of registrations through COVIDSafe that is produced by:

(i) an officer or employee of the data store administrator; or

(ii) a contracted service provider for a government contract with the data store administrator.

(6) ***Contact tracing*** is the process of identifying persons who have been in contact with a person who has tested positive for the coronavirus known as COVID19, and includes:

(a) notifying a person that the person has been in contact with a person who has tested positive for the coronavirus known as COVID19; and

(b) notifying a person who is a parent, guardian or carer of another person that the other person has been in contact with a person who has tested positive for the coronavirus known as COVID19; and

(c) providing information and advice to a person who:

(i) has tested positive for the coronavirus known as COVID19; or

(ii) is a parent, guardian or carer of another person who has tested positive for the coronavirus known as COVID19; or

(iii) has been in contact with a person who has tested positive for the coronavirus known as COVID19; or

(iv) is a parent, guardian or carer of another person who has been in contact with a person who has tested positive for the coronavirus known as COVID19.

94E COVID app data on communication devices

A person commits an offence if:

(a) the person uploads, or causes to be uploaded, data from a communication device to the National COVIDSafe Data Store; and

(b) the data is COVID app data; and

(c) consent to the upload has not been given by:

(i) the COVIDSafe user in relation to that device; or

(ii) if the COVIDSafe user is unable to give consent—a parent, guardian or carer of the COVIDSafe user; or

(iii) if the COVIDSafe user has requested a parent, guardian or carer of the COVIDSafe user to act on the COVIDSafe user's behalf—that parent, guardian or carer.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

94F COVID app data in the National COVIDSafe Data Store

(1) A person commits an offence if:

(a) the person retains data on a database outside Australia; and

(b) the data is COVID app data that has been uploaded from a communication device to the National COVIDSafe Data Store.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(2) A person commits an offence if:

(a) the person discloses data to another person who is outside Australia; and

(b) the data is COVID app data that has been uploaded from a communication device to the National COVIDSafe Data Store; and

(c) the person is not a person who:

(i) is employed by, or in the service of, a State or Territory health authority; and

(ii) discloses the data for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

94G Decrypting COVID app data

A person commits an offence if:

(a) the person decrypts encrypted data; and

(b) the data is COVID app data that is stored on a communication device.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

94H Requiring the use of COVIDSafe

(1) A person commits an offence if the person requires another person to:

(a) download COVIDSafe to a communication device; or

(b) have COVIDSafe in operation on a communication device; or

(c) consent to uploading COVID app data from a communication device to the National COVIDSafe Data Store.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(2) A person commits an offence if the person:

(a) refuses to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or

(b) takes adverse action (within the meaning of the *Fair Work Act 2009*) against another person; or

(c) refuses to allow another person to enter:

(i) premises that are otherwise accessible to the public; or

(ii) premises that the other person has a right to enter; or

(d) refuses to allow another person to participate in an activity; or

(e) refuses to receive goods or services from another person, or insists on providing less monetary consideration for the goods or services; or

(f) refuses to provide goods or services to another person, or insists on receiving more monetary consideration for the goods or services;

on the ground that, or on grounds that include the ground that, the other person:

(g) has not downloaded COVIDSafe to a communication device; or

(h) does not have COVIDSafe in operation on a communication device; or

(i) has not consented to uploading COVID app data from a communication device to the National COVIDSafe Data Store.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

(3) To avoid doubt:

(a) subsection (2) is a workplace law for the purposes of the *Fair Work Act 2009*; and

(b) the benefit that the other person derives because of an obligation of the person under subsection (2) is a workplace right within the meaning of Part 31 of that Act.

94J Extended geographical jurisdiction for offences

Section 15.1 (extended geographical jurisdiction—category A) of the *Criminal Code* applies to all offences against this Division.

Division 3—Other obligations relating to COVID app data and COVIDSafe

94K COVID app data not to be retained

The data store administrator must take all reasonable steps to ensure that COVID app data is not retained on a communication device:

(a) for more than 21 days; or

(b) in any case in which it is not possible to comply with paragraph (a) within 21 days—for longer than the shortest practicable period.

94L Deletion of registration data on request

(1) If the COVIDSafe user or former COVIDSafe user in relation to a communication device, or a parent, guardian or carer of that person, requests the data store administrator to delete any registration data of the person that has been uploaded from the device to the National COVIDSafe Data Store, the data store administrator:

(a) must take all reasonable steps to delete the data from the National COVIDSafe Data Store as soon as practicable; and

(b) if it is not practicable to delete the data immediately—must not use or disclose the data for any purpose.

(2) A request under subsection (1) may only be made by a parent, guardian or carer of the COVIDSafe user if:

(a) the COVIDSafe user is unable to make a request under subsection (1); or

(b) the COVIDSafe user has requested that parent, guardian or carer to act on the COVIDSafe user's behalf.

(3) Subsection (1) does not:

(a) prevent the data store administrator from accessing data for the purpose of, and only to the extent required for the purpose of, confirming that the correct data is being deleted; or

(b) require the data store administrator to delete from the National COVIDSafe Data Store data relating to the person that:

(i) was uploaded from another communication device in relation to which another person is a COVIDSafe user; and

(ii) was collected through the other device interacting with the device mentioned in subsection (1).

(4) This section does not apply to data that is deidentified.

94M Deletion of data received in error

A person who receives COVID app data in error must, as soon as practicable:

(a) delete the data; and

(b) notify the data store administrator that the person received the data.

94N Effect of deletion of COVIDSafe from a communication device

(1) The data store administrator must not collect from a person, through a particular communication device, COVID app data relating to the person if the person is a former COVIDSafe user in relation to that device.

(2) A person is a ***former COVIDSafe user***, in relation to a communication device, at a particular time if:

(a) COVIDSafe has been deleted from the device in relation to which the person was the COVIDSafe user; and

(b) after COVIDSafe was last deleted from that device—COVIDSafe has not been downloaded to that device.

94P Obligations after the end of the COVIDSafe data period

(1) After the end of the day determined under subsection 94Y(1), the data store administrator must not:

(a) collect any COVID app data; or

(b) make COVIDSafe available to be downloaded.

(2) As soon as reasonably practicable after the end of the day determined under subsection 94Y(1), the data store administrator must delete all COVID app data from the National COVIDSafe Data Store.

(3) As soon as reasonably practicable after the deletion, the data store administrator must:

(a) inform the Health Minister and the Commissioner that all COVID app data has been deleted from the National COVIDSafe Data Store; and

(b) take all reasonable steps to inform all COVIDSafe users (other than former COVIDSafe users) in relation to communication devices that:

(i) all COVID app data has been deleted from the National COVIDSafe Data Store; and

(ii) COVID app data can no longer be collected; and

(iii) they should delete COVIDSafe from their communication devices.

Division 4—Application of general privacy measures

94Q COVID app data is taken to be personal information

COVID app data relating to an individual is taken, for the purposes of this Act, to be personal information about the individual.

94R Breach of requirement is an interference with privacy

(1) An act or practice in breach of a requirement of this Part in relation to an individual constitutes an act or practice involving an interference with the privacy of the individual for the purposes of section 13.

Note: The act or practice may be the subject of a complaint under section 36.

(2) Subsections 7(1A) and (1B) do not limit what is taken to be an act or practice for the purposes of subsection (1) of this section, or for the purposes of the application of this Act in relation to an interference with the privacy of an individual involving a breach of a requirement of this Part.

94S Breach of requirement may be treated as an eligible data breach

(1) For the purposes of this Act, if:

(a) the data store administrator; or

(b) an officer or employee of the data store administrator; or

(c) a contracted service provider for a government contract with the data store

administrator;
breaches a requirement of this Part in relation to COVID app data:

(d) the breach is taken to be an eligible data breach by the data store administrator; and

(e) an individual to whom the data relates is taken to be at risk from the eligible data breach.

(2) For the purposes of this Act, if:

(a) a State or Territory health authority; or

(b) person employed by, or in the service of, the State or Territory health authority;

breaches a requirement of this Part in relation to COVID app data:

(c) the breach is taken to be an eligible data breach by the State or Territory health authority; and

(d) an individual to whom the data relates is taken to be at risk from the eligible data breach.

(3) Part IIIC applies in relation to such a breach as if:

(a) subsection 26WE(3) and sections 26WF, 26WH and 26WJ did not apply in relation to the breach; and

(b) Subdivision B of Division 3 of that Part:

(i) required the data store administrator, or State or Territory health authority, to notify the Commissioner that there were reasonable grounds to believe that there had been an eligible data breach; and

(ii) only required compliance with sections 26WK and 26WL in relation to the breach if the Commissioner required the administrator or authority so to comply; and

(c) sections 26WN, 26WP, 26WQ, 26WS and 26WT did not apply in relation to the breach.

(4) Without limiting the circumstances in which the Commissioner may, under subparagraph (3)(b)(ii), require the administrator or authority so to comply, the Commissioner must so require if:

(a) the Commissioner is satisfied that the breach may be likely to result in serious harm to any of the individuals to whom the information relates; and

(b) subsection (5) does not apply.

(5) The Commissioner may decide not to require compliance, or to allow an extended period for compliance, if the Commissioner is satisfied on reasonable grounds that requiring compliance, or requiring compliance within the ordinary period for compliance, would not be reasonable in the circumstances, having regard to the following:

(a) the public interest;

(b) any relevant advice given to the Commissioner by:

(i) an enforcement body; or

(ii) the Australian Signals Directorate;

(c) such other matters (if any) as the Commissioner considers relevant.

(6) Paragraph (5)(b) does not limit the advice to which the Commissioner may have regard.

94T Commissioner may conduct an assessment relating to COVID app data

(1) The Commissioner's power under section 33C to conduct an assessment includes the power to conduct an assessment of whether the acts or practices of an entity or a State or Territory authority in relation to COVID app data comply with this Part.

(2) Without limiting subsection 33C(2), if:

(a) the Commissioner is conducting under that subsection an assessment of a matter of a kind mentioned in subsection (1) of this section; and

(b) the Commissioner has reason to believe that an entity or a State or Territory authority being assessed has information or a document relevant to the assessment;

the Commissioner may, by written notice, require the entity or authority to give the information or produce the document within the period specified in the notice, which must not be less than 14 days after the notice is given to the entity or authority.

Note: For a failure to give information etc., see section 66.

94U Investigation under section 40 to cease if COVID data offence may have been committed

(1) This section applies if, in the course of an investigation under section 40, the Commissioner forms the opinion that:

(a) an offence against Division 2 of this Part; or

(b) an offence against section 6 of the *Crimes Act 1914*, or section 11.1, 11.2, 11.4 or 11.5 of the *Criminal Code*, being an offence that relates to an offence against that Division;

may have been committed.

(2) The Commissioner must:

(a) inform the Commissioner of Police or the Director of Public Prosecutions of that opinion; and

(b) in the case of an investigation under subsection 40(1), give a copy of the complaint to the Commissioner of Police or the Director of Public Prosecutions, as the case may be; and

(c) subject to subsection (5) of this section, discontinue the investigation except to the extent that it concerns matters unconnected with the offence that the Commissioner believes may have been committed.

(3) If the Commissioner of Police or the Director of Public Prosecutions:

(a) has been informed of the Commissioner's opinion under paragraph (2)(a); and

(b) decides that the matter will not be, or will no longer be, the subject of proceedings for an offence;

the Commissioner of Police or the Director of Public Prosecutions, as the case requires, must give a written notice to that effect to the Commissioner.

(4) If the Commissioner of Police or the Director of Public Prosecutions:

(a) has been informed of the Commissioner's opinion under paragraph (2)(a); and

(b) is satisfied that an investigation relating to the matter, or proceedings for an offence relating to the matter, will not be jeopardised, or otherwise affected, by continuation of the Commissioner's investigation;

the Commissioner of Police or the Director of Public Prosecutions, as the case requires, may give a written notice to that effect to the Commissioner.

(5) Upon receiving notice under subsection (3) or (4) the Commissioner may continue the investigation discontinued under paragraph (2)(c).

94V Referring COVID data matters to State or Territory privacy authorities

(1) If:

(a) a complaint has been made under section 36 about an act or practice that may involve a breach of a requirement of this Part; and

(b) before the Commissioner commences, or after the Commissioner has commenced, to investigate the matter, the Commissioner forms the opinion that:

(i) the complainant has made, or could have made, a complaint relating to

that matter to a State or Territory privacy authority; and

(ii) that matter could be more conveniently or effectively dealt with by that State or Territory authority;

the Commissioner may decide not to investigate the matter, or not to investigate the matter further.

(2) If the Commissioner so decides, the Commissioner must:

(a) transfer the complaint to that State or Territory authority; and

(b) give notice in writing to the complainant stating that the complaint has been so transferred; and

(c) give to that State or Territory authority any information or documents that relate to the complaint and are in the possession, or under the control, of the Commissioner.

(3) A complaint transferred under subsection (2) is taken, for the purposes of this Act, to have been made to that State or Territory authority.

94W Commissioner may share information with State or Territory privacy authorities

(1) Subject to subsection (2), the Commissioner may share information or documents with a State or Territory privacy authority:

(a) for the purpose of the Commissioner exercising powers, or performing functions or duties under this Act in relation to the requirements of this Part; or

(b) for the purpose of the State or Territory privacy authority exercising its powers, or performing its functions or duties.

(2) The Commissioner may only share information or documents with a State or Territory privacy authority under this section if:

(a) the information or documents were acquired by the Commissioner in the course of exercising powers, or performing functions or duties, under this Act; and

(b) the Commissioner is satisfied on reasonable grounds that the State or Territory privacy authority has satisfactory arrangements in place for protecting the information or documents.

(3) To avoid doubt, the Commissioner may share information or documents with a State or Territory privacy authority under this section whether or not the Commissioner is transferring a complaint or part of a complaint to the authority.

94X Application to State or Territory health authorities

(1) This Act applies in relation to a State or Territory health authority, as if the authority were an organisation, to the extent that the authority deals with, or the activities of the authority relate to, COVID app data.

(2) However, subsection (1) does not, in relation to a State or Territory health authority:

(a) have the effect of applying Australian Privacy Principle 9 in relation to a government related identifier that has been assigned by that State or Territory or by a State or Territory authority of that State or Territory; or

(b) have the effect of applying this Act in relation to data or information that is not COVID app data.

Division 5—Miscellaneous

94Y Determining the end of the COVIDSafe data period

(1) Subject to subsection (2), the Health Minister must, by notifiable instrument, determine a day if the Health Minister is satisfied that, by that day, use of COVIDSafe:

(a) is no longer required to prevent or control; or

(b) is no longer likely to be effective in preventing or controlling;

the entry, emergence, establishment or spread of the coronavirus known as COVID19 into

Australia or any part of Australia.

(2) The Health Minister must not make a determination under subsection (1) unless the Health Minister has consulted, or considered recommendations from, the Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee.

(3) The Commonwealth Chief Medical Officer or the Australian Health Protection Principal Committee may recommend to the Health Minister that the Health Minister make a determination under subsection (1).

94Z Agencies may be determined to be data store administrator

(1) The Secretary of the Health Department may, by notifiable instrument, determine that a particular agency is the data store administrator for the purposes of one or more provisions of this Part specified in the determination.

(2) The determination may limit the extent to which the agency is the data store administrator for those purposes.

(3) The Secretary of the Health Department must not determine under subsection (1) that any of the following is the data store administrator:

(a) an enforcement body mentioned in paragraph (a) to (ea) of the definition of ***enforcement body*** in subsection 6(1);

(b) an intelligence agency;

(c) the Australian GeospatialIntelligence Organisation;

(d) the Defence Intelligence Organisation.

94ZA Reports on operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store

(1) The Health Minister must, as soon as practicable after:

(a) the end of the 6 month period starting on the commencement of this Part; and

(b) the end of each subsequent 6 month period (if any) starting on or before the day determined under subsection 94Y(1);

cause a report to be prepared on the operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store during that 6 month period.

Note: Section 94D prevents the inclusion of COVID app data in the report. It would not be a permitted collection, use or disclosure under subsection 94D(2).

(2) If the day determined under subsection 94Y(1) occurs during the 6 month period starting on the commencement of this Part, the report under subsection (1) of this section relating to that period must be prepared within 3 months after that day.

(3) The Health Minister must cause copies of a report prepared under subsection (1) to be laid before each House of the Parliament within 15 sitting days of that House after the completion of the preparation of the report.

94ZB Reports by the Commissioner

(1) The Commissioner must, as soon as practicable after:

(a) the end of the 6 month period starting on the commencement of this Part; and

(b) the end of each subsequent 6 month period (if any) starting on or before the day determined under subsection 94Y(1);

cause a report to be prepared on the performance of the Commissioner's functions, and the exercise of the Commissioner's powers, under or in relation to this Part during the period.

Note: Section 94D prevents the inclusion of COVID app data in the report. It would not be a permitted collection, use or disclosure under subsection 94D(2).

(2) If the day determined under subsection 94Y(1) occurs during the 6 month period starting on the commencement of this Part, the report under subsection (1) of this section relating to that period must be prepared within 3 months after that day.

(3) The Commissioner must publish a report prepared under subsection (1) on the Commissioner's website.

(4) This section does not affect the matters that section 30 of the *Australian Information Commissioner Act 2010* requires the Commissioner to include in an annual report.

94ZC COVID app data remains property of the Commonwealth

COVID app data is the property of the Commonwealth, and remains the property of the Commonwealth even after it is disclosed to, or used by:

(a) a State or Territory health authority; or

(b) any other person or body (other than the Commonwealth or an authority of the Commonwealth).

94ZD Operation of other laws

(1) This section cancels the effect of a provision of any Australian law (other than this Part) that, but for this section, would have the effect of permitting or requiring conduct, or an omission to act, that would otherwise be prohibited under this Part.

(2) However, the cancellation does not apply to a provision of an Act if the provision:

(a) commences after this Part commences; and

(b) expressly permits or requires the conduct or omission despite the provisions of this Part.

Schedule 2—Repeals

Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020

1 The whole of the instrument

Repeal the instrument.

Privacy Act 1988

Note: The repeals made by items 2 and 3 of this Schedule commence at the end of 90 days after the day determined under subsection 94Y(1) of the *Privacy Act 1988* as amended by this Act.

2 Subsection 6(1)

Repeal the following definitions:

(a) definition of ***communication device***; (b) definition of ***contact tracing***; (c) definition of ***COVID app data***; (d) definition of ***COVIDSafe***; (e) definition of ***COVIDSafe user***; (f) definition of ***data store administrator***; (g) definition of ***former COVIDSafe user***; (h) definition of ***Health Department***; (i) definition of ***Health Minister***; (j) definition of ***in contact***; (k) definition of ***National COVIDSafe Data Store***; (l) definition of ***registration data***; (m) definition of ***State or Territory health authority***; (n) definition of ***State or Territory privacy authority***.

3 Part VIIIA

Repeal the Part.

4 Transitional

After the commencement of this item:

(a) the powers of the Commissioner under or in relation to Part VIIIA of the *Privacy Act 1988* as amended by this Act continue to apply in relation to matters that arose under or in relation to that Part before that commencement; and

(b) any obligations of the Health Minister or the Commissioner under that Part relating to a report continue to apply;

as if the repeals made by items 2 and 3 of this Schedule had not been made.

Australia, Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020, 25th April 2020

I, Greg Hunt, Minister for Health, make the following determination.
Dated
25 April 2020
Greg Hunt
Minister for Health

Part 1—Preliminary

1 Name

This instrument is the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020*.

2 Commencement

(1)

Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. The whole of this instrument	11.59 pm (by legal time in the Australian Capital Territory) on the day this instrument is registered.	25 April 2020

Note:
This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2)

Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under subsection 477(1) of the *Biosecurity Act 2015*.

4 Object

The object of this instrument is to make contact tracing faster and more effective by encouraging public acceptance and uptake of COVIDSafe.

5 Definitions

Note: A number of expressions used in this instrument are defined in the *Biosecurity Act 2015*, including the following:
(a) Australian law;
(b) Health Department;
(c) State or Territory body.

In this instrument:
contact tracing has the meaning given by subsection 6(4).
COVID app data has the meaning given by subsection 6(3).
COVIDSafe has the meaning given by paragraph 6(3)(a).
deidentified: information is ***deidentified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
in contact: a person has been ***in contact*** with another person if the operation of COVIDSafe in relation to the person indicates that the person may have been in the proximity of the other person.
mobile telecommunications device means an item of customer equipment (within the meaning of the *Telecommunications Act 1997*) that is used, or is capable of being used, in connection with a public mobile telecommunications service (within the meaning of that Act).
National COVIDSafe Data Store means the database administered by or on behalf of the Commonwealth for the purpose of contact tracing.
State or Territory health authority means the State or Territory body responsible for the administration of health services in a State or Territory.

Part 2—Requirements

6 Collection, use or disclosure of COVID app data

(1)
A person must not collect, use or disclose COVID app data except as provided by subsection (2).
(2)
Subsection (1) does not prevent a person from collecting, using or disclosing COVID app data if:
(a)
the collection, use or disclosure:
(i)
is by a person employed by, or in the service of, a State or Territory health authority; and
(ii)
is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing; or
(b)
the collection, use or disclosure is by an officer, employee or contractor of the Health Department or the Digital Transformation Agency for the purpose of, and only to the extent required for the purpose of:
(i)
enabling contact tracing by persons employed by, or in the service of, State or Territory health authorities; or
(ii)
ensuring the proper functioning, integrity or security of COVIDSafe or of the National COVIDSafe Data Store; or
(c)
in the case of a collection or disclosure of COVID app data—the collection or disclosure is for the purpose of, and only to the extent

required for the purpose of:

(i)

transferring encrypted data between mobile telecommunications devices through COVIDSafe; or

(ii)

transferring encrypted data, through COVIDSafe, from a mobile telecommunications device to the National COVIDSafe Data Store; or

(d)

the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i)

investigating whether a requirement of this determination has been contravened; or

(ii)

prosecuting a person for an offence against section 479 of the *Biosecurity Act 2015* in relation to a contravention of this determination; or

(e)

in the case of a use of COVID app data—the use is for the purpose of, and only to the extent required for the purpose of, producing statistical information that is deidentified.

Note: The *Privacy Act 1988* continues to apply except to the extent that it is inconsistent with this determination: see subsection 477(5) of the *Biosecurity Act 2015*.

(3)

COVID app data is data relating to a person that:

(a)

has been collected or generated through the operation of an app (***COVIDSafe***) that is made available, by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing; and

(b)

is, or has been, stored on a mobile telecommunications device.

However, it does not include information obtained, from a source other than the National COVIDSafe Data Store, in the course of undertaking contact tracing by a person employed by, or in the service of, a State or Territory health authority.

(4)

Contact tracing is the process of identifying persons who have been in contact with a person who has tested positive for the coronavirus known as COVID19, and includes:

(a)

notifying a person that the person has been in contact with a person who has tested positive for the coronavirus known as COVID19; and

(b)

notifying a person who is responsible for another person that the other person has been in contact with a person who has tested positive for the

coronavirus known as COVID19; and

(c)

providing information and advice to a person who:

(i)

has tested positive for the coronavirus known as COVID19; or

(ii)

is responsible for another person who has tested positive for the coronavirus known as COVID19; or

(iii)

has been in contact with a person who has tested positive for the coronavirus known as COVID19; or

(iv)

is responsible for another person who has been in contact with a person who has tested positive for the coronavirus known as COVID19.

7 Treatment of COVID app data

COVID app data on mobile telecommunications devices

(1)

A person must not upload COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store except with the consent of the person who has possession or control of the device.

(2)

A person must not cause COVID app data (other than initial registration data or a unique identifier) to be retained on a mobile telecommunications device for more than 21 days.

COVID app data in the National COVIDSafe Data Store

(3)

If COVID app data is uploaded from a mobile telecommunications device to the National COVIDSafe Data Store, a person must not:

(a)

retain the data on a database outside Australia; or

(b)

disclose the data to a person outside Australia.

(4)

Paragraph (3)(b) does not apply to a disclosure by a person employed by, or in the service of, a State or Territory health authority if the disclosure is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing.

(5)

The Commonwealth must cause COVID app data in the National COVIDSafe Data Store to be deleted after the COVID19 pandemic has concluded.

Note: The requirements in this section will override any obligation under an Australian law to retain data for a longer period: see subsection 477(5) of the *Biosecurity Act 2015*.

8 Decrypting COVID app data

A person must not decrypt encrypted COVID app data that is stored on a

mobile telecommunications device.

9 Coercing the use of COVIDSafe

(1)

A person must not require that another person:

(a)

download COVIDSafe to a mobile telecommunications device; or

(b)

have COVIDSafe in operation on a mobile telecommunications device; or

(c)

consent to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

(2)

A person must not:

(a)

refuse to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or

(b)

take adverse action (within the meaning of the *Fair Work Act 2009*) against another person; or

(c)

refuse to allow another person to enter premises; or

(d)

refuse to allow another person to participate in an activity; or

(e)

refuse to receive goods or services from another person; or

(f)

refuse to provide goods or services to another person;

on the ground that, or on grounds that include the ground that, the other person:

(g)

has not downloaded COVIDSafe to a mobile telecommunications device; or

(h)

does not have COVIDSafe in operation on a mobile telecommunications device; or

(i)

has not consented to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

Australia, Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020, 25th April 2020

I, Greg Hunt, Minister for Health, make the following determination.
Dated
25 April 2020
Greg Hunt
Minister for Health

Part 1—Preliminary
1 Name

This instrument is the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020*.

2 Commencement

(1)
Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. The whole of this instrument	11.59 pm (by legal time in the Australian Capital Territory) on the day this instrument is registered.	25 April 2020

Note:
This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2)
Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under subsection 477(1) of the *Biosecurity Act 2015*.

4 Object

The object of this instrument is to make contact tracing faster and more effective by encouraging public acceptance and uptake of COVIDSafe.

5 Definitions

Note: A number of expressions used in this instrument are defined in the

Biosecurity Act 2015, including the following:
(a) Australian law;
(b) Health Department;
(c) State or Territory body.

In this instrument:
contact tracing has the meaning given by subsection 6(4).
COVID app data has the meaning given by subsection 6(3).
COVIDSafe has the meaning given by paragraph 6(3)(a).
deidentified: information is ***deidentified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
in contact: a person has been ***in contact*** with another person if the operation of COVIDSafe in relation to the person indicates that the person may have been in the proximity of the other person.
mobile telecommunications device means an item of customer equipment (within the meaning of the *Telecommunications Act 1997*) that is used, or is capable of being used, in connection with a public mobile telecommunications service (within the meaning of that Act).
National COVIDSafe Data Store means the database administered by or on behalf of the Commonwealth for the purpose of contact tracing.
State or Territory health authority means the State or Territory body responsible for the administration of health services in a State or Territory.

Part 2—Requirements

6 Collection, use or disclosure of COVID app data

(1)
A person must not collect, use or disclose COVID app data except as provided by subsection (2).
(2)
Subsection (1) does not prevent a person from collecting, using or disclosing COVID app data if:
(a)
the collection, use or disclosure:
(i)
is by a person employed by, or in the service of, a State or Territory health authority; and
(ii)
is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing; or
(b)
the collection, use or disclosure is by an officer, employee or contractor of the Health Department or the Digital Transformation Agency for the purpose of, and only to the extent required for the purpose of:
(i)
enabling contact tracing by persons employed by, or in the service of, State or Territory health authorities; or
(ii)

ensuring the proper functioning, integrity or security of COVIDSafe or of the National COVIDSafe Data Store; or

(c)

in the case of a collection or disclosure of COVID app data—the collection or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i)

transferring encrypted data between mobile telecommunications devices through COVIDSafe; or

(ii)

transferring encrypted data, through COVIDSafe, from a mobile telecommunications device to the National COVIDSafe Data Store; or

(d)

the collection, use or disclosure is for the purpose of, and only to the extent required for the purpose of:

(i)

investigating whether a requirement of this determination has been contravened; or

(ii)

prosecuting a person for an offence against section 479 of the *Biosecurity Act 2015* in relation to a contravention of this determination; or

(e)

in the case of a use of COVID app data—the use is for the purpose of, and only to the extent required for the purpose of, producing statistical information that is deidentified.

Note: The *Privacy Act 1988* continues to apply except to the extent that it is inconsistent with this determination: see subsection 477(5) of the *Biosecurity Act 2015*.

(3)

COVID app data is data relating to a person that:

(a)

has been collected or generated through the operation of an app (***COVIDSafe***) that is made available, by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing; and

(b)

is, or has been, stored on a mobile telecommunications device.

However, it does not include information obtained, from a source other than the National COVIDSafe Data Store, in the course of undertaking contact tracing by a person employed by, or in the service of, a State or Territory health authority.

(4)

Contact tracing is the process of identifying persons who have been in contact with a person who has tested positive for the coronavirus known as COVID19, and includes:

(a)

notifying a person that the person has been in contact with a person who has tested positive for the coronavirus known as COVID19; and
(b)
notifying a person who is responsible for another person that the other person has been in contact with a person who has tested positive for the coronavirus known as COVID19; and
(c)
providing information and advice to a person who:
(i)
has tested positive for the coronavirus known as COVID19; or
(ii)
is responsible for another person who has tested positive for the coronavirus known as COVID19; or
(iii)
has been in contact with a person who has tested positive for the coronavirus known as COVID19; or
(iv)
is responsible for another person who has been in contact with a person who has tested positive for the coronavirus known as COVID19.

7 Treatment of COVID app data

COVID app data on mobile telecommunications devices
(1)
A person must not upload COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store except with the consent of the person who has possession or control of the device.
(2)
A person must not cause COVID app data (other than initial registration data or a unique identifier) to be retained on a mobile telecommunications device for more than 21 days.
COVID app data in the National COVIDSafe Data Store
(3)
If COVID app data is uploaded from a mobile telecommunications device to the National COVIDSafe Data Store, a person must not:
(a)
retain the data on a database outside Australia; or
(b)
disclose the data to a person outside Australia.
(4)
Paragraph (3)(b) does not apply to a disclosure by a person employed by, or in the service of, a State or Territory health authority if the disclosure is for the purpose of, and only to the extent required for the purpose of, undertaking contact tracing.
(5)
The Commonwealth must cause COVID app data in the National COVIDSafe Data Store to be deleted after the COVID19 pandemic has concluded.
Note: The requirements in this section will override any obligation

under an Australian law to retain data for a longer period: see subsection 477(5) of the *Biosecurity Act 2015*.

8 Decrypting COVID app data

A person must not decrypt encrypted COVID app data that is stored on a mobile telecommunications device.

9 Coercing the use of COVIDSafe

(1)

A person must not require that another person:

(a)

download COVIDSafe to a mobile telecommunications device; or

(b)

have COVIDSafe in operation on a mobile telecommunications device; or

(c)

consent to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

(2)

A person must not:

(a)

refuse to enter into, or continue, a contract or arrangement with another person (including a contract of employment); or

(b)

take adverse action (within the meaning of the *Fair Work Act 2009*) against another person; or

(c)

refuse to allow another person to enter premises; or

(d)

refuse to allow another person to participate in an activity; or

(e)

refuse to receive goods or services from another person; or

(f)

refuse to provide goods or services to another person;

on the ground that, or on grounds that include the ground that, the other person:

(g)

has not downloaded COVIDSafe to a mobile telecommunications device; or

(h)

does not have COVIDSafe in operation on a mobile telecommunications device; or

(i)

has not consented to uploading COVID app data from a mobile telecommunications device to the National COVIDSafe Data Store.

Australia - Office of the Australian Information Commissioner (OAIC), Covid 19, 30th June 2020

We have developed advice and guidance on privacy and freedom of information in the context of the COVID-19 outbreak for individuals, Australian Government agencies and organisations covered by the Privacy Act 1988.

Privacy guidance

Privacy advice and guidance issued during the COVID-19 outbreak includes:

- Information for individuals on the COVIDSafe app and my privacy rights.
- Guidelines for businesses collecting the personal information of individuals for contact tracing, as COVID-19 restrictions start to ease.
- Draft guidance for digital check-in providers collecting personal information for contact tracing.
- Guidance for entities on their privacy obligations regarding COVIDSafe and COVID app data.
- Privacy guidance for agencies and private sector employers to help keep workplaces safe and handle personal information appropriately, including answers to frequently asked questions.
- Detailed advice to help regulated entities assess the privacy risks involved in changed working environments and remote working arrangements.
- A step-by-step tool to help guide organisations and agencies through the Privacy Impact Assessment process.

Regulatory coordination

- The OAIC and state and territory privacy regulators have convened a National COVID-19 Privacy Team to respond to personal information handling proposals with national implications.
- We've joined with international regulators through the Global Privacy Assembly to issue a statement of support for public bodies and health practitioners to be able to communicate directly with people to tackle the outbreak.
- Australian and New Zealand Information Access Commissioners have joined their international counterparts to call for documentation, preservation and access to information as governments, businesses and citizens deal with the pandemic.

Freedom of information guidance

- We acknowledge that the impact of the coronavirus may affect the ability of agencies to meet statutory timeframes for processing freedom of information requests and recommend agencies consider a range of measures to help meet these obligations.
- We have developed FAQs for applicants about access to information issues related to COVID-19.

Australia - Office of the Australian Information Commissioner (OAIC), Privacy obligations regarding COVIDSafe and COVID app data, 30th June 2020

A legal framework of privacy protections has been established under Part VIIIA of the *Privacy Act 1988* (Privacy Act) to protect COVID app data. Amongst other things, these legislative provisions:

- prohibit certain conduct;
- outline the limited purposes for which COVID app data may be collected, used or disclosed;
- require COVID app data to be stored in, and not disclosed outside of, Australia; and
- set penalties for breaches of this law.

The Office of the Australian Information Commissioner (OAIC) has regulatory oversight of these new privacy protections. This extends to state and territory health authorities' handling of COVID app data and their activities that relate to COVID app data.

What is COVID app data?

COVID app data is data relating to any individual which is collected or generated through the operation of the COVIDSafe app and is (or has been) stored on a communication device such as a mobile phone.

This includes:

- the data provided by the individual at the time they downloaded the app and registered to use it ('registration data'), and
- data stored on an individual's communication device — and uploaded to the National COVIDSafe data store — about each contact made with another communication device using the app ('digital handshake' data).

De-identified information that is derived from COVID app data by the administrator of the National COVIDSafe Data Store, for the purpose of producing de-identified statistical information about the total number of registrations of the app, is *not* considered to be 'COVID app data' for the purposes of the Privacy Act.

The legal status of COVID app data

COVID app data is 'personal information' for the purposes of the Privacy Act.

When COVID app data is downloaded from the National COVIDSafe Data Store by a state or territory health authority, it retains its status as COVID app data under the Privacy Act. State and territory health authorities must therefore comply with the Privacy Act when handling COVID app data.

However, information collected by a state or territory health authority from a source other than directly from the National COVIDSafe Data Store will *not* be 'COVID app data'. For example, when a diagnosed individual provides to a contact tracing team the names and mobile phone numbers of other individuals with whom they have recently come into contact, this will not be considered 'COVID app data', even if some or all of the same information is also held in the National COVIDSafe Data Store.

Requiring the use of COVIDSafe

The COVIDSafe app is voluntary. While use of the app may be encouraged, the Privacy Act provides that no individual, organisation or government agency can require any individual to download or use the app. Criminal penalties apply for breach of these provisions.

It is unlawful for any person to require an individual to:

- download the COVIDSafe app
- have the app in operation on their communication device, or
- upload data from the app to the National COVIDSafe Data Store.

An individual, organisation (including a small business operator) or agency which treats its staff, suppliers or customers differently, or which charges a different price for a service, depending on whether or not an individual has or is using the COVIDSafe app, might be considered to be unlawfully 'requiring' an individual to use the app. However, this does not apply to private citizens in their personal lives. For example, it is not an offence if a relative or friend asks you to download the app before visiting their home.

Uploading data from the app

If an individual is diagnosed with COVID-19, a state or territory health official will ask the individual if they have been using the COVIDSafe app and if they agree to upload data about their close contacts. Consent must be obtained from that individual to upload the data from the app to the National COVIDSafe Data Store.

Only the individual whose name and communication device number was provided at the time of initial registration for the app can consent to upload the data. If the individual is unable to give consent, due to being a child for example, consent to upload the data must be obtained from a parent, guardian or carer acting on that individual's behalf.

It is an offence for any individual, organisation or government agency to require an individual to upload their data, or cause for the data to be uploaded, from the app to the National COVIDSafe Data Store, without obtaining consent from that individual.

Disclosure outside Australia

COVID app data in the National Data Store must be stored on a database in Australia.

It is an offence to disclose COVID app data that has been uploaded to the national COVIDSafe data store to another individual outside Australia unless:

- the disclosure is by a person employed or in the service of a state or territory health authority, and
- the disclosure is for the purpose of, and only to the extent required for the purpose of, conducting contact tracing.

Collecting, using or disclosing COVID app data

COVID app data may only be collected, used or disclosed:

- by a person employed or in the service of a state or territory health authority to conduct contact tracing:
    - only to the extent required to undertake that contact tracing
- by the National COVIDSafe Data Store administrator (or their contracted service provider):
    - to enable contact tracing by a person employed or in the service of a state or territory health authority
    - to ensure the proper functioning, integrity and security of the app or the National COVIDSafe Data Store
    - to delete registration data on request from (or on behalf of) an individual who is the subject of the registration data, and
    - to produce de-identified statistical information about the number of registrations for the app
- by the OAIC:
    - to assess and investigate compliance with the Privacy Act in relation to the handling of COVID app data
    - to review compliance with the notifiable data breach scheme in relation to

handling of COVID app data
- to refer matters to state or territory privacy regulators as appropriate, and
- to refer suspected breaches of the Privacy Act in relation to handling of COVID app data to the police or director of public prosecutions as appropriate.

• by the police or director of public prosecutions:
- to investigate and prosecute alleged breaches of the Privacy Act in relation to handling of COVID app data.

Obligations to protect and manage data appropriately

All parties handling COVID app data must also comply with the Australian Privacy Principles (APPs). With the exception of APP 9, the APPs will also apply to state and territory health authorities in relation to their handling of COVID app data.

This includes APP 11, which requires organisations handling COVID app data to take reasonable steps to protect the data from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure.

APP 1 also requires each organisation handling COVID app data, including state and territory health authorities, to:

• manage the data in an open and transparent way

• implement practices, procedures and systems to ensure its compliance with all relevant privacy rules, and

• have a clearly expressed and up-to-date privacy policy which explains how it manages COVID app data.

Incidental collection

If COVID app data is incidentally collected as part of a wider, lawful collection of information (for example, during a criminal investigation), the data must be deleted as soon as practicable and must not otherwise be accessed, used or disclosed to anyone. The data also cannot be used as evidence in any proceedings.

Deletion of registration data on request

The National COVIDSafe Data Store administrator must, upon the request of the individual, their parent, guardian or carer, delete that individual's registration data from the National COVIDSafe Data Store.

The information must be deleted as soon as is practicable and if it cannot be deleted immediately, it must not be used or disclosed for any purpose.

This requirement does not apply to digital handshake data, held in the National COVIDSafe Data Store, comprising of Bluetooth connections between the communication device of the individual who is seeking deletion (or on whose behalf the deletion is sought) and other communication devices, or to de-identified data.

At the end of the pandemic

The Health Minister must determine a date by which the Health Minister is satisfied that use of the COVIDSafe app is no longer required, or is no longer likely to be effective, in preventing or controlling the spread of COVID-19 in Australia.

Immediately after midnight on that declared date, the National COVIDSafe Data Store administrator must:

• prevent any new downloads of the COVIDSafe app by individuals

• stop any new uploads of data from the COVIDSafe app into the National COVIDSafe Data Store.

As soon as reasonably practicable after the declared date, the National COVIDSafe Data Store administrator must delete all COVID app data from the National COVIDSafe Data Store.
The National COVIDSafe Data Store administrator must also notify the Health Minister and the OAIC that all COVID app data has been deleted from the National COVIDSafe Data Store.
The National COVIDSafe Data Store administrator must also take all reasonable steps to notify all users of the COVIDSafe app (who have not already deleted the app) that their data has been deleted and they should now delete the app from their communication devices. The National COVIDSafe Data Store administrator must also take all reasonable steps to inform users that COVID app data can no longer be collected.
Data breaches
The notifiable data breach scheme has been extended to include certain conduct by the National COVIDSafe Data Store administrator, and state and territory health authorities.
A breach of any of the new COVID app-related provisions of the Privacy Act by the National COVIDSafe Data Store administrator, or by a state or territory health authority, will be considered an 'eligible data breach'. All individuals to whom the data relates are considered to be 'at risk' from the data breach and both the OAIC and affected individuals must be notified as soon as practicable about the data breach, unless the OAIC grants an exemption to the requirement to notify individuals. This is a lower threshold than for eligible data breaches under the notifiable data breach scheme in Part IIIC of the Privacy Act, which only become notifiable if the data breach is 'likely to result in serious harm' to any of the individuals to whom the information relates.
A failure to notify the data breach as required is an 'interference with privacy', which triggers the OAIC's powers.
Interference with privacy: OAIC powers
A breach of any of the new COVID app-related provisions of the Privacy Act, or the APPs, is considered an 'interference with privacy', which triggers the OAIC's investigative and regulatory powers under the Privacy Act, in relation to regulated entities.
The OAIC has powers to:

- conduct assessments
- investigate complaints
- commence investigations on its 'own motion'
- refer matters to state or territory privacy regulators
- make a declaration that compensation be paid to individuals who suffer from an interference with their privacy
- seek civil penalties for serious and repeated interferences with privacy, and
- refer matters to the police if the OAIC thinks a crime has been committed.

The OAIC also has an obligation to report publicly every six months on the performance of the Privacy Commissioner's functions and exercise of the Privacy Commissioner's powers under the new COVID app-related provisions of the Privacy Act.
The Health Minister has an obligation to report every six months on the operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store.

Belgium, Service Public Federal Chancellerie Du Premier Ministre [C – 2020/10437] 25 AOUT 2020. — Accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les services d'inspections d'hygiène et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID–19 se fondant sur une base de données auprès de Sciensano

BELGISCH STAATSBLAD — 15.10.2020 – Ed. 2 — MONITEUR BELGE

Vu le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE;

Vu la loi spéciale du 8 août 1980 de réformes institutionnelles, et notamment ses articles 5, § 1er, I, 6bis, § 2, 1° et 2°, et 92bis;

Vu que l'Autorité fédérale n'est pas exclusivement compétente en ce qui concerne la politique de crise au cas où une pandémie (aiguë) nécessite des mesures urgentes. L'Autorité fédérale, les Communautés et les Régions sont compétentes chacune dans les limites de ses compétences propres. L'Autorité fédérale est, à ce titre à tout le moins, également compétente aussi pour la coordination ou la gestion d'une situation de crise de type pandémique ;

Vu que l'autorité fédérale et les entités fédérées ont la compétence d'adopter des mesures portant sur la lutte contre une crise touchant la santé publique, chacune dans le cadre de ses compétences matérielles;

Vu le décret du Parlement flamand du 21 novembre 2003 relatif à la politique de santé préventive;

Vu le décret du Parlement de la Communauté germanophone du 1er juin 2004 relatif à la promotion de la santé et à la prévention médicale;

Vu l'ordonnance du 19 juillet 2007 relative à la politique de prévention en santé;

Vu la loi du 10 avril 2014 portant des dispositions diverses en matière de santé et l'accord de coopération conclu en application de celle-ci entre l'INAMI et Sciensano;

Vu la loi du 25 février 2018 portant création de Sciensano, les articles 4, § 4 et 7, § 2;

Vu la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

Vu le décret du 2 mai 2019 modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé;

Vu le décret du Parlement flamand du 29 mai 2020 portant organisation de l'obligation de déclaration et du suivi des contacts dans le cadre du COVID–19;

Vu l'arrêté du Collège réuni de la Commission communautaire commune du 23 avril 2009 relatif à la prophylaxie des maladies transmissibles;

Vu l'arrêté du Gouvernement flamand du 19 juin 2009 relatif aux initiatives visant à prévenir l'extension des effets néfastes causés par des facteurs biotiques;

Vu l'arrêté royal n° 18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID–19;

Vu l'Arrêté royal n° 25 du 28 mai 2020 modifiant l'arrêté royal n° 18 du 4 mai 2020 portant

création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID–19;
Vu l'arrêté royal n° 44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles des entités fédérées dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID–19 sur la base d'une base de données auprès de Sciensano; Vu l'arrêté du Gouvernement wallon de pouvoirs spéciaux n° 35 du 5 mai 2020 organisant le tracing socio-sanitaire dans le cadre de la lutte contre l'épidémie COVID–19 ;
Vu l'arrêté du gouvernement de la Communauté germanophone du 7 mai 2020 portant création d'un centre de contact chargé du suivi de la chaîne d'infection dans le cadre de la lutte contre la crise sanitaire provoquée par le coronavirus (COVID–19);
Considérant que cet accord de collaboration a pu être réalisé en respect de la répartition de compétences qui en vertu de la loi spéciale de réformes institutionnelles ont été attribuées aux différents niveaux de pouvoirs grâce à une collaboration intense au sein de la Conférence Interministérielle qui s'inscrit dans une longue tradition de collaboration au sein de la Conférence Interministérielle de santé entre les différents niveaux de pouvoirs de notre pays ;
Considérant que, depuis le début de la crise pandémique, l'Etat fédéral, en concertation avec les différents niveaux de pouvoir, a pris des mesures dans la compétence de la sécurité civile, pour protéger les citoyens de notre pays.
Considérant que l'Organisation mondiale de la santé a déclaré le 11 mars 2020 que l'épidémie de virus SARS-CoV-2 constitue une pandémie;
Considérant que, dans le contexte de la crise sanitaire du coronavirus COVID–19 et afin de prévenir la propagation du coronavirus COVID–19, le Conseil national de sécurité, qui réunissait des représentants du gouvernement fédéral ainsi que des représentants des entités fédérées, a été chargé de prendre des mesures concertées;
Considérant que l'une de ces mesures nécessaires est la détection précoce des personnes qui ont été en contact avec des personnes infectées par le coronavirus COVID–19 ou sérieusement suspectées d'être infectées par le coronavirus COVID–19, de même que la détection des collectivités dont font partie ces personnes, afin que les recommandations nécessaires puissent être données à ces personnes pour les empêcher d'infecter d'autres personnes avec le coronavirus COVID–19, telles que l'élaboration de lignes directrices en matière d'hygiène et de prévention, la proposition d'une quarantaine et l'invitation à passer un test de dépistage du coronavirus COVID–19;
Considérant que l'État fédéral est compétent pour la politique de crise lorsqu'une pandémie aiguë nécessite une action urgente, dans le respect des compétences matérielles de chaque entité (doc. Sénat, n° 5-2232/5);
Considérant que, dans le cadre de leur compétence en matière de médecine préventive, et dans le cadre de la coordination organisée par l'autorité fédérale en cas de situation de crise de type pandémique, les entités fédérées ont mis en place des centres d'appel pour effectuer ce suivi des contacts ainsi que pour pouvoir leur donner des recommandations pour éviter qu'ils infectent d'autres personnes;
Considérant que, pour faire face à cette crise au niveau national et pour optimiser le suivi des contacts, il est nécessaire de rassembler les informations dans une base de données fédérale unique qui échange des données avec trois bases de données relevant de la compétence des entités fédérées;
Considérant que l'autorité fédérale dispose indubitablement de compétences lui permettant

d'organiser le traitement des données dans le cadre de la lutte contre la propagation du coronavirus COVID–19. À cette fin, elle peut, dans le cadre de l'exercice de ses compétences, créer une base de données et, sur la base de sa compétence résiduelle en matière d'exercice de la médecine, imposer aux professionnels de la santé l'obligation d'introduire les données requises dans cette base, par dérogation au principe du secret professionnel. En outre, elle peut accorder aux entités fédérées un accès à une telle base de données, sur une base volontaire, comme c'est déjà le cas pour d'autres bases de données fédérales telles que la Banque-Carrefour de la sécurité sociale;
Considérant que le Conseil d'État (avis 67.435/3, 67.426/3, 67.427/3 du 26 mai 2020) a déclaré, dans son avis, qu'un tel accord de coopération offre la solution la plus sûre sur le plan juridique. Dans ces circonstances, compte tenu également du fait que l'arrêté royal n° 18 du 4 mai 2020 est déjà appliqué dans la pratique, l'accord de coopération peut avoir un effet rétroactif au 4 mai 2020, à savoir le jour où l'arrêté en question est entré en vigueur ;
il est nécessaire de conclure un accord de coopération,
ENTRE,
L'État fédéral, représenté par le Gouvernement fédéral en la personne de Madame Sophie Wilmès, Première ministre, et Madame Maggie De Block, Ministre des Affaires sociales et de la Santé publique et de l'Asile et de la Migration;
la Communauté flamande, représentée par le Gouvernement flamand en la personne de Monsieur Jan Jambon, Ministre-Président, et Monsieur Wouter Beke, Ministre du Bien-Être, de la Santé publique, de la Famille et de la Lutte contre la Pauvreté;
la Région wallonne, représentée par le Gouvernement wallon en la personne de Monsieur Elio Di Rupo, Ministre-Président, et Madame Christie Morreale, Ministre de l'Emploi, de la Formation, de la Santé, de l'Action sociale, de l'Égalité des Chances;
la Commission communautaire commune, représentée par le Collège réuni en la personne de Monsieur Rudi Vervoort, Président du Collège réuni et Monsieur Alain Maron et Madame Elke Van den Brandt, membres ayant la Santé et l'Action sociale dans leurs attributions; et
la Communauté germanophone, représentée par le Gouvernement de la Communauté germanophone, en la personne de Monsieur Oliver Paasch, Ministre-Président, et Monsieur Antonios Antoniadis, Vice-Ministre Président, Ministre de la Santé et des Affaires Sociales, de l'Aménagement du Territoire et du Logement.

CHAPITRE I. — Disposition générale
Article 1er.
§ 1er. Aux fins du présent accord de coopération, on entend par :
1° Règlement Général sur la Protection des Données : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE;
2° cluster : une concentration de personnes infectées ou potentiellement infectées par le coronavirus COVID–19 dans des collectivités;
3° collectivité : une communauté de personnes pour lesquelles les inspections d'hygiène compétentes estiment qu'il existe un risque accru de propagation du coronavirus COVID–19;
4° centre de contact : instance désignée par les entités fédérées compétentes ou par les agences compétentes pour contacter la personne concernée par tout moyen de communication, y compris par téléphone, par courrier électronique ou au moyen d'une visite physique dans le cadre des objectifs fixés à l'article 3, § 2, et qui partage ensuite les données collectées avec la

base de données I;
5° coronavirus COVID–19 : virus du SARSCoV-2;
6° Base de données I : la base de données de Sciensano qui sera créée en vertu du présent accord de coopération pour le traitement et l'échange de données aux finalités de traitement prévues à l'article 3;
7° Base de données II : la base de données existante à Sciensano, utilisée pour la recherche scientifique et établie par la loi du 10 avril 2014 portant des dispositions diverses en matière de santé et l'accord de coopération conclu en application de celle-ci entre l'INAMI et Sciensano, visé à l'article 22, 20° de la loi relative à l'assurance obligatoire soins de santé et indemnités coordonnée le 14 juillet 1994 et la loi du 25 février 2018 portant création de Sciensano;
8° Base de données III : la base de données des instructions d'appel et des instructions pour le personnel du centre de contact conformément aux dispositions de l'article 10, § 1er;
9° Base de données IV : la base de données contenant les coordonnées des collectivités;
10° Base de données V : le journal central des enregistrements de l'application numérique de traçage des contacts qui permet de contrôler le fonctionnement de l'application numérique de traçage des contacts, telle que décrite à l'article 14, et qui, à Sciensano, est séparée des Bases de données I et II;
11° le numéro NISS : le numéro d'identification, visé à l'article 8, § 1er, 1° ou 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale;
12° équipes mobiles : les collaborateurs de l'équipe de soutien COVID (Outbreak Support team) organisée par les inspections d'hygiène qui prennent des mesures sur place dans le cas d'un cluster;
13° Personnes de catégorie I : les personnes pour lesquelles le médecin a prescrit un test de dépistage du coronavirus COVID–19;
14° Personnes de catégorie II : les personnes qui ont été testées pour le coronavirus COVID–19;
15° Personnes de catégorie III : les personnes pour lesquelles le médecin a une présomption sérieuse d'infection par le coronavirus COVID–19, sans qu'un test de dépistage du coronavirus COVID–19 n'ait été effectué ou prescrit, ou lorsque le test de dépistage du coronavirus COVID–19 a révélé qu'elles n'étaient pas infectées;
16° Personnes de catégorie IV : les personnes avec lesquelles (i) les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles sont infectées, et (ii) les Personnes de catégorie III ont été en contact au cours d'une période de quatorze jours avant à quatorze jours après les premiers signes d'infection par le coronavirus COVID–19, une certaine marge d'appréciation pouvant être prise en compte sur la base des connaissances scientifiques;
17° Personnes de catégorie V : les médecins traitants des Personnes des catégories I, II et III;
18° Personnes de catégorie VI : le médecin de référence - ou, en l'absence de médecin de référence au sein de la collectivité concernée - le responsable administratif des collectivités avec lesquelles les Personnes des catégories I, II et III ont été en contact au cours d'une période de quatorze jours avant à quatorze jours après les premiers symptômes de l'infection par le coronavirus COVID–19, une certaine marge d'appréciation pouvant être prise en compte sur la base des connaissances scientifiques;
19° pseudonymisation ou données pseudonymisées : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures

techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable, comme prévu à l'article 4, 5), du Règlement Général sur la Protection des Données;
20° les enquêteurs de terrain : les collaborateurs des centres de contact qui peuvent effectuer des visites physiques dans le cadre du suivi des contacts;
21° hôpital : établissement de soins tel que visé par la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins, ainsi que sur les hôpitaux de revalidation;
22° prestataire de soins de santé : un professionnel de la santé visé par la loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé et par la loi du 29 avril 1999 relative aux pratiques non conventionnelles dans les domaines de l'art médical, de l'art pharmaceutique, de la kinésithérapie, de l'art infirmier et des professions paramédicales;
§ 2. Le présent accord de coopération poursuit les objectifs suivants :
1° dans le cadre du suivi manuel des contacts et du déploiement d'équipes mobiles :
a. la création de la Base de données I, à l'intérieur de laquelle les données sont traitées aux fins du suivi des contacts;
b. l'échange de données entre la Base de données I et les Bases de données III et IV, afin d'aider les centres de contact désignés par les entités fédérées ou les agences compétentes (en ce compris les enquêteurs de terrain), et la création de ces bases de données;
c. l'échange de données entre la Base de données I et les services d'inspection d'hygiène, ainsi qu'avec les équipes mobiles;
d. l'identification et la détection des foyers du coronavirus COVID–19 et des clusters;
e. la prise de mesures sur place pour contenir les foyers et les clusters du coronavirus COVID–19;
f. fournir des conseils aux personnes infectées par le coronavirus COVID–19, à l'égard desquelles un médecin a de sérieuses suspicions ou lorsqu'il existe un risque élevé que ce soit le cas, en vue de rompre la chaîne d'infection par le coronavirus COVID–19;
g. continuer à suivre les personnes à qui des conseils ont été donnés; et
h. continuer à garantir les fonctions de la surveillance épidémiologique existante par Sciensano.

2° la mise en place d'un cadre permettant le suivi numérique des contacts au moyen d'une application numérique de traçage des contacts;
3° permettre aux instituts de recherche et administrations, dont Sciensano, de mener des études scientifiques ou statistiques sur la lutte contre la propagation du coronavirus COVID–19 et/ou de soutenir les politiques dans ce domaine, par l'échange de données entre la Base de données I et la Base de données II.
§ 3. Sauf disposition contraire, le présent accord de coopération ne porte pas préjudice aux règles en vigueur en matière de suivi des contacts pour la détection des maladies infectieuses ou contagieuses dans le cadre des compétences matérielles en matière de médecine préventive.
§ 4 Les parties, chacune dans son domaine de compétence, prennent les mesures nécessaires à la mise en œuvre des dispositions du présent accord de coopération et à l'harmonisation des initiatives communautaires, régionales et fédérales existantes avec celui-ci.
§ 5. Les parties peuvent, au moyen d'un accord de coopération d'exécution prévu à l'article 92bis, § 1er, alinéa 3, de la loi spéciale du 8 août 1980 de réformes institutionnelles, définir les modalités requises pour la mise en œuvre du présent accord.
§ 6. Les professionnels de la santé sont déliés de leur obligation de garder le secret professionnel, visée à l'article 458 du Code pénal, dans le cadre du présent accord de coopération.
Les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19

a révélé qu'elles sont infectées, et les Personnes de catégorie III sont déliées de leur obligation de garder le secret professionnel, visée à l'article 458 du Code pénal, dans le cadre du présent accord de coopération.
Art. 2.
§ 1er. Afin d'atteindre les objectifs visés à l'article 1er, § 2, une Base de données I, qui contient les catégories de données décrites à l'article 6, est créée au sein de Sciensano. Ces données sont traitées conformément aux finalités telles que définies à l'article 3, pour la durée déterminée à l'article 15. Ces données seront communiquées par les personnes autorisées ou au nom des personnes autorisées des hôpitaux et des laboratoires, ainsi que par les médecins et le personnel du centre de contact, des services d'inspection d'hygiène et des équipes mobiles.
§ 2. La Base de données I est créée sans préjudice de la Base de données II déjà existante.
Pour atteindre l'objectif visé à l'article 1er, § 2, 1°, h, et 3°, les données de la Base de données I seront pseudonymisées avant d'être incluses dans la Base de données II conformément aux dispositions des articles 9 et 10.
§ 3. Pour atteindre les objectifs visés à l'article 1er, § 2, 1° b, e, f et g, et parallèlement à la Base de données I, les bases de données temporaires suivantes sont également créées, entre lesquelles les catégories de données définies à l'article 6 seront échangées, mais uniquement pour les finalités de traitement définies à l'article 3 et conformément aux dispositions de l'article 10, pour la durée déterminée à l'article 15 :
1° la Base de données III;
2° la Base de données IV

§ 4. Sciensano est le responsable du traitement des Bases de données I et II.
§ 5. Les entités fédérées compétentes ou les agences désignées par les autorités compétentes, chacune pour sa compétence, agissent en tant que responsables du traitement des Bases de données III et IV, en ce qui concerne les données à caractère personnel collectées et utilisées par les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes et prennent les mesures appropriées pour que les personnes visées à l'article 4 reçoivent les informations visées aux articles 13 et 14 du Règlement Général sur la Protection des Données et les communications visées aux articles 15 à 22 et à l'article 34 du Règlement Général sur la Protection des Données en ce qui concerne les finalités de traitement visées à l'articles 3, § 2. Ces informations doivent être fournies dans un langage simple et clair et de manière concise, transparente, compréhensible et facilement accessible.

CHAPITRE II. — Finalités de traitement
Art. 3.
§ 1er. Le traitement des données à caractère personnel de la Base de données I vise les finalités de traitement suivantes :
1° la mise à disposition par la Base de données I au centre de contact compétent (en ce compris les enquêteurs de terrain) des catégories de données à caractère personnel définies à l'article 7, § 2, des :
(i) Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles étaient infectées et
(ii) Personnes de catégorie III ;
au travers d'un échange avec la Base de données III, en vue de contacter les personnes visées au présent alinéa par tout moyen de communication possible, en ce compris par téléphone, par courrier électronique ou au moyen d'une visite physique, afin de leur donner d'éventuelles

recommandations, mais en particulier de leur demander de fournir des informations, telles que les coordonnées, le risque de contamination du contact et la date à laquelle ces personnes ont eu des contacts;
2° A. la mise à disposition par la Base de données I au centre de contact compétent des catégories de données à caractère personnel définies à l'article 7, § 3, au travers d'un échange avec la Base de données III, en vue de contacter les Personnes de catégorie IV, par tout moyen de communication possible, en ce compris par téléphone, courrier électronique ou au moyen d'une visite physique, pour leur fournir des recommandations en matière d'hygiène et de prévention, leur proposer une quarantaine ou les inviter à se soumettre au test de dépistage du coronavirus COVID–19, en bénéficiant d'un suivi à ce niveau;
B. la mise à disposition par la Base de données I au centre de contact compétent des catégories de données à caractère personnel définies à l'article 7, § 4, au travers d'un échange avec la Base de données III, en vue de contacter les Personnes de catégories VI par tout moyen de communication possible, y compris par téléphone, par courrier électronique ou par visite à la collectivité, afin de les informer de la contamination (présumée) des (i) Personnes de catégorie II dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles étaient infectées, et (ii) des Personnes de catégorie III;
3° la mise à disposition des catégories de données à caractère personnel des Personnes de catégories I, II, et II, telles que définies à l'article 6, par la Base de données I, aux équipes mobiles et aux services d'inspection d'hygiène des autorités fédérées, dans le cadre des initiatives visant à prévenir la propagation des effets nocifs causés par le coronavirus COVID–19, chacune dans son domaine de compétence, toujours conformément à l'article 10, §2, pour la réalisation de leurs missions réglementaires.
Les équipes mobiles et les services d'inspections d'hygiène compétentes dont il est question à l'alinéa 1er sont celles visées dans :
a) le décret du Parlement flamand du 21 novembre 2003 relatif à la politique de santé préventive;
b) le décret du Parlement de la Communauté germanophone du 1er juin 2004 relatif à la promotion de la santé et à la prévention médicale et ses arrêtés d'exécution;
c) l'ordonnance de la Région de Bruxelles Capitale du 19 juillet 2007 relative à la politique de prévention en santé;
d) le décret du 2 mai 2019 modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé;
e) l'arrêté du Collège réuni de la Commission communautaire commune du 23 avril 2009 relatif à la prophylaxie des maladies transmissibles;
f) l'arrêté du Gouvernement flamand du 19 juin 2009 relatif aux initiatives visant à prévenir l'extension des effets néfastes causés par des facteurs biotiques.
4° la mise à disposition de données à caractère personnel pseudonymisées relevant des catégories de données à caractère personnel, relatives aux Personnes de catégories I à V, visées à l'article 6 conformément aux dispositions de l'article 10, à la base de données II déjà existante, afin de mettre les données pseudonymisées visées au présent alinéa après anonymisation, ou au moins pseudonymisation dans le cas où l'anonymisation ne permettrait pas aux institutions de recherche d'effectuer leur étude scientifique ou statistique, à la disposition des institutions de recherche, dont Sciensano, selon la procédure prévue à cet effet afin de permettre aux institutions de recherche d'effectuer des études scientifiques ou statistiques sur la lutte contre la propagation du coronavirus COVID–19 et/ou, après pseudonymisation, de soutenir la politique dans ce domaine conformément au titre 4 de la loi du 30 juillet 2018 relative à la

protection des personnes physiques à l'égard des traitements de données à caractère personnel.
§ 2. Les centres de contact désignés par les entités fédérées ou les agences compétentes peuvent, dans la mesure où ils sont compétents et conformément à l'article 10, § 1er :
1° traiter les catégories de données à caractère personnel visées à l'article 7, § 2 des (i) Personnes de catégorie II dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles étaient infectées et, (ii) des Personnes de catégorie III, afin de contacter les personnes visées au présent alinéa par tout moyen de communication possible, y compris par téléphone, par courrier électronique ou au moyen d'une visite physique, afin de leur donner d'éventuelles recommandations, mais en particulier de leur demander de fournir des informations, telles que les coordonnées, le risque de contamination du contact et la date à laquelle ces personnes ont eu des contact;
2° A. traiter les catégories de données à caractère personnel définies à l'article 7, § 3, aux fins de contacter les Personnes de catégorie IV par tout moyen de communication possible, y compris par téléphone, courrier électronique ou au moyen d'une visite physique, pour leur fournir, entre autres, des recommandations en matière d'hygiène et de prévention, leur proposer une quarantaine, ou les inviter à se soumettre au test de dépistage du coronavirus COVID–19, en bénéficiant d'un suivi;
B. traiter les catégories de données à caractère personnel définies à l'article 7, § 4, pour contacter les Personnes de catégorie VI par tout moyen de communication possible, y compris par téléphone, par courrier électronique ou au moyen d'une visite à la collectivité, afin de les informer de la contamination (présumée) des Personnes de catégorie II, pour autant que le test de dépistage du coronavirus COVID–19 montre qu'elles sont infectées, et des Personnes de catégorie III;
§ 3. Les équipes mobiles et les services d'inspection d'hygiène compétentes des entités fédérées, dans le cadre des initiatives visant à prévenir l'extension des effets néfastes causés par le coronavirus COVID–19, peuvent, chacun dans son domaine de compétence, toujours conformément à l'article 10, § 2, traiter les catégories de données à caractère personnel des Personnes de catégories I, II, III et IV définies à l'article 6, pour l'accomplissement de leurs missions réglementaires.
Les équipes mobiles et les services d'inspections d'hygiène compétents dont il est question à l'alinéa 1er sont ceux visés dans :
a) le décret du Parlement flamand du 21 novembre 2003 relatif à la politique de santé préventive;
b) le décret du Parlement de la Communauté germanophone du 1er juin 2004 relatif à la promotion de la santé et à la prévention médicale et ses arrêtés d'exécution;
c) l'ordonnance de la Région de Bruxelles Capitale du 19 juillet 2007 relative à la politique de prévention en santé;
d) le décret du 2 mai 2019 modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé;
e) l'arrêté du Collège réuni de la Commission communautaire commune du 23 avril 2009 relatif à la prophylaxie des maladies transmissibles;
f) l'arrêté du gouvernement flamand du 19 juin 2009 relatif aux initiatives visant à prévenir l'extension des effets néfastes causés par des facteurs biotiques.
§ 4. Les données collectées dans le cadre du présent accord de coopération ne peuvent être utilisées à d'autres fins que celles prévues par le présent article, notamment mais pas exclusivement à des fins policières, commerciales, fiscales, pénales ou de sécurité de l'État.

CHAPITRE III. — Personnes dont les données à caractère personnel sont traitées dans le cadre du présent accord de coopération

Art. 4.

Pour les finalités de traitement prévues à l'article 3, seront traitées les catégories de données à caractère personnel, définies aux articles 6, 7, 8, et 9 du présent accord de coopération, des personnes suivantes :

1° les Personnes de catégorie I;
2° les Personnes de catégorie II;
3° les Personnes de catégorie III;
4° les Personnes de catégorie IV;
5° les Personnes de catégorie V;
6° les Personnes de catégorie VI.

CHAPITRE IV. — Catégories de données à caractère personnel collectées dans le cadre du présent accord de coopération

Art. 5.

Les données à caractère personnel collectées et traitées dans le cadre du présent accord de coopération sont traitées conformément aux réglementations relatives à la protection des traitements de données à caractère personnel, en particulier le Règlement Général sur la Protection des Données et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Art. 6.

§ 1er. Une déclaration obligatoire pour les personnes telle que visée dans

a) le décret du Parlement flamand du 21 novembre 2003 relatif à la politique de santé préventive,

b) le décret du Parlement de la Communauté germanophone du 1er juin 2004 relatif à la promotion de la santé et à la prévention médicale et ses arrêtés d'exécution;

c) l'ordonnance de la Région de BruxellesCapitale du 19 juillet 2007 relative à la politique de prévention en santé;

d) le décret du 2 mai 2019 modifiant le Code wallon de l'action sociale et de la santé en ce qui concerne la prévention et la promotion de la santé;

e) l'arrêté du Collège réuni de la Commission communautaire commune du 23 avril 2009 relatif à la prophylaxie des maladies transmissibles;

est faite, par dérogation à cette réglementation pour ce qui concerne le secret professionnel, auprès de la Base de données I.

Une déclaration obligatoire pour les Personnes de catégorie I dont le médecin ne soupçonne pas qu'elles sont infectées par le coronavirus COVID–19 et pour les Personnes de catégorie II dont le test de dépistage du coronavirus COVID–19 n'a révélé aucune infection, lorsque le résultat n'est pas contesté par le médecin, sera faite auprès de la Base de données I dans le cadre de cet accord de coopération.

§ 2. La Base de données I contient, pour autant qu'elles soient disponibles, les catégories suivantes de données à caractère personnel relatives aux Personnes de catégorie I, et ce aux fins prévues à l'article 3, § 1er :

1° le numéro NISS;
2° le nom et le prénom;
3° le sexe;
4° la date de naissance et, le cas échéant, la date de décès;

5° l'adresse;
6° les coordonnées, y compris le numéro de téléphone et l'adresse électronique de la personne concernée et de la personne à contacter en cas d'urgence ou du représentant légal, et l'indication du lien qu'ont ces personnes avec la personne concernée (parent, tuteur, médecin généraliste, ...);
7° la date de l'apparition des symptômes;
8° le numéro INAMI du prescripteur du test de dépistage du coronavirus COVID–19;
9° les données relatives au test de dépistage du coronavirus COVID–19 prescrit , en ce compris la date et le type de test de dépistage du coronavirus COVID–19 prescrit;
10° l'indication de l'exercice ou du nonexercice de la profession de prestataire de soins;
11° le service hospitalier, le numéro d'identification et les coordonnées de l'hôpital, si la personne concernée est hospitalisée;
12° éventuellement, le résultat du CT-scan, si la personne concernée est hospitalisée;
13° la collectivité éventuelle dont la personne concernée fait partie ou avec laquelle elle est entrée en contact.
Si le numéro d'identification du Registre national visé à l'article 8, § 1er, 1°, de la loi du 15 janvier 1990 sur la création et l'organisation d'une Banque Carrefour de la sécurité sociale est disponible, les nom et prénom, date de naissance, sexe et adresse sont extraits du Registre national ou des registres de la Banque Carrefour visés à l'article 4 de la loi du 15 janvier 1990 sur la création et l'organisation d'une Banque Carrefour de la sécurité sociale.
§ 3. La Base de données I contient, pour autant qu'elles soient disponibles, les catégories suivantes de données à caractère personnel relatives aux Personnes de catégorie II :
1° les données visées au § 2;
2° la date, le résultat, le numéro d'échantillon et le type de test de dépistage du coronavirus COVID–19;
3° le numéro INAMI du laboratoire qui a effectué le test de dépistage du coronavirus COVID–19;
4° si le résultat du test de dépistage n'a pas permis de constater une contamination, l'éventuelle décision d'annulation prise par un médecin;
5° si le résultat du test de dépistage n'a pas permis de constater une contamination, le numéro INAMI du médecin qui a pris la décision d'annulation.
Les données à caractère personnel visées aux 1°, 2° et 3° sont communiquées à Sciensano par les fournisseurs d'informations suivants : les personnes autorisées ou sur ordre des personnes autorisées du laboratoire, de l'hôpital ou de l'autre établissement de soins ou du prestataire de soins qui a effectué le test de dépistage du coronavirus COVID–19. Les données visées aux 4° et 5° sont communiquées à Sciensano par le médecin qui a pris la décision d'annulation.
§ 4. La Base de données I contient, pour autant qu'elles soient disponibles, les catégories suivantes de données à caractère personnel relatives aux Personnes de catégorie III :
1° le numéro NISS;
2° le nom et le prénom;
3° le sexe;
4° la date de naissance et, le cas échéant, la date de décès;
5° l'adresse;
6° les coordonnées de la personne concernée, en ce compris, le numéro de téléphone et l'adresse électronique de la personne concernée, ainsi que de la personne à contacter en cas d'urgence ou du représentant légal et l'indication du lien qu'ont ces personnes avec la personne concernée (parents, tuteur, médecin généraliste, ...);

7° le diagnostic présumé de contamination par le coronavirus COVID–19;
8° le numéro INAMI du médecin qui émet la forte suspicion;
9° l'indication de l'exercice ou du nonexercice de la profession de prestataire de soins;
10° la collectivité éventuelle dont la personne concernée fait partie ou avec laquelle elle est entrée en contact;
11° la date de l'apparition des symptômes;
12° les données nécessaires permettant au centre de contact de prendre tout contact utile avec la personne concernée, en ce compris le code postal et la langue.
Ces informations sont communiquées à Sciensano par le médecin qui a une forte suspicion que les Personnes de catégorie III soient infectées par le coronavirus COVID–19. Si le numéro d'identification du Registre national visé à l'article 8, § 1er, 1°, de la loi du 15 janvier 1990 sur la création et l'organisation d'une Banque Carrefour de la sécurité sociale est disponible, les nom et prénom, date de naissance, sexe et adresse sont extraits du Registre national ou des registres de la Banque Carrefour visés à l'article 4 de la loi du 15 janvier 1990 sur la création et l'organisation d'une Banque Carrefour de la sécurité sociale.
§ 5. La Base de données I contient, pour autant qu'elles soient disponibles, les catégories suivantes de données à caractère personnel relatives aux Personnes de catégorie IV (et le cas échéant, aux Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles étaient infectées, et aux Personnes de catégorie III) communiquées à Sciensano par les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes :
1° le numéro NISS;
2° le nom et le prénom;
3° le sexe;
4° la date de naissance et, le cas échéant, la date du décès;
5° l'adresse;
6° les coordonnées, en ce compris le numéro de téléphone et l'adresse électronique;
7° les données nécessaires permettant au centre de contact de prendre tout autre contact utile avec la personne visée au présent paragraphe et la liste des personnes avec lesquelles la personne visée au présent paragraphe a eu des contacts récents, en ce compris le code postal et la langue, ainsi que le risque estimé de contagion de la personne visée au présent paragraphe;
8° la liste des collectivités dont la personne visée au présent paragraphe fait partie ou avec lesquelles elle est entrée en contact, dont les données sont communiquées par la Base de données IV;
9° les critères pertinents permettant d'évaluer si le risque d'infection est élevé ou faible et de donner des conseils, en ce compris les symptômes éventuels, le moment où les symptômes sont apparus, le type de test de dépistage du coronavirus COVID–19 prescrit, la visite chez le médecin, l'enregistrement du refus éventuel de voir un médecin;
10° les informations pertinentes communiquées au centre de contact par la personne visée au présent paragraphe concernant les déplacements effectués, les symptômes et le suivi des mesures d'isolement, de prévention et d'hygiène;
11° le simple fait qu'il y ait eu contact entre les Personnes de catégorie IV et les Personnes de catégories I, II, III, y compris l'appartenance au ménage des Personnes de catégorie IV;
12° la réponse à la question de savoir si (i) les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles sont infectées ; (ii) les Personnes de catégorie III ; ou (iii) les Personnes de catégorie IV utilisent ou non une application numérique de traçage des contacts.

§ 6. La Base de données I contient les données complémentaires suivantes relatives aux Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles sont infectées, et aux Personnes de catégories III et IV collectées et fournies par les centres de contact compétents : toutes les données nécessaires à l'organisation et au suivi du contact avec la personne concernée par le personnel du centre de contact , telles que la langue de la personne concernée, le statut de contact de la personne concernée, les numéros de ticket des enregistrements de prise de contact ou des tentatives de prise de contact, les types de contact, l'heure des tickets, l'heure et la durée de la prise de contact, le résultat de la prise de contact.
§ 7. La Base de données I contient les données supplémentaires suivantes sur des personnes appartenant à un cluster, collectées et fournies par les équipes mobiles ou les inspections d'hygiène compétentes : toutes les données nécessaires à l'organisation et au suivi du contact pris avec la personne concernée dans le groupe par le personnel du centre de contact, telles que la langue de la personne concernée, le statut de contact de la personne concernée, les numéros de ticket des prises de contacts ou des tentatives de prise de contact, les types de prise de contact, l'heure des tickets, l'heure et la durée de la prise de contact, le résultat de la prise de contact.
Art. 7.
§ 1er La Base de données III contient les catégories de données à caractère personnel communiquées par Sciensano, à partir de la Base de données I, au centre de contact désigné par les entités fédérées compétentes ou par les agences compétentes, aux fins énoncées à l'article 3, § 1er, 1° et 2°.
§ 2. La Base de données III contient les catégories suivantes de données à caractère personnel relatives aux Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles sont infectées, et aux Personnes de catégorie III :
1° le numéro NISS;
2° le nom et le prénom;
3° le sexe;
4° la date de naissance;
5° les coordonnées, en ce compris l'adresse, le numéro de téléphone et l'adresse électronique, de la personne concernée, ainsi que des personnes à contacter en cas d'urgence;
6° les données nécessaires permettant au centre de contact de prendre tout contact utile avec la personne concernée, en ce compris le code postal et la langue;
7° l'indication que la personne doit être appelée par téléphone en tant que personne (présumée) infectée afin de retracer ses contacts;
8° le cas échéant, le résultat du test de dépistage du coronavirus COVID–19 et la date du test;
9° le numéro du ticket, la date, l'heure et le résultat de la prise de contact.
§ 3. La Base de données III contient les catégories suivantes de données à caractère personnel relatives aux Personnes de catégorie IV :
1° le numéro NISS;
2° le nom et le prénom;
3° le sexe;
4° la date de naissance et, le cas échéant, la date du décès;
5° l'adresse;
6° les coordonnées, en ce compris le numéro de téléphone et l'adresse électronique;
7° les données nécessaires permettant au centre de contact de prendre tout autre contact utile avec la personne visée au présent paragraphe et la liste des personnes avec lesquelles la personne

visée au présent paragraphe a eu des contacts récents, en ce compris le code postal et la langue de la personne visée au présent paragraphe;
8° la liste des collectivités dont la personne visée au présent paragraphe fait partie ou avec lesquelles elle est entrée en contact, dont les données sont communiquées par la Base de données IV;
9° les critères pertinents permettant d'évaluer si le risque d'infection est élevé ou faible et de donner des conseils, en ce compris les symptômes éventuels, le moment où les symptômes sont apparus, le type de test de dépistage du coronavirus COVID–19 prescrit, la visite chez le médecin, l'enregistrement du refus éventuel de voir un médecin;
10° les données pertinentes communiquées au centre de contact et aux équipes mobiles par la personne visée au présent paragraphe concernant les déplacements effectués, les symptômes et le suivi des mesures d'isolement, de prévention et d'hygiène;
11° le simple fait qu'il y ait eu contact entre la Personne de catégorie IV, en ce compris l'appartenance au ménage de celle-ci, et d'une part, les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a montré que ces personnes sont infectées, et, d' autre part, les Personnes de catégorie III.
§ 4. La Base de données III contient les catégories de données suivantes relatives aux Personnes de catégorie VI :
1° le nom, le type, les coordonnées de la collectivité;
2° les coordonnées du médecin de référence et/ou de la personne responsable de la collectivité, en ce compris ses nom, prénom et numéro de téléphone.

Art. 8.
§ 1er. La Base de données IV contient les catégories suivantes de données à caractère personnel relatives aux Personnes de catégories V et VI aux fins énoncées à l'article 3, § 1er, 2°,B:
1° le numéro d'identification provenant d'une source authentique, en particulier le Registre national et la Banque Carrefour de la sécurité sociale, et le numéro d'identification interne;
2° les nom, le type, l'adresse, le numéro figurant dans la Banque Carrefour des Entreprises, de la collectivité à laquelle la personne appartient ou avec laquelle elle a eu des contacts;
3° les coordonnées du médecin de référence et/ou de la personne responsable de la collectivité, en ce compris le nom, prénom et le numéro de téléphone.

Art. 9.
§ 1er. La Base de données II est complétée par les données à caractère personnel, relatives aux Personnes de catégories I, II et III, énumérées à l'article 6 mais uniquement après pseudonymisation, et exclusivement aux fins prévues à l'article 1er, § 2, 1°, h, à l'article 1er, § 2, 3° et à l'article 3, § 1er, 4°. Il s'agit plus précisément des catégories suivantes de données à caractère personnel :
1° un numéro unique qui ne permet pas d'identifier la personne;
2° l'année de naissance et, le cas échéant, l'année et le mois du décès;
3° le sexe;
4° le code postal;
5° le numéro INAMI du prescripteur du test de dépistage du coronavirus COVID–19;
6° le type, la date, le numéro d'échantillon et le résultat du test de dépistage du coronavirus COVID–19 ou le diagnostic présumé en l'absence de test de dépistage du coronavirus COVID–19 ;
7° le numéro INAMI du laboratoire qui a effectué le test de dépistage du coronavirus

COVID–19;
8° en cas de résultat de test de dépistage du coronavirus COVID–19 négatif, une éventuelle décision d'annulation par un médecin;
9° en cas de décision d'annulation d'un résultat de test négatif, le numéro INAMI du médecin qui a pris la décision d'annulation;
10° le cas échéant, le type et le code postal de la collectivité dont la personne fait partie ou avec laquelle elle est entrée en contact;
11° le résultat des examens médicaux, y compris le résultat du CT-scan;
12° l'indication de l'exercice ou non de la profession de prestataire de soins;
13° les données pertinentes pour le traçage des contacts, en ce compris les symptômes, la date des premiers symptômes, les déplacements, le suivi des mesures d'isolement et d'hygiène;
14° le simple fait -qu'il y ait eu contact, y compris le fait de faire partie du ménage, entre les Personnes de catégorie IV et, -d'une part, les Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé que ces personnes sont infectées, et, d'autre part les Personnes de catégorie III.
§ 2. La Base de données II est complétée par les données à caractère personnel, relatives aux Personnes de catégorie IV, énumérées à l'article 6 mais uniquement après pseudonymisation, et ce exclusivement aux fins énoncées à l'article 3, § 1er, 4°. Il s'agit plus précisément des données à caractère personnel suivantes :
1° un numéro unique qui ne permet pas d'identifier la personne;
2° l'année de naissance et, le cas échéant, l'année et le mois du décès;
3° le sexe;
4° les symptômes;
5° le contact ou l'absence de contact avec des personnes vulnérables;
6° le résultat et la date du test de dépistage du coronavirus COVID–19 prescrit;
7° l'exercice de la profession de prestataire de soins;
8° les données strictement nécessaires relatives à la prise de contact, en ce compris la date du ticket et le résultat général de la prise de contact sous la forme d'un code;
9° tous les critères pertinents pour estimer le risque élevé ou faible;
10° le code postal de l'adresse.

CHAPITRE V. — Accès et transmission des données à caractère personnel

Art. 10.
§ 1er. Les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, chacun dans leur domaine de compétence exclusif, n'ont accès qu'aux catégories de données à caractère personnel visées à l'article 7, § 2, § 3 et § 4 relatives aux Personnes de catégorie II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé qu'elles sont infectées, et relatives aux Personnes de catégories III, IV, et VI.
L'accès à ces données à caractère personnel n'est possible que pour les finalités mentionnées à l'article 3, § 1er, 1° à 3° compris, à l'article 3, § 2 notamment pour identifier et contacter le patient, la collectivité à laquelle il appartient ou avec laquelle il a été en contact et les personnes avec lesquelles il est entré en contact.
§ 2. Les équipes mobiles et les services d'inspection d'hygiène compétents des entités fédérées ont, chacun dans leur domaine de compétence exclusif, et uniquement aux fins mentionnées à l'article 3, § 1er, 3°, accès aux catégories de données à caractère personnel, relatives aux Personnes de catégories I, II, III, IV et si nécessaire des Personnes de catégories V et VI, visées

à l'article 6, dans la Base de données I, notamment dans le cadre d'initiatives visant à prévenir la propagation des effets néfastes causés par le coronavirus COVID–19.
§ 3. Les données à caractère personnel telles que communiquées et conservées dans la Base de données I, ne peuvent être transmises ultérieurement, après pseudonymisation, à la Base de données II, qu'aux fins définies à l'article 3, § 1er, 4°, conformément au Règlement Général sur la Protection des Données et à la loi du 5 septembre 2018 instituant le comité de sécurité de l'information. Les données à caractère personnel telles que communiquées et conservées dans la Base de données II, ne peuvent être transmises à des tiers aux fins stipulées à l'article 3, § 1er, 4° qu'après la délibération, visée à l'article 11, de la Chambre sécurité sociale et santé du Comité de sécurité de l'information.
§ 4. Tout accès des personnes physiques aux données à caractère personnel contenues dans les Bases de données conforme au § 1er jusqu'au § 3 du présent article ne peut avoir lieu que dans la mesure nécessaire aux tâches qui leur sont assignées afin de réaliser les finalités du traitement et que dans la mesure prévue dans le présent accord de coopération ainsi que dans la législation des entités fédérées.

CHAPITRE VI. — Compétence du Comité de sécurité de l'information

Art. 11.
§ 1er. Dans la mesure où cela n'est pas repris dans le présent accord de coopération, tant la communication de données à caractère personnel par type d'acteur à Sciensano pour traitement dans la Base de données I que la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers tels que prévus dans l'article 10 ont toujours lieu après délibération de la Chambre sécurité sociale et santé du Comité de sécurité de l'information visée dans la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement Général sur la Protection des Données.
§ 2. Sans préjudice de l'application du paragraphe 1er, la Chambre « sécurité sociale et santé » du Comité de sécurité de l'information ne délibère sur les communications à ou par la Base de données I de Sciensano que dans la mesure où elles servent les fins visées à l'article 3, sans que la Chambre « sécurité sociale et santé » du Comité de sécurité de l'information puisse déterminer elle-même une autre fin.
§ 3. La Chambre « sécurité sociale et santé » du Comité de la sécurité de l'information peut préciser, pour chaque finalité de traitement définie à l'article 3, quelles données à caractère personnel relevant d'une certaine catégorie de données à caractère personnel peuvent être traitées et communiquées à l'une des Base de données II, III et IV ou qui doivent être communiquées à partir de la Base de données IV à la Base de données I , dans la mesure où cela est utile afin d'atteindre la finalité du traitement en question. Cette compétence est exercée conformément à l'article 46 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.
Si, sur la base de cette compétence, la Chambre « sécurité sociale et santé » du Comité de sécurité de l'information détermine ou complète les données à caractère personnel dans la catégorie de données à caractère personnel définie à l'article 6 ci-dessus, Sciensano l'indiquera clairement sur son site web conformément aux dispositions du Règlement Général sur la Protection des Données en matière de transparence.
§ 4. Conformément à l'article 1er, § 5, et sans préjudice de l'application des paragraphes 1er, 2 et 3, les points suivants peuvent être clarifiés, modifiés ou complétés par le biais d'un accord de coopération d'exécution tel que prévu à l'article 92bis, § 1er, troisième alinéa, de la loi spéciale

du 8 août 1980 de réformes institutionnelles :
1° les institutions qui peuvent être comprises sous le vocable de collectivités,
2° les catégories de fournisseurs d'informations qui doivent de façon obligatoire communiquer des données à caractère personnel à Sciensano pour enregistrement et traitement ultérieur dans la base de données définie à l'article 2, § 1er, et
3° les catégories de données à caractère personnel traitées dans les bases de données visées à l'article 2.

Art. 12.
§ 1er. Dans le cadre de ses compétences définies à l'article 11, § 3, la Chambre « sécurité sociale et santé » du Comité de sécurité de l'information précise les règles en la matière et définit au moins les éléments suivants :
1° les données à caractère personnel supplémentaires qui doivent être demandées et la finalité de traitement, parmi les finalités de traitement définies à l'article 3, pour laquelle des données à caractère personnel supplémentaires doivent être demandées;
2° l'identité du responsable du traitement;
3° de quelles catégories définies aux articles 6, 7, 8 et 9 relèvent les données à caractère personnel supplémentaires, dans la mesure où elles sont adéquates, pertinentes et limitées à ce qui est nécessaire pour la finalité de traitement telle que définie au 1°;
4° les catégories de personnes visées à l'article 4 à propos desquelles des données à caractère personnel supplémentaires sont traitées;
5° les mesures visant à garantir un traitement licite et loyal des données à caractère personnel;
6° la manière dont les personnes dont les données à caractère personnel sont traitées sont informées de ce traitement conformément au présent accord de coopération.
§ 2. L'accès au Registre national visé à l'article 1er de la loi du 8 août 1983 organisant un Registre national des personnes physiques et aux registres de la Banque Carrefour visés à l'article 4 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale est accordé exclusivement pour les finalités de traitement visées à l'article 3.
§ 3. La communication de données à caractère personnel provenant d'autres sources authentiques à la Base de données I, requiert une délibération de la Chambre sécurité sociale et santé du Comité de sécurité de l'information. Une telle communication ne sera possible qu'à condition que la communication de données à caractère personnel supplémentaires soit nécessaire pour les finalités de traitement décrites à l'article 3.

CHAPITRE VII. — Mesures de sécurité

Art. 13.
§ 1er. Sciensano, en ce qui concerne les Bases de données I et II, et les entités fédérées compétentes ou les agences désignées par les entités fédérées compétentes, en ce qui concerne les Bases de données III et IV, mettent en œuvre les mesures techniques et organisationnelles appropriées, conformément à l'article 32 du Règlement Général sur la Protection des Données, afin de garantir un niveau de sécurité adapté au risque. Ces mesures seront précisées par le biais d'un protocole d'accord.
§ 2. Sciensano, en ce qui concerne les Bases de données I et II, et les entités fédérées compétentes ou les agences désignées par les entités fédérées, en ce qui concerne les Bases de données III et IV, respecteront les principes de protection des données dès la conception et de protection des

données par défaut, tels que définis à l'article 25 du Règlement Général sur la Protection des Données. Ces principes seront précisées par le biais d'un protocole d'accord.

CHAPITRE VIII Applications numériques de traçage des contacts

Art. 14.
§ 1er. L'application numérique de traçage des contacts pour prévenir la propagation du coronavirus COVID–19 dans la population vise à informer les utilisateurs qu'ils ont eu un contact à risque avec un autre utilisateur infecté, sans que l'utilisateur infecté soit identifié par l'application numérique de traçage des contacts, et avec l'objectif supplémentaire que l'utilisateur averti prenne alors volontairement les mesures nécessaires, sur la base des recommandations de Sciensano et des entités fédérées compétentes, pour prévenir la propagation du coronavirus COVID–19.
§ 2. L'application numérique de traçage des contacts se limite au traitement des informations qui doivent permettre :
1° que les contacts entre les utilisateurs de l'application numérique de traçage des contacts soient captés sans qu'il soit possible de retracer l'identité d'un utilisateur;
2° à un utilisateur de pouvoir signaler l'infection du coronavirus COVID–19 de manière volontaire, anonymisée, ou au moins pseudonymisée, par le biais d'un acte positif de sa part si cet utilisateur entre dans la catégorie
i. des Personnes de catégories II, dans la mesure où le test de dépistage du coronavirus COVID–19 a révélé que cet utilisateur est infecté, ou
ii. des Personnes de catégorie III;
3° que les utilisateurs de l'application numérique de traçage des contacts soient avertis lorsqu'ils se sont trouvés pendant un certain temps à proximité d'un utilisateur infecté par le coronavirus COVID–19 qui l'a signalé conformément aux dispositions du 2°.
§ 3. L'application numérique de traçage des contacts doit répondre aux conditions minimales suivantes :
1° l'application numérique de traçage des contacts est développée en prenant comme référence le protocole DP3T (Decentralized Privacy-Preserving Proximity Tracing);
2° l'application numérique de traçage des contacts consiste en une application mobile installée par l'utilisateur sur son appareil et en un journal central des enregistrements, à savoir la Base de données V, qui permet un fonctionnement contrôlé de l'application numérique de traçage des contacts tel que défini au paragraphe 2, 2° et 3°;
3° Sciensano est le responsable du traitement de de la Base de données V ;
4° l'application numérique de traçage des contacts peut assurer l'interopérabilité avec d'autres États membres européens, des pays qui font partie de l'Espace économique européen ou des pays qui ont été considérés comme ayant un niveau de protection des données adéquat par la Commission européenne, tel que défini dans le Règlement Général sur la Protection des Données (décision d'adéquation), qui utilisent également le protocole visé au 1° et qui offrent des garanties de protection des données identiques ou équivalentes;
5° la communication entre appareils sur lesquels l'application mobile de l'application numérique de traçage des contacts a été installée s'effectue uniquement sur la base de données qui ne permettent pas d'identifier l'utilisateur;
6° l'application numérique de traçage des contacts permet à un utilisateur, dont l'infection par le coronavirus COVID–19 a été constatée, d'utiliser un code d'autorisation, afin de garantir que seules des informations validées concernant les infections puissent être communiquées au

responsable du traitement de la Base de données V, évitant ainsi les fausses notifications et les notifications erronées et accidentelles d'une infection via l'application numérique de traçage des contacts;
7° l'application numérique de traçage des contacts garantit que seul le fait de l'infection, ainsi que la date à laquelle l'utilisateur est suspecté d'être devenu contagieux, sont communiqués au responsable du traitement de la Base de données V, et cela de telle sorte que l'identité de l'utilisateur ne puisse être retracée;
8° l'application numérique de traçage des contacts permet aux utilisateurs de désactiver, temporairement ou définitivement, l'application mobile de l'application numérique de traçage des contacts qu'ils utilisent sur leur appareil. L'application mobile de l'application numérique de traçage des contacts peut être désactivée à tout moment par l'utilisateur, avec la garantie que la désinstallation de l'application mobile de l'application numérique de traçage des contacts ne sera pas plus difficile que son installation, et en veillant également à ce que les utilisateurs soient informés lorsque, comme décrit au § 3, 9º et 10º, la Base de données V est désactivée et que l'utilisation de l'application mobile de l'application numérique de traçage des contacts n'est plus recommandée, afin que, sur la base de ces informations, l'utilisateur puisse alors décider volontairement de désactiver ou de supprimer de l'application mobile de l'application numérique de traçage des contacts sur son appareil;
9° l'utilisateur doit pouvoir transmettre volontairement et de manière autorisée un constat d'infection via l'application mobile de l'application numérique de traçage des contacts à la Base de données V, sans que l'identité de l'utilisateur puisse être retracée, et de telle sorte que les éventuelles données à caractère personnel nécessaires pour permettre à un utilisateur de s'authentifier lorsqu'il souhaite signaler une infection soient conservées, si possible en dehors de l'application de traçage des contacts, et en tout cas ne soient, quoi qu'il en soit, jamais transmises à la Base de données V, et soient effacées de l'application mobile de l'application numérique de traçage des contacts immédiatement après une authentification réussie;
10° aucune donnée de géolocalisation n'est, de quelque manière que ce soit, utilisée ou traitée dans l'application numérique de traçage des contacts;
11° lorsqu'un utilisateur est informé d'un contact avec un utilisateur infecté, aucun détail qui permettrait d'identifier l'utilisateur infecté n'est communiqué;
12° le code source de l'application numérique de traçage des contacts, est rendu public, avant le lancement et l'entrée en vigueur de l'application numérique de traçage des contacts;
13° l'accès à la Base de données V est limité aux personnes autorisées du responsable du traitement, à savoir Sciensano, et à ses fournisseurs de services TIC qui contribuerait au fonctionnement de la Base de données, où cet accès sera en outre strictement limité au nombre minimal pour garantir le fonctionnement de l'application -numérique de traçage des contacts telle que décrite au § 2, 2° et 3°.
§ 4. L'application numérique de traçage des contacts respecte les principes énoncés aux articles 5 et 25 du Règlement Général sur la Protection des Données.
Seules les données nécessaires pour confirmer l'infection au coronavirus COVID–19 d'un utilisateur et pour avertir les utilisateurs de l'application numérique de traçage des contacts qu'ils se sont trouvés pendant un certain temps à proximité d'une personne infectée par le coronavirus COVID–19 peuvent être traitées, en tenant compte des principes de protection des données dès la conception et par défaut.
Ces catégories de données sont énumérées de manière exhaustive dans le présent accord de coopération ou, le cas échéant, dans les accords de coopérations d'exécution visés à l'article 1, § 5.

§ 5. L'installation, l'utilisation et la désinstallation de l'application numérique de traçage des contacts par un utilisateur se fait exclusivement de manière volontaire.
L'installation ou non, l'utilisation ou non et la désinstallation ou non de l'application mobile de l'application numérique de traçage des contacts ne peuvent donner lieu à aucune mesure de nature civile ou pénale, à aucun acte discriminatoire, ni à aucun avantage ou désavantage. Une violation de ces principes ou le fait pour une autorité, une entreprise ou un individu d'obliger un autre individu à installer, utiliser et désinstaller l'application numérique de traçage des contacts sera sanctionné en vertu du droit commun.
§ 6. Toutes les données relatives aux contacts entre utilisateurs, stockées sur l'appareil de l'utilisateur, sont supprimées au plus tard trois semaines après avoir été générées sur le dispositif de l'utilisateur d'une application numérique de traçage des contacts.
Les données qui aboutissent dans la Base de données V ne peuvent plus être utilisées par l'application mobile et numérique de traçage des contacts sur l'appareil de l'utilisateur. Les informations conservées dans la Base de données V doivent être supprimées au plus tard trois semaines après leur enregistrement dans cette Base de données.
Les données liées à la communication volontaire d'une infection au coronavirus COVID–19 constatée ainsi que les données utilisées pour l'authentification de la personne infectée, dans la mesure où ces informations sont traitées en application du paragraphe 2, 2°, doivent être effacées immédiatement sur l'appareil de l'utilisateur après avoir été saisies dans l'application numérique de traçage des contacts.
§ 7. Ni l'application numérique de traçage des contacts, ni les données traitées au moyen de celle-ci ne peuvent être utilisées à d'autres fins que celles prévues au paragraphe 1er, notamment mais pas exclusivement, à des fins policières, commerciales, fiscales, pénales ou de sûreté de l'État.
§ 8. Une analyse d'impact relative à la protection des données est établie et publiée en application des articles 35 et 36 du Règlement Général sur la Protection des Données.
§ 9. Ce sont les entités fédérées qui décident quelle(s) application(s) mobile(s) sont mises à la disposition des utilisateurs dans le cadre du traçage de contacts par les autorités et qui en contrôlent la conformité avec la réglementation. Les procédures à cet égard, ainsi que la poursuite du fonctionnement de l'application numérique de traçage des contacts et les traitements de données utiles dans ce cadre sont réglés par un accord de coopération d'exécution visé à l'article 92bis, § 1er, alinéa 3, de la loi spéciale du 8 août 1980 de réformes institutionnelles, sans préjudice des dispositions du présent article. Cet accord de coopération d'exécution contient au minimum :
1° une description du système de traçage, notamment pour s'assurer que les risques qui sont limités par le protocole DP3T de référence ne sont pas réintroduits par l'application numérique de traçage des contacts et/ou un système permettant la réidentification;
2° une description claire des traitements résultant de l'utilisation de l'application numérique de traçage des contacts et une définition claire des concepts importants tels que le contact à risque, le code d'autorisation, la clé sécurisée et le numéro de série temporaire non personnalisé;
3° les spécifications techniques auxquelles l'application numérique de traçage des contacts devra se conformer;
4° les spécifications nécessaires pour assurer l'interopérabilité avec d'autres États membres européens, des pays qui font partie de l'Espace économique européen ou des pays qui ont été désignés comme ayant un niveau de protection des données adéquat par la Commission européenne, comme défini dans le Règlement Général sur la Protection des Données (décision d'adéquation), qui utilisent également le protocole visé au 1° et qui offrent des garanties

identiques ou équivalentes en matière de protection des données;
5° les garanties spécifiques pour limiter le risque de réidentification sur la base de l'authentification de l'utilisateur infecté, par exemple par l'utilisation d'une banque de données « tampon », dont le fonctionnement est décrit dans l'accord de coopération d'exécution ;
6° la manière dont les personnes concernées sont informées du fonctionnement des applications numériques de traçage des contacts et de l'échange des données qu'elles génèrent;
7° la procédure de contrôle du bon fonctionnement de l'application numérique de traçage des contacts.

CHAPITRE IX. — Délai de conservation

Art. 15.
§ 1er. Sous réserve des dispositions du paragraphe 2, les données à caractère personnel seront supprimées de la Base de données I au plus tard soixante jours après leur enregistrement. Les données à caractère personnel de la Base de données III sont supprimées quotidiennement. Après la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus COVID–19, les données à caractère personnel de la Base de données IV seront transférées aux entités fédérées compétentes pour l'exercice de leur compétence en matière de détection des maladies infectieuses, dans le cadre des compétences matérielles dans le domaine des soins de santé préventifs conformément au § 3 du présent article. Les données sauvegardées dans la Base de données V sont supprimées après trois semaines au plus tard, conformément aux dispositions de l'article 14, § 6.
§ 2. Les données à caractère personnel pseudonymisées telles que définies à l'article 10, § 3, qui sont transmises pour la finalité de traitement définie à l'article 3, § 1er, 4°, seront supprimées conformément au délai généralement accepté pour la conservation des dossiers concernant la santé et dans le cadre de la recherche scientifique en matière de santé, à savoir trente ans.
§ 3. À l'exception des données des Bases de données II et IV, les Bases de données et leur fonctionnement seront en tout cas désactivées, supprimées ou effacées par le responsable du traitement au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus COVID–19. Conformément au § 1 du présent article, les données à caractère personnelle dans la Base de données IV seront transférées aux entités fédérées au plus tard cinq jours après le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus COVID–19.

CHAPITRE X. — Transparence et droits des personnes concernées

Art. 16.
§ 1er. Sciensano, en tant que responsable du traitement des Bases de données I et II, prend les mesures appropriées afin que les personnes concernées reçoivent les informations visées aux articles 13 et 14 du Règlement Général sur la Protection des Données et la communication visée aux articles 15 à 22 inclus et à l'article 34 du Règlement Général sur la Protection des Données en rapport avec le traitement aux fins prévues à l'article 3. Ces informations doivent être fournies dans un langage clair et simple et sous une forme concise, transparente, compréhensible et facilement accessible.
§ 2. Sciensano crée et assure la maintenance d'un site web destiné aux personnes concernées visées à l'article 4 sur lequel sont publiées des informations adéquates conformément à l'article 14 du Règlement Général sur la Protection des Données et les données de contact du délégué

à la protection des données.
§ 3. Sciensano gère et assure la maintenance d'un système pour l'exercice des droits prévus aux articles 15 à 22 inclus et à l'article 34 du Règlement Général sur la Protection des Données.
§ 4. Sciensano, les entités fédérées compétentes et les agences désignées par les entités fédérées compétentes, chacune dans son domaine de compétence, définissent de manière transparente leurs responsabilités respectives, notamment en ce qui concerne l'exercice des droits de la personne concernée et la fourniture d'informations. À cette fin, Sciensano, les entités fédérées compétentes et les agences désignées par les entités fédérées compétentes concluent un protocole d'accord définissant les rôles et les relations respectives des responsables conjoints du traitement vis-à-vis des personnes concernées.

CHAPITRE XI. — Dispositions diverses

Art. 17.
Les litiges entre les parties au présent accord concernant l'interprétation et l'exécution de cet accord de coopération sont soumis à une juridiction de coopération au sens de l'article 92bis, § 5, de la loi spéciale du 8 août 1980 de réformes institutionnelles. Le mode de désignation des membres du tribunal de coopération sera déterminé dans un protocole d'accord de coopération d'exécution. Les frais de fonctionnement du tribunal de coopération seront divisés à parts égales entre les parties à cet accord de coopération d'exécution.

Art. 18.
§ 1er. La Conférence interministérielle santé publique surveille la mise en œuvre et le respect de cet accord de coopération et, le cas échéant, soumet des propositions d'adaptation. Le Conférence interministérielle santé publique exerce également une fonction de médiation dans le cadre de cet accord de coopération avant que les litiges ne soient soumis à un tribunal de coopération, comme le stipule l'article 17.
§ 2. La Conférence interministérielle santé publique se réunit dès qu'une partie à l'accord de coopération en fait la demande.

Art. 19.
§ 1er. Le présent accord de coopération entre en vigueur le 4 mai 2020 en ce qui concerne les dispositions correspondant en substance à l'arrêté royal nº 18 du 4 mai 2020 portant création d'une base de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID–19, tel que modifié par l'arrêté royal n° 25 du 28 mai 2020 modifiant l'arrêté royal n° 18 du 4 mai 2020 portant création d'une base de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID–19. L'article 14 ainsi que les dispositions relatives aux applications numériques de traçage des contacts entrent en vigueur le 29 juin 2020, en ce qui concerne les dispositions correspondant en substance à l'arrêté royal nº 44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignes par les entités fédérées compétentes ou par les agences compétentes par les inspections sanitaires et les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID–19 sur la base d'une base de données auprès de Sciensano, tel qu'applicable à partir du 29 juin 2020.
§ 2. Sous réserve des dispositions de l'article 15, § 2 et § 3, les mesures apportées par cet accord de coopération prendront fin le jour de la publication de l'arrêté royal proclamant la fin de l'épidémie du coronavirus COVID–19.

§ 3. Sans préjudice du paragraphe 2, l'accord de coopération sera résilié par le biais d'un nouvel accord de coopération, qui sera porté à la connaissance des citoyens.
Fait à Bruxelles, le 25 août 2020, en un exemplaire original.

Pour l'Etat fédéral : La Première Ministre, S. WILMES
La Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration, M. DE BLOCK

Pour la Communauté flamande : Pour le Ministre-Président, absent : Le Vice-ministre-président du Gouvernement flamand et Ministre flamand de l'Enseignement, des Sports, du Bien-Être des Animaux et du Vlaamse Rand, B. WEYTS
Le Ministre du Bien-être, de la Santé publique, de la Famille et de la Lutte contre la pauvreté W. BEKE

Pour la Région wallonne : Le Ministre-président E. DI RUPO
La Ministre de l'Emploi, de la Formation, de la Santé, de l'Action sociale, de l'Égalité des chances Ch. MORREALE

Pour la Commission communautaire commune : Le Président du Collège réuni, R. VERVOORT
Le Membre du Collège réuni, compétent pour l'Action sociale et la Santé A. MARON
Le Membre du Collège réuni, compétent pour l'Action sociale et la Santé E. VAN DEN BRANDT

Pour la Communauté germanophone : Le Ministre-président O. PAASCH
Le Vice-ministre-président et Ministre de la Santé et des Affaires sociales, de l'Aménagement du territoire et du Logement, A. ANTONIADIS

Council of Europe, Joint Statement on Digital Contact Tracing, Strasbourg 28th April 2020

Join statement Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe.
One month after our first Joint Declaration on the right to data protection in the context of the COVID-19 pandemic, countries and peoples around the world continue to relentlessly invest all efforts in preventing further propagation of the virus. Since the start of the pandemic, governments and stakeholders involved in the fight against the virus, such as the scientific research community, have been relying on data analytics and digital technologies to address this novel threat. Recalling that the data protection standards laid down by Convention 108 and its modernised version, Convention 108, are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health, it is crucial to ensure that the necessary data protection safeguards are implemented when adopting extraordinary measures to protect public health. Regarding the use of mobile data and technology in the fight against COVID-19, specific measures are being deployed or otherwise proposed and include: use of mobile location data to evaluate movements of population or to enforce confinement measures, use of devices as digital proof of immunity, symptoms' detection, self-testing, or finally digital tracing of the contacts of an infected person.
All those innovative, or less innovative tools, rely on people possessing and carrying with them appropriate mobile devices. For example, people that do not possess a suitable mobile device will be excluded from such approaches. Furthermore, those tools which rely on the processing of personal data, have an impact on the privacy and data protection, and other fundamental rights and freedoms of individuals. It is crucial, therefore,to ensure that the measures and related data processing are necessary and proportionate in relation to the legitimate purpose pursued and that they reflect, at all stages, a fair balance between all interests concerned, and the rights and freedoms at stake, as the European Convention on Human Rights (Article 8) and Convention 108 (Articles5 and 11) prescribe. Looking at contact tracing (and alerting) in particular, it should first and foremost be recalled that this monitoring process has always been used –manually -in epidemic monitoring to reduce the spread of infections; identifying the persons who may have come into contact with an infected person to alert them, where necessary, and allow them to get the necessary care and self-isolate to avoid further spread of the disease. Mobile applications are now seen by many as a complementary response to the need to rapidly perform such contact monitoring. Indeed, mobile solutions that enable the automatic detection of contacts would save precious hours of work of public health staff tracing the chain of infection, could fill in important gaps that human memory would not be able to, and could do so with rapidity that matches the speed of the virus. Although technological tools can play an important role in addressing the current challenge, the first –essential –question we have task ourselves before systematic and uncritical adoption of technology (not having assessed their effectiveness and proportionality) is: are those "Apps" the solution? Considering the absence of evidence of their efficacy, are the promises worth the predictable societal and legal risks? Where governments decide to resort to this digital contact tracing in their management of the COVID-19 pandemic, what are the legal and technical safeguards that have to be in place to mitigate the risks at stake?

I. Effectiveness
As already spelt-out in the first joint declaration, "large-scale personal data processing can only

be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance (e.g. contact tracking), including their accuracy, override the benefits of other alternative solutions which would be less intrusive. The effectiveness of digital contact tracing depends on a multiplicity of factors, which are interrelated:

- a comprehensive national epidemiologic strategy articulating instrumental support to the public health system, manual contact tracing and a strong emphasis on widespread testing; - the model chosen (technology used, architecture retained, definition of 'proximity' between the devices, both in terms of distance and duration, etc.); and
- widespread access to mobile devices and connection (which may also require specific technical functionalities such as "Bluetooth low energy"), while regretfully acknowledging that considerable segments of the population are unable to acquire or use them, in particular high-risk groups such as the elderly. Where public authorities decide to use digital contact tracing, the following sections should guide the design and implementation of those systems, with the adoption of the corresponding appropriate legal framework to regulate the system.

II. Trust and voluntariness

The acceptability of a digital contact tracing system clearly depends on the trust that such a system can inspire, and deliver. As public trust is essential for the broad adoption of the system, it is important to highlight that trust can be significantly strengthened through the integration of privacy enhancing features, and transparent information of the persons, regarding in particular the functioning of the system, its purpose and the data processed. Achieving broad acceptability can thus be supported by implementing a trustworthy system, which is not imposed upon people but used on a voluntary basis instead. This also means that there should be no negative consequences imposed for not participating in the system. Voluntariness does not mean that the processing of personal data will necessarily be based on consent as its legal basis. Convention 108 allows the processing on grounds of public interest, including public health, provided for by law. Therefore, national laws, promoting a genuine voluntary recourse to such systems, would constitute an appropriate legal ground for this processing provided that the needed safeguards are put in place.

III. Impact assessment and privacy by design

Considering the likely impact of digital contact tracing systems on the rights and fundamental freedoms of individuals, their development should be based on a prior assessment of such a likely impact prior to their deployment. Their design should be done in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms, to ensure notably that location data of individuals are not used, that no direct identification is possible, that re-identification is prevented.

IV. Purpose specification

The purpose of a COVID-19 digital contact tracing system is to identify persons potentially exposed to the virus and strictly excludes further processing of data for any unrelated purposes (e.g., commercial or law enforcement purposes).

V. Data: sensitivity, quality, minimisation

Health-related data are a special category of data which can only be processed where appropriate safeguards, which complement the other data protection requirements, are provided as

enshrined in Article 6 of Convention 108. Considering the particular nature of location data, and the fact that proximity between persons can be obtained without locating them, digital contact tracing should be done on the basis of records of connections between devices rather than on the basis of location data (GPS generated data for instance). As the implications may be serious (self-isolation, testing) for the individuals identified as potential contacts of someone infected, ensuring the quality and accuracy of data is crucial. Data processed for digital contact tracing purposes should be reduced to the strictest minimum and any data that is not related or necessary should not be collected.

VI. Automated decision-making
Even in the current situation, individuals retain the right not to be subject to a decision significantly affecting them based solely on an automated processing of data without having their views taken into consideration. It is clear that implications such as self-isolation and testing can have such significant effects. Users of the digital tracing system must therefore not have consequences imposed on them without a clear facility to challenge these consequences, particularly in light of the inaccuracies or misrepresentations possible in such systems.

VII. De-identification
Users of the digital tracing system must not be directly identified, and digital contact tracing systems should only use unique and pseudonymised identifiers, generated by and specific to the system. Those identifiers must be renewed regularly and must be cryptographically strong.

VIII. Security
Digital contact tracing systems have to include state-of-the-art encryption, communications security, secure development practices and user authentication to prevent from risks such as access, modification or disclosure of the data of the digital contact tracing system.

IX. Architecture
Digital contact tracing systems should be based on an architecture which relies as much as possible on the processing and storing of data on devices of the individual users. Several models of centralised, partially centralised or decentralised architectures exist but none completely prevents from vulnerabilities and risks of re-identification.

X. Interoperability
Since the COVID-19pandemicknows no frontiers, interoperability between systems should be ensured to enable the exchange of available information beyond national borders, provided that the necessary safeguards are ensured, including appropriate grounds for transferring data, robust security measures, and means to ensure accuracy of inbound and outbound data.

XI. Transparency
In light of the intrusiveness of digital contact tracing systems, full transparency through an open source development of the code is highly recommended, enabling anyone interested to audit(and possibly improve) the code.
Information provided to individuals should use clear and simple plain language. Individuals have the right to obtain knowledge of the reasoning underlying data processing where results are applied to them, such as in the case of digital contact tracing. The general manner in which a particular digital tracing system works must be made fully public before and during

operation.

XII. Temporariness

The data used for digital contact tracing should only be kept for the duration of the management of the COVID-19 pandemic and storage limitation periods should be defined in light of the epidemiological relevance of the data (such as the incubation time of the virus for instance). At the term of that pre-defined period, all personal data should be deleted and technical measures enabling the automatic deactivation of the application and deletion of the data are to be supported.

XIII. Oversight and Audit

Digital contact tracing systems should be subject to independent and effective oversight and audits to ensure respect of the rights to privacy and data protection. Data protection authorities should be involved from the outset in the development of those systems, and use their powers of intervention and investigation to ensure that data protection requirements are enforced. The COVID-19 pandemic creates unprecedented common challenges which require our greatest commitment, and caution. What is ahead of us belongs to political choices, to societal support and to our individual commitment. Despite the urgency, digital contact tracing raises new questions that cannot be neglected before deciding to implement such population wide measures. Beyond privacy and data protection considerations, digital contact tracing approaches raise questions of inequality and discrimination that also have to be considered.

Council of Europe, Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, Strasbourg, 30 March 2020

The COVID-19 pandemic (more commonly known as Coronavirus) poses unprecedented threats and challenges for individuals, and countries around the world. The need to stop its spread and cure those who are suffering is a prominent goal shared by nations globally. The efforts deployed by the World Health Organisation, other international organisations, governments, health-care institutions and their staff as well as businesses to prevent an even larger scale propagation of the virus, to save people, and protect the society are limitless and should be strongly supported. States have to address the threat resulting from the COVID-19 pandemic in respect of democracy, rule of law and human rights, including the rights to privacy and data protection. In the effort of curbing the number of new contaminations, governments have had to resort to extraordinary measures, including the declaration of a state of emergency in many cases. While the alarming public health situation of those countries has justified the introduction of specific regimes, it should be stressed that, during those limited periods, the exercise of human rights, as enshrined in several international (such as the International Covenant on Civil and Political Rights and the European Convention on Human Rights) and national instruments is applicable and cannot be suspended but only derogated or restricted by law, to the extent strictly required by the exigencies of the situation while respecting the essence of the fundamental rights and freedoms.

General data protection principles and rules

When it comes to the right to data protection, it should first of all be noted that Convention 108, as well as the modernised "Convention 108+",set forth high standards for the protection of personal data which are compatible and reconcilable with other fundamental rights and relevant public interests. It is important to recall that data protection can in no manner be an obstacle to saving lives and that the applicable principles always allow for a balancing of the interests at stake. In accordance with Convention 108+ it is crucial, that even in particularly difficult situations, data protection principles are respected and therefore it is ensured that data subjects are made aware of the processing of personal data related to them; processing of personal data is carried out only if necessary and proportionate to the explicit, specified and legitimate purpose pursued; an impact assessment is carried out before the processing is started; privacy by design is ensured and appropriate measures are adopted to protect the security of data, in particular when related to special categories of data such as health related data; data subjects are entitled to exercise their rights. One of the main data protection principles provided for by Convention 108+is the principle of lawfulness, according to which processing of data can be carried out either on the basis of the data subject's consent or some other legitimate basis laid down by law. It should be noted that, as explicitly provided by the Explanatory Report to Convention 108+, such legitimate basis notably encompasses data processing necessary for the vital interests of individuals, and data processing carried out on the basis of grounds of public interest, such as in the case of monitoring of life-threatening epidemic. The right to data protection for instance does not prevent public health authorities to share the list of health professionals (names and contact details) with entities tasked with the distribution of FFP2 masks. Neither can the right to data protection be claimed to be incompatible with epidemiologic monitoring, stressing that anonymised data is not covered

by data protection requirements. The use of aggregate location information to signal gatherings infringing confinement requirements or to indicate movements of persons traveling away from a severely touched area (in terms of number of COVID-19 positive persons) would thus not be prevented by data protection requirements. Furthermore, "Convention 108+" acknowledges the need to allow some exceptions and restrictions in the name of pressing objectives of public interest and individuals' vital interests. Nevertheless, restrictions to its principles and rights must respond to very clear requirements, even during the state of emergency, to ensure the persisting respect of the rule of law and fundamental rights.

European Union, Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic (Text with EEA relevance). C/2020/4934. *OJ L 227I , 16.7.2020*

COMMISSION IMPLEMENTING DECISION (EU) 2020/1023 of 15 July 2020
amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic
(Text with EEA relevance)

THE EUROPEAN COMMISSION,
Having regard to the Treaty on the Functioning of the European Union,
Having regard to Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, and in particular Article 14(3) thereof,

Whereas:
(1) Article 14 of Directive 2011/24/EU assigned the Union to support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth (the 'eHealth Network') designated by the Member States.

(2) Commission Implementing Decision (EU) 2019/1765 (2) provides for the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth. Article 4 of that Decision entrusts the eHealth Network with the task of facilitating greater interoperability of the national information and communications technology systems and cross-border transferability of electronic health data in cross-border healthcare.

(3) In the light of the public health crisis caused by the COVID-19 pandemic, several Member States have developed mobile applications that support contact tracing and enable the users of such applications to be alerted to take appropriate action, such as testing or self-isolating, if they have been potentially exposed to the virus through proximity to another user of such applications, who has reported a positive diagnosis. These applications rely on Bluetooth technology to detect proximity between devices. As restrictions on travel between Member States have been lifted since June 2020, greater interoperability of the national information and communications technology systems should be achieved between the Member States in the eHealth Network, by implementing a digital infrastructure enabling interoperability between national mobile applications supporting contact tracing and warning.

(4) The Commission has been supporting Member States as regards the mobile applications mentioned above. On 8 April 2020, the Commission adopted a Recommendation 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 (the 'Commission Recommendation'). The Member States in the eHealth

Network adopted, with the Commission's support, a Common EU toolbox for Member States on mobile applications to support contact tracing as well as interoperability guidelines for approved contact tracing mobile applications in the EU. The toolbox explains the national requirements for national contact tracing and warning mobile applications, in particular that they should be voluntary, approved by the respective national health authority, privacy-preserving, and dismantled as soon as no longer needed. Following the most recent developments of the COVID-19 crisis, the Commission and the European Data Protection Board have each issued guidance on mobile applications and contact tracing tools in relation to data protection. The design of Member States' mobile applications and of the digital infrastructure enabling their interoperability builds upon the Common EU toolbox, the above-mentioned guidance, and the technical specifications agreed in the eHealth Network.

(5) In order to facilitate the interoperability of national contact tracing and warning mobile applications, a digital infrastructure was developed with the support of the Commission by the Member States participating in the eHealth Network which decided to advance their cooperation in this area on a voluntary basis, as an IT tool for exchange of data. This digital infrastructure is referred to as 'the federation gateway'.

(6) This Decision lays down provisions on the role of the participating Member States and of the Commission for the functioning of the federation gateway for the cross-border interoperability of national contact tracing and warning mobile applications.

(7) Processing of personal data of application users of contact tracing and warning mobile applications, which is done under the responsibility of the Member States or other public organisations or official bodies in the Member States, should be carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council ('the General Data Protection Regulation') and Directive 2002/58/EC of the European Parliament and of the Council. Processing of personal data under the responsibility of the Commission for the purpose of managing and ensuring the security of the federation gateway should comply with Regulation (EU) 2018/1725 of the European Parliament and of the Council.

(8) The federation gateway should consist of a secure IT infrastructure providing a common interface, where designated national authorities or official bodies can exchange a minimum set of data in relation to contacts with persons infected by SARS-CoV-2, in order to inform others on their potential exposure to that infection and promoting effective cooperation on healthcare between Member States by facilitating the exchange of relevant information.

(9) This Decision should therefore lay down modalities for the cross-border exchange of data between designated national authorities or official bodies through the federation gateway within the EU.

(10) The participating Member States, represented by the designated national authorities or official bodies determine together the purpose and means of processing of personal data through the federation gateway and are therefore joint controllers. Article 26 of the General Data Protection Regulation places an obligation on joint controllers of personal data processing operations to determine, in a transparent manner, their respective responsibilities for compliance with the obligations under that Regulation. It also provides for the possibility to

have those responsibilities determined by Union or Member State law to which the controllers are subject. Each of the controllers should ensure that they have a legal basis at national level for processing in the federation gateway.

(11) The Commission, as a provider of technical and organisational solutions for the federation gateway, processes pseudonymised personal data on behalf of the participating Member States in the federation gateway as joint controllers and is therefore a processor. Pursuant to Article 28 of the General Data Protection Regulation and Article 29 of Regulation (EU) 2018/1725, the processing by a processor shall be governed by a contract or a legal act under Union or Member State law which is binding on the processor with regard to the controller and which specifies the processing. This Decision sets out rules on processing by the Commission as a processor.

(12) When processing personal data in the framework of the federation gateway, the Commission is bound by Commission Decision (EU, Euratom) 2017/46.

(13) Taking into account that the purposes for which controllers process personal data in the national contact tracing and warning mobile applications do not necessarily require the identification of a data subject, the controllers may not always be in a position to ensure the application of data subjects' rights. The rights referred to in Articles 15 to 20 of the General Data Protection Regulation may therefore not apply when the conditions pursuant to Article 11 of that Regulation are fulfilled.

(14) The existing Annex to Implementing Decision (EU) 2019/1765 needs to be renumbered due to the addition of two new annexes.

(15) Implementing Decision (EU) 2019/1765 should therefore be amended accordingly.

(16) Considering the urgency of the situation provoked by the COVID-19 pandemic, this Decision should apply from the day following that of its publication in the Official Journal of the European Union.

(17) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 9 July 2020.

(18) The measures provided for in this Decision are in accordance with the opinion of the Committee set up under Article 16 of Directive 2011/24/EU,

HAS ADOPTED THIS DECISION:

Article 1
Implementing Decision (EU) 2019/1765 is amended as follows:
(1)
in Article 2(1), the following points (g), (h), (i), (j), (k), (l), (m), (n) and (o) are inserted:
'(g) "application user" means a person in possession of a smart device who has downloaded and runs an approved contact tracing and warning mobile application;

(h) "contact tracing" means measures implemented in order to trace persons who have been exposed to a source of a serious cross-border threat to health within the meaning of Article 3(c) of Decision No 1082/2013/EU of the European Parliament and of the Council;

(i) "national contact tracing and warning mobile application" means a software application approved at national level running on smart devices, in particular smartphones, designed usually for wide-ranging and targeted interaction with web resources, which processes proximity data and other contextual information collected by many sensors found in the smart devices for the purpose of tracing contacts with persons infected with SARS-CoV-2 and alerting persons who may have been exposed to SARS-CoV-2. These mobile applications are able to detect the presence of other devices using Bluetooth and exchange information with backend servers by using the internet;

(j) "federation gateway" means a network gateway operated by the Commission through a secure IT tool that receives, stores and makes available a minimum set of personal data between Member States' backend servers for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications;

(k) "key" means a unique ephemeral identifier related to an application user reporting to have been infected with SARS-CoV-2, or who may have been exposed to SARS-CoV-2;

(l) "verification of infection" means the method applied for confirming an infection with SARS-CoV-2, namely whether this was self-reported by the application user or resulted from confirmation from a national health authority or a laboratory test;

(m) "countries of interest" means the Member State, or Member States, where an application user has been in the 14 days prior to the date of upload of the keys and where he has downloaded the approved national contact tracing and warning mobile application and/or has travelled;

(n) "country of origin of the keys" means the Member State where the backend server that uploaded the keys to the federation gateway is located;

(o) "log data" means an automatic record of an activity in relation to the exchange of, and access to, data processed through the federation gateway, that show in particular the type of processing activity, the date and time of the processing activity, and the identifier of the person processing the data.
(2)
in Article 4(1), the following point (h) is inserted:
'(h) provide guidance to the Member States on the cross-border exchange of personal data through the federation gateway between national contact tracing and warning mobile applications.';

(3)
in Article 6(1), the following points (f) and (g) are inserted:
'(f) develop, implement and maintain appropriate technical and organisational measures related to the security of transmission and hosting of personal data in the federation gateway for the purpose of ensuring the interoperability of national contact tracing and warning mobile

applications;
(g) support the eHealth Network in agreeing on the technical and organisational compliance of the national authorities with the requirements for the cross-border exchange of personal data in the federation gateway by providing and carrying out the necessary tests and audits. Experts from the Member States may assist the Commission auditors.';

(4)
Article 7 is amended as follows:
(a) the title is replaced by 'Protection of personal data processed through the eHealth Digital Service Infrastructure';

(b) in paragraph 2 'Annex' is replaced by 'Annex I';

(5)
the following Article 7a is inserted:
'Article 7a
Cross-border exchange of data between national contact tracing and warning mobile applications through the federation gateway
1. Where personal data is exchanged through the federation gateway, the processing shall be limited to the purposes of facilitating the interoperability of national contact tracing and warning mobile applications within the federation gateway and the continuity of contact tracing in a cross-border context.
2. The personal data referred to in paragraph 3 shall be transmitted to the federation gateway in a pseudonymised format.
3. The pseudonymised personal data exchanged through and processed in the federation gateway shall only comprise the following information:
(a) the keys transmitted by the national contact tracing and warning mobile applications up to 14 days prior to the date of upload of the keys;

(b) log data associated to the keys in line with the technical specifications protocol used in the country of origin of the keys;

(c) the verification of infection;

(d) the countries of interest and the country of origin of the keys.
4. The designated national authorities or official bodies processing personal data in the federation gateway shall be joint controllers of the data processed in the federation gateway. The respective responsibilities of the joint controllers shall be allocated in accordance with Annex II. Each Member State wishing to participate in the cross-border exchange of data between national contact tracing and warning mobile applications shall notify the Commission, prior to joining, of its intention and indicate the national authority or official body that has been designated as the responsible controller.
5. The Commission shall be the processor of personal data processed within the federation gateway. In its capacity as processor, the Commission shall ensure the security of processing, including the transmission and hosting, of personal data within the federation gateway and shall comply with the obligations of a processor laid down in Annex III.
6. The effectiveness of the technical and organisational measures for ensuring the security of processing of personal data within the federation gateway shall be regularly tested, assessed

and evaluated by the Commission and by the national authorities authorised to access the federation gateway.
7. Without prejudice to the decision of the joint controllers to terminate the processing in the federation gateway, the operation of the federation gateway shall be deactivated at the latest 14 days after all the connected national contact tracing and warning mobile applications cease to transmit keys through the federation gateway.';

(6) the Annex becomes Annex I;

(7) Annexes II and III are added, the text of which is set out in the Annex to this Decision.

Article 2
This Decision shall enter into force on the day following that of its publication in the Official Journal of the European Union.

Done at Brussels, 15 July 2020.
For the Commission
The President
Ursula VON DER LEYEN

ANNEX
In Implementing Decision (EU) 2019/1765, the following Annexes II and III are added:
'ANNEX II
RESPONSIBILITIES OF THE PARTICIPATING MEMBER STATES AS JOINT CONTROLLERS FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

SECTION 1

Subsection 1

Division of responsibilities
(1) The joint controllers shall process personal data through the federation gateway in accordance with the technical specifications stipulated by the eHealth Network.

(2) Each controller shall be responsible for the processing of personal data in the federation gateway in accordance with the General Data Protection Regulation and Directive 2002/58/EC.

(3) Each controller shall set up a contact point with a functional mailbox that will serve for the communication between the joint controllers and between the joint controllers and the processor.

(4) A temporary subgroup set up by the eHealth network in accordance with Article 5(4) shall be tasked to examine any issues arising from the interoperability of national contact tracing and warning mobile applications and from the joint controllership of related processing of

personal data and to facilitate coordinated instructions to the Commission as a processor. Amongst other issues, the controllers may, in the framework of the temporary subgroup, work towards a common approach on the retention of data in their national backend servers, taking into account the retention period set forth in the federation gateway.

(5) Instructions to the processor shall be sent by any of the joint controllers' contact point, in agreement with the other joint controllers in the subgroup referred to above.

(6) Only persons authorised by the designated national authorities or official bodies may access personal data of users exchanged in the federation gateway.

(7) Each designated national authority or official body shall cease to be joint controller from the date of withdrawal of its participation in the federation gateway. It shall however remain responsible for processing in the federation gateway that occurred prior to its withdrawal.

Subsection 2
Responsibilities and roles for handling requests of and informing data subjects
(1) Each controller shall provide the users of its national contact tracing and warning mobile application ("the data subjects") with information about the processing of their personal data in the federation gateway for the purposes of cross-border interoperability of the national contact tracing and warning mobile applications, in accordance with Articles 13 and 14 of the General Data Protection Regulation.

(2) Each controller shall act as the contact point for the users of its national contact tracing and warning mobile application and shall handle the requests relating to the exercise of the rights of data subjects in accordance with the General Data Protection Regulation, submitted by those users or their representatives. Each controller shall designate a specific contact point dedicated to requests received from data subjects. If a joint controller receives a request from a data subject, which does not fall under its responsibility, it shall promptly forward it to the responsible joint controller. If requested, the joint controllers shall assist each other in handling data subjects' requests and shall reply to each other without undue delay and at the latest within 15 days from receiving a request for assistance.

(3) Each controller shall make available to the data subjects the content of this Annex including the arrangements laid down in points 1 and 2.

SECTION 2
Management of security incidents, including personal data breaches
(1) The joint controllers shall assist each other in the identification and handling of any security incidents, including personal data breaches, linked to the processing in the federation gateway.

(2)
In particular, the joint controllers shall notify each other of the following:
a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing processing in the federation gateway;

b) any security incidents that are linked to the processing operation in the federation gateway;

c) any personal data breach, the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

d) any breach of the technical and/or organisational safeguards of the processing operation in the federation gateway.

(3) The joint controllers shall communicate any personal data breaches with regard to the processing operation in the federation gateway to the Commission, to the competent supervisory authorities and, where required so, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679 or following notification by the Commission.

SECTION 3
Data Protection Impact Assessment
If a controller, in order to comply with its obligations specified in Articles 35 and 36 of the General Data Protection Regulation needs information from another controller, it shall send a specific request to the functional mailbox referred to in Subsection 1(3) of Section 1. The latter shall use its best efforts to provide such information.

ANNEX III
RESPONSIBILITIES OF THE COMMISSION AS DATA PROCESSOR FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

The Commission shall:
(1) Set up and ensure a secure and reliable communication infrastructure that interconnects national contact tracing and warning mobile applications of the Member States participating in the federation gateway. To fulfil its obligations as data processor of the federation gateway, the Commission may engage third parties as sub-processors; the Commission shall inform the joint controllers of any intended changes concerning the addition or replacement of other sub-processors thereby giving the controllers the opportunity to jointly object to such changes as set out in Annex II, Subsection 1(4) of Section 1. The Commission shall ensure that the same data protection obligations as set out in this Decision apply to these sub-processors.

(2) Process the personal data, only based on documented instructions from the controllers, unless required to do so by Union or Member State law; in such a case, the Commission shall inform the controllers of that legal requirement before processing, unless that law prohibits submitting such information on important grounds of public interest.

(3)
The processing by the Commission entails the following:
a) Authentication of national backend servers, based on national backend server certificates;

b) Reception of the data referred to in Article 7a, paragraph 3, of the Implementing Decision

uploaded by national backend servers by providing an application programming interface that allows national backend servers to upload the relevant data;

c) Storage of the data in the federation gateway, upon receiving them from national backend servers;

d) Making the data available for download by national backend servers;

e) Deletion of the data when all participating backend servers have downloaded them or 14 days after their reception, whichever is earlier.

f) After the end of the provision of service, delete any remaining data unless Union or Member State law requires storage of the personal data.
The processor shall take the necessary measures to preserve the integrity of the data processed.

(4)
Take all state of the art organisational, physical and logical security measures to maintain the federation gateway. To this end, the Commission shall:
a) designate a responsible entity for the security management at the level of the federation gateway, communicate to the controllers its contact information and ensure its availability to react to security threats;

b) assume the responsibility for the security of the federation gateway;

c) ensure that all individuals that are granted access to the federation gateway are subject to contractual, professional or statutory obligation of confidentiality;

(5)
Take all necessary security measures to avoid compromising the smooth operational functioning of the national backend servers. To this end, the Commission shall put in place specific procedures related to the connection from the backend servers to the federation gateway. This includes:
a) risk assessment procedure, to identify and estimate potential threats to the system;

b)
audit and review procedure to:
i. check the correspondence between the implemented security measures and the applicable security policy;

ii. control on a regular basis the integrity of system files, security parameters and granted authorisations;

iii. monitor to detect security breaches and intrusions;

iv. implement changes to mitigate existing security weaknesses

v. allow for, including at the request of controllers, and contribute to, the performance of

independent audits, including inspections, and reviews on security measures, subject to conditions that respect Protocol (No 7) to the TFEU on the Privileges and Immunities of the European Union (2);

c) changing the control procedure to document and measure the impact of a change before its implementation and keep the controllers informed of any changes that can affect the communication with and/or the security of their infrastructures;

d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of equipment should be performed;

e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers, as well as the European Data Protection Supervisor of any personal data breach and define a disciplinary process to deal with security breaches.

(6)
Take state of the art physical and/or logical security measures for the facilities hosting the federation gateway equipment and for the controls of logical data and security access. To this end, the Commission shall:
a) enforce physical security to establish distinct security perimeters and allowing detection of breaches;

b) control access to the facilities and maintain a visitor register for tracing purposes;

c) ensure that external people granted access to the premises are escorted by duly authorised staff;

d) ensure that equipment cannot be added, replaced or removed without prior authorisation of the designated responsible bodies;

e) control access from and to the national backend servers to the federation gateway;

f) ensure that individuals who access the federation gateway are identified and authenticated;

g) review the authorisation rights related to the access to the federation gateway in case of a security breach affecting this infrastructure;

h) keep the integrity of the information transmitted through the federation gateway;

i) implement technical and organisational security measures to prevent unauthorised access to personal data;

j) implement, whenever necessary, measures to block unauthorised access to the federation gateway from the domain of the national authorities (i.e.: block a location/IP address).

(7) Take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality or security.

(8) Maintain a risk management plan related to its area of responsibility.

(9) Monitor – in real time – the performance of all the service components of its federation gateway services, produce regular statistics and keep records.

(10) Provide support for all federation gateway services in English, 24/7 via phone, mail or Web Portal and accept calls from authorised callers: the federation gateway's coordinators and their respective helpdesks, Project Officers and designated persons from the Commission.

(11) Assist the controllers by appropriate technical and organisational measures, insofar as it is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the General Data Protection Regulation.

(12) Support the controllers by providing information concerning the federation gateway, in order to implement the obligations pursuant to Articles 32, 35 and 36 of the General Data Protection Regulation.

(13) Ensure that data processed within the federation gateway is unintelligible to any person who is not authorised to access it.

(14) Take all relevant measures to prevent that the federation gateway's operators have unauthorised access to transmitted data.

(15) Take measures in order to facilitate the interoperability and the communication between the federation gateway's designated controllers.

(16) Maintain a record of processing activities carried out on behalf of the controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725'.

European Union, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01, C/2020/2523, *OJ C 124I , 17.4.2020*

COMMUNICATION FROM THE COMMISSION
Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection
(2020/C 124 I/01)

1. CONTEXT

The COVID-19 pandemic has created unprecedented challenge for the Union and the Member States, their healthcare systems, way of life, economic stability and values. Digital technologies and data have a valuable role to play in combating the COVID-19 crisis. Mobile applications typically installed on smartphones (apps) can support public health authorities at national and EU level in monitoring and containing the COVID-19 pandemic and are particularly relevant in the phase of lifting containment measures. They can provide direct guidance to citizens and support contact tracing efforts. In a number of countries, both within the EU and worldwide, national or regional authorities or developers have announced the launch of apps with different functionalities aimed at supporting the fight against the virus.

On 8 April 2020, the Commission adopted a Recommendation towards 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 (the "Recommendation") [1]. The purpose of the Recommendation is, inter alia, to develop a common European approach ("Toolbox") for the use of mobile applications, coordinated at EU level, for empowering citizens to take effective social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease. The Recommendation sets out the general principles which should guide the development of such a toolbox and it indicates that the Commission will publish further guidance, including on the personal data protection and privacy implications of the use of applications in this field.

With the Joint European Roadmap towards lifting COVID-19 containment measures, the Commission, in cooperation with the President of the European Council, set out a number of principles to guide the phase-out of the containment measures due to the COVID-19 outbreak. Mobile applications, including contact tracing functionalities, can play an important role in this context. Depending on the features of the apps and the extent to which the population uses them, they can have a significant impact on disease diagnosis, treatment and management of COVID-19 inside and outside the hospital setting. They are particularly relevant when containment measures are lifted and when the risk of infection grows as more and more people are in contact with each other. These applications can help to interrupt infection chains faster and more efficiently than general containment measures, and can reduce the risk of the virus spreading significantly. They should thus be an important element in the exit strategy, complementing other measures like increased testing capacities [2]. An important prerequisite for the development, acceptance and up-take of such apps by individuals is trust. People must have the certainty that compliance with fundamental rights is ensured and that

[1] Recommendation C(2020) 2296 final of 8 April 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

[2] https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

the apps will be used only for the specifically defined purposes, that they will not be used for mass surveillance, and that individuals will remain in control of their data. This is the foundation for the accuracy and effectiveness of such apps in containing the spread of the virus. It is therefore essential to identify solutions that are the least intrusive and fully comply with personal data protection and privacy requirements as set out in EU law. Moreover, the apps should be deactivated at the latest when the pandemic is declared to be under control. The apps should also include state- of- the- art information security protections.
This guidance takes into account the contribution from the European Data Protection Board (EDPB) [3], and discussions within the eHealth network. The EDPB plans to publish Guidelines in the upcoming days on geolocation and other tracing tools in the context of the COVID-19 out-break.
Scope of the guidance
In order to ensure a coherent approach across the EU and provide guidance to Member States and app developers, this document sets out features and requirements which apps should meet to ensure compliance with EU privacy and personal data protection legislation, in particular the General Data Protection Regulation [4] (GDPR) and the ePrivacy Directive [5]. This guidance does not address any further conditions, including limitations that Member States might have included in their national laws with regard to processing of data concerning health.
The guidance is not legally binding. It is without prejudice to the role of the Court of Justice of the EU, which is the only institution that can give authoritative interpretation of EU law.
The present guidance addresses only voluntary apps supporting the fight against COVID 19 pandemic (apps downloaded, installed and used on a voluntary basis by individuals) with one or several of the following functionalities:
— provide accurate information to individuals about the COVID-19 pandemic;

— provide questionnaires for self-assessment and for guidance to individuals (symptom checker functionality) [6];

— alert persons who have been in proximity for a certain duration to an infected person, in order to provide information such as whether to self-quarantine and where to get tested (contact tracing and warning functionality);

— provide a communication forum between patients and doctors in situation of self-isolation

[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (OJ L 119, 4.5.2016, p. 1).

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[6] If the apps provide information related to diagnosis, prevention, monitoring, prediction or prognosis, potential qualification as medical devices according to the medical devices regulatory framework should be assessed. As regards said framework, see Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1) and Regulation (EU) 2017/745 of the European Parliament and the Council of 5 April 2017 on medical devices (OJ L 117, 5.5.2017, p. 1).

or where further diagnosis and treatment advice is provided (increased use of telemedicine).
Under the ePrivacy Directive, imposing the use of an app involving the confidentiality of communications rights set out in Article 5 is only possible through a law which is necessary, appropriate and proportionate in order to protect certain specific objectives. Given the high degree of intrusiveness of such an approach and the challenges involved, including in terms of putting in place appropriate safeguards, the Commission is of the view that a careful analysis is required before using this option. For these reasons, the Commission recommends the use of voluntary apps.
This guidance does not cover apps aimed at enforcing quarantine requirements (including those which are mandatory).
2. CONTRIBUTION OF APPS TO THE FIGHT AGAINST COVID-19
The symptom checker functionality is a tool for public health authorities to guide citizens on testing for COVID-19, to provide information on self-isolation, on how to avoid transmission to others and when to seek healthcare. It can also complement primary care surveillance and better inform what the transmission rates of COVID-19 are in the population.
Contact tracing and warning functionalities are tools to identify the persons that have been in contact with a person infected by COVID-19 and to inform him/her about appropriate next steps, such as self-quarantine, testing or providing advice on what to do in case of symptoms n. This functionality is therefore useful both for individuals and public health authorities. It can also play an important role in managing containment measures during de-escalation scenarios. Its impact can be boosted by a strategy supporting wider testing of persons showing mild symptoms.
Both functionalities may also be a relevant source of data for public health authorities and facilitate the transmission of such data to national epidemiological authorities and to the European Centre for Disease Prevention and Control (ECDC). This would help understand transmission patterns and, if combined with testing results, estimate the positive predictive value of respiratory symptoms in a given community and provide information on the level of virus circulation.
The degree of reliability of estimates is directly linked to the number and reliability of data transmitted.
Therefore, in combination with appropriate testing strategies, both symptoms checker and contact tracing functionalities can provide information on the level of virus circulation, and help to assess the impact of physical distancing and confinement measures. As set out in the Recommendation, in order to enable cross-border collaboration and to ensure contact detection between users of different apps (which is particularly important in cross border movements of citizens) interoperability between the IT solutions of different Member States should be ensured. Where an infected person is in contact with a user of an app of another Member State, cross-border transmission of personal data of that user to health authorities of its Member State should be possible to the extent strictly necessary. Work on this issue will take place as part of the toolbox announced by the Recommendation. Interoperability should be ensured both by means of technical requirements and by improving the communication and cooperation between national health authorities. A model of particular cooperation [7]could also be used as a governance model for contact tracing apps during the COVID-19 pandemic.
3. ELEMENTS FOR A TRUSTFUL AND ACCOUNTABLE USE OF APPS

[7] Such cooperation already takes place as regards the project MyHealth@EU for exchange of patient summaries and ePrescriptions. See also art. 5(5) and recital 17 of Commission Implementing Decision 2019/1765.

The 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, non-discrimination, freedom to conduct a business, and freedom of assembly and of association. The interference with privacy and the right to protection of personal data may be particularly significant given that some of the functionalities are based on a data-intensive model.
The elements presented below aim to provide guidance on how to limit the intrusiveness of the app functionalities in order to ensure compliance with the EU personal data protection and privacy legislation.
3.1. National health authorities (or entities carrying out tasks in the public interest in the field of health) as data controller
The identification of who is deciding on the means and purposes of the data processing (the data controller) is crucial in order to establish who is responsible for compliance with the EU personal data protection rules, and in particular: who should provide information to the individuals who download the app about what is going to happen with their personal data (already existing or to be generated through the device, such as a smartphone, on which the app is being installed), what their rights will be, who will be responsible in the case of data breach, etc.
Given the sensitivity of the personal data at hand and the purpose of data processing described below, the Commission is of the view that the apps should be designed in such a manner that the national health authorities (or entities carrying out task in the public interest in the field of health) are the controllers [8]. The controllers are responsible for the compliance with the GDPR (accountability principle). The scope of such access should be limited based on the principles described in section 3.5 below.
This will also contribute to higher trust among the population and therefore acceptance of the apps (and underlying infection transmission chains information systems) and will ensure that they fulfil the intended purpose of protecting public health. The underlying policies, requirements and controls should be aligned and implemented in a coordinated way by the responsible national health authorities.
3.2. Ensuring that the individual remains in control
A determining factor for individuals to trust the apps is demonstrating that they remain in control of their personal data. To ensure this, the Commission considers that in particular the following conditions should be met:
— the installation of the app on their device should be voluntary and without any negative consequences for the individual who decides not to download/use the app;

— different app functionalities (e.g. information, symptom checker, contact tracing and warning functionalities) should not be bundled so that the individual can provide his/her consent specifically for each functionality. This should not prevent the user from combining different app functionalities if this is offered as an option by the provider;

— if proximity data are used (data generated by the exchange of Bluetooth Low Energy (BLE) signals between devices within an epidemiologically relevant distance and during an epidemiologically relevant time), they should be stored on the individual's device. If those data are to be shared with health authorities, they should be shared only after confirmation that the person concerned is infected with the COVID-19 and on the condition that he/she chooses

[8] See recital 45 of the GDPR.

to do so;

— health authorities should provide the individuals with all necessary information related to the processing of his or her personal data (in line with Articles 12 and 13 of the GDPR and Article 5 of the ePrivacy Directive);

— the individual should be able to exercise his/her rights under the GDPR (in particular, access, rectification; deletion). Any restriction of the rights under the GDPR and ePrivacy Directive should be in accordance with these acts and be necessary, proportionate and provided in the legislation;

— the apps should be deactivated at the latest when the pandemic is declared to be under control; the deactivation should not depend on de-installation by the user.

3.3. Legal basis for processing

Installation of the apps and storing of information on the user's device

As noted above, under the ePrivacy Directive (Article 5), storing of information on the user's device or gaining access to the information already stored is allowed only if (i) the user has given consent or (ii) the storage and/or access is strictly necessary for the information society service (e.g. the app) explicitly requested (i.e. installed and activated) by the user.

The storage of information on the individual's device and getting access to the information already stored on this device is normally necessary for the apps to function. In addition, the contact tracing and warning functionality requires some other information (such as ephemeral, periodically changing alias user IDs of users of this functionality in proximity) to be stored on the user's device. Furthermore, this functionality may require the (infected, or likely infected) user to upload proximity data. Such an upload is not necessary for the functioning of the app as such. Therefore, the requirements of option (ii) mentioned in the previous paragraph are not met. That leaves consent (option (i) above) as the most appropriate ground for the relevant activities. This consent should be "freely given", "specific", "explicit" and "informed" within the meaning of the GDPR. It should be expressed through a clear affirmative action of the individual; this excludes tacit forms of consent (e.g. silence; inactivity) [9].

Legal basis for processing by national health authorities – Union or Member State law

National health authorities typically process personal data when there is a legal obligation laid down in EU or Member State law providing for such processing and meeting the conditions of Article 6(1)(c) and Article 9(2)(i) of the GDPR or when such processing is necessary for the performance of a task carried out to further the public interest recognised by EU or Member State law[10].

Any national law has to provide specific and suitable measures to safeguard the rights and freedoms of data subjects. As a general rule, the stronger the impact on the freedoms of the individuals, the stronger corresponding safeguards should be provided for in the relevant law. EU and Member State laws that pre-exist to the COVID-19 outbreak and those which Member States are enacting specifically to fight the spread of epidemics may in principle, be used as a legal basis for processing of individuals' data if they provide for measures allowing for the monitoring of epidemics and if that law meets further requirements set out in Article

[9] See the guidelines from the European Data Protection Board on consent: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[10] Article 6(1)(e) GDPR.

6 (3) GDPR.
Given the nature of the personal data concerned (in particular health data as special categories of personal data) as well as the circumstances of the current COVID-19 pandemic, relying on the law as the legal basis would contribute to legal certainty, since it would (i) prescribe in detail the processing of specific health data and clearly specify the purposes for the processing; (ii) spell out clearly who is the controller, i.e. the entity processing the data, and who, beside the controller, can have access to such data; (iii) exclude the possibility to process such data for different purposes than those listed in the legislation and (iv) provide for specific safeguards. In order not to undermine the public usefulness and acceptance of the apps the national legislator should pay particular attention that the solution chosen is as inclusive vis-a-vis citizens as possible.
Processing by health authorities on the basis of the legislation does not change the fact that the individuals remain free to install the app or not and to share their data with health authorities. No adverse consequences for the users should therefore occur whenever the app is uninstalled.
Contact tracing and warning apps provide for the warning of individuals. When this warning is provided directly by the app, the Commission draws attention to the prohibition of subjecting individuals to a decision based solely on automated processing which produces legal effect or similarly significantly affects him or her (Article 22 GDPR).
3.4. Data minimisation
The data produced via devices and already previously stored in those devices is protected as follows:
— As "personal data", i.e. any information relating to an identified or an identifiable natural person (Article 4(1) of the GDPR), it is protected under the GDPR. Health data benefit from additional protection (Article 9 of the GDPR).

— As "location data", i.e. data processed in an electronic communications network or by an electronic communication service, indicating the geographic position of the terminal equipment of the user, it is protected under the ePrivacy Directive (Art 5(1), 6 and 9) [11],

— Any information stored in and accessed from user's terminal equipment is protected under Article 5(3) of the ePrivacy Directive.
Non-personal data (such as irreversibly anonymised data) is not protected under the GDPR.
The Commission recalls that the principle of data minimisation requires that only personal data that is adequate, relevant and limited to what is necessary in relation to the purpose [12] may be processed. An assessment of the necessity to process the personal data and the relevance of such personal data should be carried out in the light of the purpose(s) pursued.
The Commission notes, for instance, that if the purpose of the functionality is symptom checking or telemedicine, these purposes do not require access to the contact list of the person owning the device.
Generating and processing less data limits the security risks. Therefore the compliance with data minimisation measures also provides for security safeguards.
— Information functionality:
An app with merely this functionality will not need to process any health data of individuals.

[11] The Electronic Communications Code provides that services which are functionally equivalent to electronic communications services are also covered.
[12] Principle of data minimisation.

It will merely provide them with information. In order to fulfil this purpose no information stored in and accessed from terminal equipment may be processed other than what is necessary to provide the information.

— Symptom checker and telemedicine functionalities:

If the app includes one or two of these functionalities, it will be processing personal health data. Therefore, a list of data which may be processed should be specified in the underlying legislation applicable to the health authorities.

In addition, the health authorities may need the phone numbers of the persons who used the symptom checker and uploaded the results. Information stored in and accessed from terminal equipment may be processed only insofar as it is necessary to enable the app to fulfil its purpose and allow it to function.

— Contact tracing and warning functionality:

A majority of COVID-19 infections occur through droplets that travel only over a limited distance. Identifying as quickly as possible persons who have been in proximity with an infected person is a key factor to interrupt the infection chain. The determining proximity is a function of the distance and duration of a contact and should be done from an epidemiologic point of view. The interruption of the infection chain is particularly relevant to avoid resurgence of infections in the crisis exit phase.

Proximity data could be necessary for this. For the metering of proximity and close contacts Bluetooth Low Energy (BLE) communications between devices appears more precise, and therefore more appropriate, than the use of geolocation data (GNSS/GPS, or cellular location data). BLE avoids the possibility of tracking (contrary to geolocation data). The Commission therefore recommends the use of BLE communications data (or data generated by equivalent technology) to determine proximity.

Location data is not necessary for the purpose of contact tracing functionalities, as their goal is not to follow the movements of individuals or to enforce prescriptions. In addition, the processing of location data in the context of contact tracing would be difficult to justify in light of the principle of data minimisation and may create security and privacy issues. For this reason the Commission advises not to use location data in this context.

Irrespective of the technical means used to determine proximity, it does not appear necessary to store the exact time of the contact or the place (if available). However it might be useful to store the day of the contact to know whether the contact occurred when the person developed symptoms (or 48 hours before [13]) and to guide the follow up message with advice for instance on how long to self-quarantine.

Proximity data should only be generated and processed if there is an actual risk of infection (depending on the closeness and duration of the contact).

It should be noted that the necessity and proportionality of the collection of data will thus depend on factors such as the extent to which testing facilities are available in particular when measures such as confinement were already ordered. The warning of persons who have been in close contact with an infected person can be done in two ways:

Under the first approach, an alert is automatically delivered via the app to the close contacts when a user notifies the app – with the approval or confirmation by the health authority, for instance via a QR or TAN code – that he or she has tested positive (decentralised processing). The content of the alert message should preferably be determined by the health authority. Under the second approach the arbitrary temporary identifiers are stored on a backend server

[13] The infected person is contagious 48 h before the onset of symptoms.

held by the health authority (backend server solution). Users cannot be directly identified through these data. Through the identifiers, users who have been in close contact with a positively tested user, receive an alert on their device. If the health authorities wish to contact the users who have been in close contact with an infected person also via phone or SMS, they need the consent of those users to provide their phone numbers.

3.5. Limiting the disclosure/access of data

— Information functionality:

No information stored in and accessed from terminal equipment can be shared with health authorities other than necessary to have the information functionality. Since this functionality provides only for the means of communication, health authorities will not get access to any other data.

— Symptom checker and telemedicine functionalities:

The symptom checker functionality can be useful for Member States to guide citizens about whether they should get tested, provide information about isolation and when and how to access healthcare in particular for risk groups. This functionality can also complement primary care surveillance and help understand what the infection rates of COVID-19 are in the population. Therefore, it may be decided that responsible health authorities and national epidemiological authorities should get access to the information provided by the patient. ECDC could receive aggregated data from national authorities for epidemiological surveillance.

If the choice is made to allow for a contact with health officials rather than only through the app itself, then disclosing to national health authorities the telephone number of app users is also necessary.

— Contact tracing and warning functionality:

— Data of the infected person

The apps generate pseudo-randomly ephemeral and periodically changing identifiers of the phones that are in contact with the user. One option is that the identifiers are stored on the device of the user (so called decentralised processing). Another option can provide that these arbitrary identifiers are stored on the server to which the health authorities have access (so called backend server solution). The decentralised solution is more in line with the minimisation principle. Health authorities should have access only to proximity data from the device of an infected person so that they are able to contact people at risk of infection.

These data will be available to the health authorities only after the infected person (after having been tested) proactively shares these data with them.

The infected person should not be informed about the identity of the persons with whom he/she has been in potentially epidemiologically relevant contact and who will be alerted.

— Data of the persons who have been in (epidemiological) contact with the infected person

The identity of the infected person should not be disclosed to the persons with whom he/she has been in epidemiological contact. It is sufficient to communicate to them the fact that they have been in epidemiological contact with an infected person during the past 16 days. As noted above, data about the time and place of such contacts should not be stored. It is therefore neither necessary nor possible to communicate those data.

To trace epidemiological contacts of an e app user who is found to be infected, the national health authorities should be informed only about the identifier of the person with whom

the infected person has been in epidemiological contact since 48 hours before the onset of symptoms until 14 days after the onset of symptoms, based on proximity and duration of the contact.
The ECDC could receive aggregated contact tracing data from national authorities for epidemiological surveillance on indicators defined in collaboration with Member States.
3.6. Providing for precise purposes of processing
The legal basis (Union or Member State law) should provide for the purpose of the processing. The purpose should be specific, so that there is no doubt what kind of personal data is necessary to process in order to achieve the desired objective and explicit. .
The precise purpose(s) will depend on the functionalities of the app. There may be several purposes for each functionality of an app. In order to provide the individuals with full control of their data, the Commission recommends not to bundle different functionalities. In any event, the individual should have the possibility to choose between different functionalities pursuing each a separate purpose.
The Commission advises against the use of the data gathered under the above conditions for other purposes than the fight against COVID-19. Should purposes like scientific research and statistics be necessary, they should be included in the original list of purposes and clearly communicated to users.
— Information functionality:
The purpose of this functionality is the provision of the information that is relevant from the point of view of the health authorities in the context of the crisis.
— Symptom-checker and telemedicine functionalities:
Symptom checker functionality can provide an indication of which proportion of the individuals reporting symptoms compatible with COVID-19 is actually infected (e.g. by swabbing and testing all or a random number of individuals with such symptoms, if there is capacity to do so). This identification of the purpose should make clear that the personal health data will be processed in order (i) to provide the individual with the possibility to self asses, on the basis of a set of questions asked, if he or she has developed symptoms of COVID-19, or (ii) to get medical advice if having developed the symptoms of COVID-19.
— Contact tracing and warning functionalities:
The mere indication of a purpose "prevention of further COVID-19 infections" is not specific enough. In this case, the Commission recommends to specify further the purpose(s) along the lines of: "retaining of the contacts of the persons who use the app and who may have been exposed to infection by COVID-19 in order to warn those persons who could have been potentially infected".
3.7. Setting strict limits to data storage
The principle of storage limitation requires that personal data may not be kept for longer than necessary. Timelines should be based on medical relevance (depending on the purpose of the app: the incubation period, etc.) as well as realistic durations for administrative steps that may need to be taken.
— Information functionality:
If any data is collected while installing this functionality, it should be deleted immediately. There is no justification for keeping such data.
— Symptom checker and telemedicine functionalities:
Such data should be deleted by the health authorities after maximum one month (incubation period plus margin) or after the person was tested and the result is negative. Health authorities may retain data for longer periods for surveillance reporting and research provided it is in an

anonymised form.
— Contact tracing and warning functionalities:
Proximity data should be deleted as soon as they are no longer necessary for the purpose of alerting individuals. This should be the case after maximum one month (incubation period plus margin) or after the person was tested and the result is negative. Health authorities may retain the proximity data for longer periods for surveillance reporting and research provided it is in an anonymised form.
The data should be stored on the user's device and only data that has been communicated by the users and is necessary to fulfil the purpose should be uploaded to the server available to the health authorities where this option is chosen (i.e. only upload the data to the server of "close contacts" of a person who tested positive of infection of COVID-19).
3.8. Ensuring the security of the data
The Commission recommends that the data should be stored on the terminal device of the individual in an encrypted form using state-of-the art cryptographic techniques. In the case that the data is stored in a central server, the access, including the administrative access, should be logged.
Proximity data should only be generated and stored on the terminal device of the individual in encrypted and pseudonymised format. In order to ensure that tracking by third parties –is excluded the activation of Bluetooth should be possible without having to activate other location services.
During the collection of proximity data via BLE it is preferable to create and store temporary user IDs that change regularly rather than storing the actual device ID. This measure provides additional protection against eavesdropping and tracking by hackers and therefore makes it more difficult to identify individuals.
The Commission recommends that the source code of the app should be made public and available for review.
Additional measures to secure the data processed can be envisaged notably with automatic deletion or anonymisation of the data after a certain point in time. In general, the degree of the security should match the amount and sensitivity of personal data processed.
All transmissions from the personal device to the national health authorities should be encrypted.
Where the national legalisation provides that the personal data gathered can also be processed for scientific research purposes, pseudonymisation should, in principle, be used.
3.9. Ensuring the accuracy of the data
Ensuring the accuracy of the personal data processed is not only a pre-requisite for the efficiency of the app but is also a requirement under the personal data protection legislation.
In this context, ensuring the accuracy of the information on whether a contact with an infected person (epidemiological distance and duration) has taken place is essential, to minimise the risk of having false positives. This should address scenarios when two users of the app are in contact in the street, in public transport or in a building. It is unlikely that the use of location data based on mobile phone networks is accurate enough for this.
It is therefore advisable to rely on technologies allowing a more precise assessment of the contact (such as Bluetooth).
3.10. Involving Data Protection Authorities
The Data Protection Authorities should be fully involved and consulted in the context of the development of the app and they should keep its deployment under review. Given that the processing of data in the context of the app will qualify as a processing on a large scale of special categories of data (health data), the Commission draws attention to Article 35 GDPR

on data protection impact assessment.

European Union, Commission Recommendation (EU) 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, *OJ L 114, 14.4.2020*

COMMISSION RECOMMENDATION (EU) 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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) The public health crisis caused by the current COVID-19 pandemic (hereinafter, 'COVID-19 crisis') is compelling the Union and the Member States to face an unprecedented challenge to its health care systems, way of life, economic stability and values. No single Member State can succeed alone in combating the COVID-19 crisis. An exceptional crisis of such magnitude requires determined action of all Member States and EU institutions and bodies working together in a genuine spirit of solidarity.

(2) Digital technologies and data have a valuable role to play in combating the COVID-19 crisis, given that many people in Europe are connected to the internet via mobile devices. Those technologies and data can offer an important tool for informing the public and helping relevant public authorities in their efforts to contain the spread of the virus or allowing healthcare organisations to exchange health data. However, a fragmented and uncoordinated approach risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis, whilst also causing serious harm to the single market and to fundamental rights and freedoms.

(3) It is therefore necessary to develop a common approach to the use of digital technologies and data in response to the current crisis. That approach should be effective in supporting competent national authorities, in particular health authorities and policy makers, by providing them with sufficient and accurate data to understand the evolution and spread of the COVID-19 virus as well as its effects. Similarly, these technologies may empower citizens to take effective and more targeted social distancing measures. At the same time, the proposed approach aims to uphold the integrity of the single market and protect fundamental rights and freedoms, particularly the rights to privacy and protection of personal data.

(4) Mobile applications can support health authorities at national and EU level in monitoring and containing the ongoing COVID-19 pandemic. They can provide guidance to citizens and facilitate the organisation of the medical follow-up of patients. Warning and tracing applications can play an important role in contact tracing, limiting the propagation of disease and interrupting transmission chains. Therefore, in combination with appropriate testing strategies and contact tracing, the applications can be particularly relevant in providing information on the level of virus circulation, in assessing the effectiveness of physical distancing and confinement measures, and in informing de-escalation strategies.

(5) Decision No 1082/2013/EU of the European Parliament and the Council (1) lays down specific rules on epidemiological surveillance, monitoring, early warning of, and combating serious cross-border threats to health. Article 2(5) of the Decision requires the Commission, in liaison with the Member States, to ensure coordination and information exchange between the mechanisms and structures established under that Decision and similar mechanisms and structures established at Union level or under the Euratom Treaty whose activities are relevant for preparedness and response planning, monitoring, early warning of, and combating serious cross-border threats to health. The forum for coordination of efforts in the context of serious cross-border threats to health is the Health Security Committee, set up by the Article 17 of the aforementioned Decision. At the same time, Article 6[1] of the Decision sets up a network for the epidemiological surveillance of communicable diseases, operated and coordinated by the European Centre for Disease Control.

(6) Directive 2011/24/EU of the European Parliament and of the Council [2]on the application of patients' rights in cross-border healthcare requires the eHealth Network to work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare.

(7) Regulation (EU) 2016/679 of the European Parliament and of the Council [3] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data lays down the conditions for processing personal data, including data concerning health. Such data may be processed inter alia 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.

(8) Several Member States have introduced specific legislation that allow them to process health data, based on public interest (Article 6(1)(c) or (e) and Article 9(2)(i) of Regulation (EU) 2016/679). In any case, the purposes and means of the data processing, what data are to be processed and by whom, should be clear and specific.

(9) The Commission may consult the European Data Protection Supervisor and the European Data Protection Board, in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council [4]and Article 70 of Regulation (EU) 2016/679.

---

[1] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC (OJ L 293, 5.11.2013, p. 1).

[2] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (OJ L 119, 4.5.2016, p. 1).

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions,

(10) Directive 2002/58/EC of the European Parliament and of the Council [5]lays down the rules applicable to traffic and location data, and to the storing of information and the gaining of access to information stored in the terminal equipment, such as a mobile device, of a user or subscriber. Pursuant to Article 5(3) of the Directive, such storage or gaining of access is only permitted in narrowly defined circumstances or on the basis of consent of the user or subscriber, after having been provided with clear and comprehensive information, in accordance with the requirements of Regulation (EU) 2016/679. In addition, Article 15(1) of the Directive allows Member States to adopt legislative measures to restrict the scope of certain rights and obligations established by the Directive, including those set out in Article 5, when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to achieve certain objectives.

(11) The European Commission announced in its Communication, 'A European strategy for data' [6]that the EU would create a single market in which data can flow within the EU and across sectors, for the benefit of all, where European rules, in particular privacy and data protection, as well as competition law, are fully respected and where rules for access and use of data are fair, practical and clear. In particular, the Commission stated it would consider the need for legislative action to foster business-to-government data sharing for the public interest.

(12) Since the beginning of the COVID-19 crisis, a variety of mobile applications have been developed, some of them by public authorities, and there have been calls from Member States and the private sector for coordination at Union level, including to address cybersecurity, security and privacy concerns. These applications tend to serve three general functions: (i) informing and advising citizens and facilitating the organisation of medical follow-up of persons with symptoms, often combined with a self-diagnosis questionnaire; (ii) warning people who have been in proximity to an infected person in order to interrupt infection chains and preventing resurgence of infections in the reopening phase; and (iii) monitoring and enforcement of quarantine of infected persons, possibly combined with features assessing their health condition during the quarantine period. Certain applications are available to the general public, while others only to closed user groups directed at tracing contacts in the workplace. The effectiveness of these applications has generally not been evaluated. Information and symptom-checker apps may be useful to raise awareness of citizens. However, expert opinion suggests that applications aiming to inform and warn users seem to be the most promising to prevent the propagation of the virus, taking into account also their more limited impact on privacy, and several Member States are currently exploring their use.

(13) Some of those mobile applications could be deemed medical devices where they are intended by the manufacturer to be used inter alia for diagnosis, prevention, monitoring,

bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final.

prediction, prognosis, treatment or alleviation of disease and would therefore fall within scope of under Regulation (EU) 2017/745 of the European Parliament and of the Council [7], or Council Directive 93/42/EEC [8]. For self-diagnosis and symptom-checker applications, where they provide information related to diagnosis, prevention, monitoring, prediction or prognosis, their potential qualification as medical devices according to the medical devices regulatory framework (Directive 93/42/EEC or Regulation (EU) 2017/745) should be assessed.

(14) The effectiveness of these mobile applications depends on a number of factors. Such factors include user penetration, that is, the percentage of the population using a mobile device and, of those, the percentage, who have downloaded the application and consented to the processing of personal data concerning them and not withdrawn that consent. Other important factors are public trust that the data will be protected by appropriate security measures, used exclusively to alert individuals who may have been exposed to the virus, public health authorities' endorsement, ability of the health authorities to take action based on the data generated by the application, integration and data sharing with other systems and applications, cross-border and cross-regional interoperability with other systems.

(15) Warning and tracing applications are useful for Member States for contact tracing purposes and can play an important role in containment during de-escalation scenarios. They can also be a valuable tool for citizens to practise effective and better targeted social distancing. Their impact can be boosted by a strategy supporting wider testing. Contact tracing implies that public health authorities rapidly identify all contacts of a confirmed COVID-19 patient, ask them to self-isolate, and rapidly test and isolate them if they develop symptoms. In addition, anonymised and aggregated data derived from such applications, combined with information on disease incidence, could be used to assess the effectiveness of community and physical distancing measures. While these applications are of evident usefulness for Member States, they also potentially add value to the work of the ECDC.

(16) Self-diagnoses and symptom checker applications could provide relevant information on the number of cases with COVID-19 compatible symptoms, by age and week, from well-defined areas where there is a high coverage of the application. If successful, national public health authorities can decide to use application data for COVID-19 syndromic primary care surveillance. These data could be provided to the ECDC weekly, in aggregated format (e.g. number of influenza-like illness (ILI) or acute respiratory infection (ARI) per week, by age group, out of the total population covered by the sentinel doctors). This would allow national authorities and the ECDC to estimate the positive predictive value of respiratory symptoms in a given community, thus providing information on the level of virus circulation based on the data from the application.

(17) Given the functions of smartphone applications as described above, their use is capable of affecting the exercise of certain fundamental rights such as inter alia the right to respect for private and family life. As any interference with those rights should be in accordance with

[7] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

[8] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1).

the law, Member States' laws which would set out or permit limitations to the exercise of certain fundamental rights should be in line with the general principles of Union law as stated in Article 6 of the Treaty on the European Union, their constitutional traditions and their obligations under international law.

(18) For the acceptance of different types of applications (and underlying infection transmission chains information systems) and for ensuring that they fulfil the stated purpose of epidemiological surveillance, the underlying policies, requirements and controls must be aligned and implemented in a coordinated way by the responsible national health authorities. The experience of several Member States that started introducing contact tracing applications shows that, in order to increase the acceptance, an integrated governance is useful to prepare and implement the measures, 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. A wide communication concerning the application is also essential for its take-up and success.

(19) In order to detect proximity encounters between users of different contact tracing applications (a scenario most likely to happen among people moving across national/ regional borders), interoperability between applications should be envisaged. National health authorities supervising infection transmission chains should be able to exchange interoperable information about users that have tested positive with other Member States or regions in order to address cross-border transmission chains.

(20) Certain companies including telecommunications providers and major technology platforms have published or made available to public authorities anonymised and aggregated location data. Such data is necessary for research to combat the virus, modelling to understand how the virus will spread and modelling of the economic effects of the crisis. In particular, the data will help to understand and model the spatial dynamics of the epidemic and to assess the impact of social distancing measures (travel limitations, non-essential activities closures, total lock-down etc.) on mobility. This is essential firstly to contain the effects of the virus and assess the needs notably in terms of Personal Protective Equipment and Intensive Care Units and, second, to support the exit strategy with data-driven models that indicate the potential effects of the relaxation of the social distancing measures.

(21) The current crisis has shown that public health authorities and research institutions would benefit from further access to essential information to analyse the evolution of the virus and to assess the effectiveness of public health measures.

(22) Certain Member States have taken measures to simplify access to necessary data. However, the EU's common efforts combating the virus are hampered by the current fragmentation of approaches.

(23) A common Union approach to the COVID-19 crisis has also become necessary since measures taken in certain countries, such as the geolocation-based tracking of individuals, the use of technology to rate an individual's level of health risk and the centralisation of sensitive data, raise questions from the viewpoint of several fundamental rights and freedoms guaranteed in the EU legal order, including the right to privacy and the right to the protection

of personal data. In any event, pursuant to the Charter of Fundamental Rights of the Union, restrictions on the exercise of the fundamental rights and freedoms laid down therein must be justified and proportionate. Any such restrictions should, in particular, be temporary, in that they remain strictly limited to what is necessary to combat the crisis and do not continue to exist, without an adequate justification, after the crisis has passed.

(24) Furthermore, the World Health Organisation and other bodies have warned of the risk that applications and inaccurate data could result in stigmatisation of persons who share certain characteristics because of a perceived link with the disease.

(25) In accordance with the principle of data minimization, public health authorities and research institutions should process personal data only where adequate, relevant and limited to what is necessary, and should apply appropriate safeguards such as pseudonymisation, aggregation, encryption and decentralization.

(26) Effective cybersecurity and data security measures are essential to protect the availability, authenticity integrity and confidentiality of data.

(27) Consultation with data protection authorities, in accordance with the requirements set out in Union law on the protection of personal data, is essential to ensure that personal data is processed lawfully and that the rights of the individuals concerned are respected.

(28) Article 14 of Directive 2011/24/EU assigned the Union to support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States ('the eHealth Network'). Its objectives include working towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare. Commission Implementing Decision (EU) 2019/1765 [9], lays down the rules for the establishment, management and transparent functioning of the eHealth Network. Because of its composition and area of expertise, the eHealth Network should be the main forum for discussions on the data needs of the public health authorities and research institutions, whilst also involving officials from national regulatory authorities for electronic communications, ministries in charge of digital matters and data protection authorities.

(29) The eHealth Network and the Commission should also closely co-operate with other bodies and networks that can provide the input necessary to give effect to this Recommendation, including the Health Security Committee, the network for the epidemiological surveillance of the communicable diseases, the ECDC, the European Data Protection Board, the Body of European Regulators for Electronic Communications and the Network Information Systems Cooperation Group.

(30) Transparency and clear and regular communication, and allowing for the input of

[9] Commission Implementing Decision (EU) 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (OJ L 270, 24.10.2019, p. 83).

persons and communities most affected, will be paramount to ensuring public trust when combating the COVID-19 crisis.

(31) Considering the rapid evolution of the situation in the various Member States in respect of the COVID-19 crisis, it is essential that Member States report and the Commission reviews the approach embodied in this Recommendation, quickly and regularly for as long as the crisis persists.

(32) This Recommendation should, where necessary, be complemented by additional guidance by the Commission, including on the data protection and privacy implications of the use of warn and prevent mobile applications,
HAS ADOPTED THIS RECOMMENDATION:
PURPOSE OF THIS RECOMMENDATION
(1)
This recommendation sets up a process for developing a common approach, referred to as a Toolbox, to use digital means to address the crisis. The Toolbox will consist of practical measures for making effective use of technologies and data, with a focus on two areas in particular:
(1) A pan-European approach for the use of mobile applications, coordinated at Union level, for empowering citizens to take effective and more targeted social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease. This will involve a methodology monitoring and sharing assessments of effectiveness of these applications, their interoperability and cross-border implications, and their respect for security, privacy and data protection; and

(2) A common scheme for using anonymized and aggregated data on mobility of populations in order (i) to model and predict the evolution of the disease, (ii) to monitor the effectiveness of decision-making by Member States' authorities on measures such as social distancing and confinement, and (iii) to inform a coordinated strategy for exiting from the COVID-19 crisis.

(2) Member States should take these actions as a matter of urgency and in close coordination with other Member States, the Commission and other relevant stakeholders, and without prejudice to the competences of the Member States in the domain of public health. They should ensure that all actions are taken in accordance with Union law, in particular law on medical devices and the right to privacy and the protection of personal data along with other rights and freedoms enshrined in the Charter of Fundamental Rights of the Union. The Toolbox will be complemented by Commission guidance, including guidance on the data protection and privacy implications of the use of mobile warning and prevention applications.
DEFINITIONS
(3)
For the purposes of this Recommendation:
(a) 'Mobile applications' means software application running on smart devices, in particular smartphones, designed usually for wide-ranging and targeted interaction with web resources, which process proximity data and other contextual information collected by many sensors found in any smart device and which are able to exchange information via many network interfaces with other connected devices;

(b) 'eHealth Network' means the network established by Article 14 of Directive 2011/24/EU and whose tasks have been clarified by the Implementing Decision (EU) 2019/1765.

(c) 'Health Security Committee' means the body composed of representatives of the Member States, established under the Article 17 of the Decision No 1082/2013/EU.

(d) 'Epidemiological Surveillance Network' means the network for the epidemiological surveillance of communicable diseases and of related special health issues operated and coordinated by the ECDC and bringing into permanent communication the Commission, the ECDC, and the competent authorities responsible at national level for epidemiological surveillance, set up under the Article 6 of the Decision No 1082/2013/EU.
PROCESS FOR DEVELOPING A TOOLBOX FOR USE OF TECHNOLOGY AND DATA
(4) This process should facilitate the urgent development and adoption by Member States and the Commission of a toolbox of practical measures including a European approach for COVID-19 mobile applications and for the use of mobility data for modelling and predicting the evolution of the virus.

(5) For the development of the toolbox, Member States, represented in the eHealth Network, should meet, together with representatives of the Commission and the European Centre for Disease Control, immediately and frequently thereafter. They should share views on how best to use data from various sources to tackle the COVID-19 crisis whilst achieving a high level of trust and security in a manner compatible with Union law, in particular on the protection of personal data and privacy, as well as to share best practices and facilitate common approaches in that respect.

(6) The eHealth Network should meet immediately to operationalize this Recommendation.

(7) The Member States, represented in the eHealth Network, should, as appropriate, inform and seek input from the Health Security Committee, the Body of European Regulators for Electronic Communications, the NIS Cooperation Group and relevant Commission agencies, including ENISA, Europol, and Council working groups, when giving effect to this Recommendation.

(8) The European Data Protection Board and the European Data Protection Supervisor should also be closely involved to ensure the Toolbox integrates data protection and privacy-by-design principles.

(9) Member States authorities and the Commission should ensure regular, clear and comprehensive communication to the public on the actions taken pursuant to this Recommendation and provide opportunities for the public to interact and participate in discussions.

(10)
Paramount throughout the process should be respect for all fundamental rights, notably privacy as well as data protection, the prevention of surveillance and stigmatization. On these specific issues, the Toolbox should therefore:

(1) strictly limit the processing of personal data for the purposes of combating the COVID-19 crisis and ensure that the personal data are not used for any other purposes such as law enforcement or commercial purposes;

(2) ensure regular review of the continued need for the processing of personal data for the purposes of combating the COVID-19 crisis and set appropriate sunset clauses, so as to ensure that the processing does not extend beyond what is strictly necessary for those purposes;

(3) take measures to ensure that, once the processing is no longer strictly necessary, the processing is effectively terminated and the personal data concerned are irreversibly destroyed, unless, on the advice of ethics boards and data protection authorities, their scientific value in serving the public interest outweighs the impact on the rights concerned, subject to appropriate safeguards.

(11) The Toolbox should be developed progressively in the light of discussions with all interested parties and monitoring of the situation, best practice, issues and solution concerning the sources and types of data necessary and available for public health authorities and public health research institutions for combating the COVID-19 pandemic.

(12) The Toolbox should be shared with the European Union's international partners to exchange best practices and help address the virus spread worldwide.
A PAN-EUROPEAN APPROACH FOR COVID-19 MOBILE APPLICATIONS
(13)
The first priority for the Toolbox should be a pan-European approach for COVID-19 mobile applications, to be developed together by Member States and the Commission, by 15 April 2020. The European Data Protection Board and the European Data Protection supervisor will be associated to the process. This approach should consist of:
(1) specifications to ensure the effectiveness of mobile information, warning and tracing applications for combating COVID-19 from the medical and technical point of view;

(2) measures to prevent proliferation of applications that are not compatible with Union law, to support requirements for accessibility for persons with disabilities, and for interoperability and promotion of common solutions, not excluding a potential pan-European application;

(3) governance mechanisms to be applied by public health authorities and cooperation with the ECDC;

(4) the identification of good practices and mechanisms for exchange of information on the functioning of the applications; and

(5) sharing data with relevant epidemiological public bodies and public health research institutions, including aggregated data to ECDC.

(14) Member State authorities, represented in the eHealth Network, should establish a process of exchanging information and ensuring interoperability of applications when cross-border scenarios are foreseen.
PRIVACY AND DATA PROTECTION ASPECTS OF USE OF THE MOBILE

APPLICATIONS
(15) The development of the Toolbox should be guided by privacy and data protection principles.

(16)
With particular regard the use of COVID-19 mobile warning and prevention applications, the following principles should be observed:
(1) safeguards ensuring respect for fundamental rights and prevention of stigmatization, in particular applicable rules governing protection of personal data and confidentiality of communications;

(2) preference for the least intrusive yet effective measures, including the use of proximity data and the avoidance of processing data on location or movements of individuals, and the use of anonymised and aggregated data where possible;

(3) technical requirements concerning appropriate technologies (e.g. Bluetooth Low Energy) to establish device proximity, encryption, data security, storage of data on the mobile device, possible access by health authorities and data storage;

(4) effective cybersecurity requirements to protect the availability, authenticity integrity, and confidentiality of data;

(5) the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control, at the latest;

(6) uploading of proximity data in case of a confirmed infection and appropriate methods of warning persons who have been in close contact with the infected person, who shall remain anonymous; and

(7) transparency requirements on the privacy settings to ensure trust into the applications.

(17) The Commission will publish guidance further specifying privacy and data protection principles in the light of practical considerations arising from the development and implementation of the Toolbox.
USE OF MOBILITY DATA TO INFORM MEASURES AND EXIT STRATEGY
(18)
The second priority for the Toolbox should be a common approach for the use of anonymised and aggregated mobility data necessary for:
(1) modelling to map and predict the diffusion of the disease and the impact on needs in the health systems in Member States, such as, but not limited, to Intensive Care Units in Hospitals and Personal Protective Equipment; and

(2) optimising the effectiveness of measures to contain the diffusion of the COVID-19 virus and to address its effects, including confinement (and de-confinement), and to obtain and use those data.

(19) In developing this approach, Member States (represented in the eHealth Network,

which will coordinate with the Health Security Committee, the Epidemiological Network the ECDC and, if necessary, ENISA), should exchange best practices on the use of mobility data, share and compare modelling and predictions of the diffusion of the virus, and monitor the impact of measures to limit its diffusion.

(20)
This deliverable should include:
(1) the appropriate use of anonymous and aggregated mobility data for modelling to understand how the virus will spread and modelling of the economic effects of the crisis;

(2) advice to public authorities on asking providers of the data for the methodology that they have applied for anonymising the data and to carry out a plausibility test of the methodology applied;

(3) safeguards to be put in place to prevent de-anonymisation and avoid re-identifications of individuals, including guarantees of adequate levels of data and IT security, and assessment of re-identification risks when correlating the anonymised data with other data;

(4) immediate and irreversible deletion of all accidentally processed data capable of identifying individuals and notifying the providers of the data as well as competent authorities of the accidental processing and deletion;

(5) deletion of the data in principle after a period of 90 days, or in any event no later than when the pandemic is declared under control; and

(6) restricting processing of the data exclusively for the purposes stated above and exclude sharing of the data with any third party.
REPORTING AND REVIEW
(21) The pan-European approach for COVID-19 mobile applications will be published on 15 April and will be complemented by Commission guidance on privacy and data protection.

(22) Member States should, by 31 May 2020, report to the Commission on the actions taken pursuant to this Recommendation. Such reports should continue on regular basis for as long as the COVID-19 crisis persists.

(23) As of 8 April 2020, Member States should make the measures applied in the areas covered by this Recommendation accessible to other Member States and to the Commission for peer review. Within one week, Member States and the Commission may submit observations on these measures. The Member State concerned should take utmost account of such observations.

(24) The Commission will, starting in June 2020, on the basis of these Member States reports, assess the progress made and the effect of this Recommendation. The Commission may make further recommendations to Member States, including on the timing of the measures applied in the areas covered by this Recommendation.
Done at Brussels, 8 April 2020.
For the Commission
Thierry BRETON
Member of the Commission

European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020

The European Data Protection Board has adopted the following statement:
Governments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19. This can involve the processing of different types of personal data.

Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. The fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way. It is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world. Even so, the EDPB would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data and in all cases it should be recalled that any measure taken in this context must respect the general principles of law and must not be irreversible. Emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period.

1. Lawfulness of processing
The GDPR is a broad piece of legislation and provides for rules that also apply to the processing of personal data in a context such as the one relating to COVID-19. The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein. For example, when processing is necessary for reasons of substantial public interest in the area of public health. Under those circumstances, there is no need to rely on consent of individuals.

With regard to the processing of personal data, including special categories of data by competent public authorities (e.g. public health authorities), the EDPB considers that articles 6 and 9 GDPR enable the processing of personal data, in particular when it falls under the legal mandate of the public authority provided by national legislation and the conditions enshrined in the GDPR.
In the employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health.
The GDPR also foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health (Art. 9.2.i), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Art.9.2.c), as recital 46 explicitly refers to the control of an epidemic.
With regard to the processing of telecom data, such as location data, national laws implementing the ePrivacy Directive must also be respected. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals.

However, Art. 15 of the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security. Such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society. These measures must be in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Moreover, it is subject to the judicial control of the European Court of Justice and the European Court of Human Rights. In case of an emergency situation, it should also be strictly limited to the duration of the emergency at hand.

2. Core principles relating to the processing of personal data

Personal data that is necessary to attain the objectives pursued should be processed for specified and explicit purposes.

In addition, data subjects should receive transparent information on the processing activities that are being carried out and their main features, including the retention period for collected data and the purposes of the processing. The information provided should be easily accessible and provided in clear and plain language.

It is important to adopt adequate security measures and confidentiality policies ensuring that personal data are not disclosed to unauthorised parties. Measures implemented to manage the current emergency and the underlying decision-making process should be appropriately documented.

3. Use of mobile location data

Can Member State governments use personal data related to individuals' mobile phones in their efforts to monitor, contain or mitigate the spread of COVID-19?

In some Member States, governments envisage using mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19. This would imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area by phone or text message. Public authorities should first seek to process location data in an anonymous way (ie. processing data aggregated in a way that individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ("cartography").
Personal data protection rules do not apply to data which has been appropriately anonymised.

When it is not possible to only process anonymous data, the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security (Art. 15).

If measures allowing for the processing of non-anonymised location data are introduced, a Member State is obliged to put in place adequate safeguards, such as providing individuals of electronic communication services the right to a judicial remedy.

The proportionality principle also applies. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved. Invasive measures, such as the "tracking" of individuals (i.e. processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the

concrete modalities of the processing. However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation).

4. Employment

Can an employer require visitors or employees to provide specific health information in the context of COVID-19?

The application of the principle of proportionality and data minimisation is particularly relevant here. The employer should only require health information to the extent that national law allows it.

Is an employer allowed to perform medical check-ups on employees?
The answer relies on national laws relating to employment or health and safety. Employers should only access and process health data if their own legal obligations requires it.

Can an employer disclose that an employee is infected with COVID-19 to his colleagues or to externals?
Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

What information processed in the context of COVID-19 can be obtained by the employers?
Employers may obtain personal information to fulfil their duties and to organise the work in line with national legislation.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

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
Adopted on 21st April 2020

The European Data Protection Board
Having regard to Article 70(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 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 (hereinafter "GDPR"),
Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,
Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

1. INTRODUCTION & CONTEXT
Governments and private actors are turning toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns. The EDPB underlines that the data protection legal framework was designed to be flexible and as such, is able to achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.
The EDPB firmly believes that, when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European approach in response to the current crisis, or at least put in place an interoperable framework.
The EDPB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures. The general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.
These guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:
using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures ;
contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible.
The efficiency of the contribution of contact tracing applications to the management of the pandemic depends on many factors (e.g., percentage of people who would need to install it; definition of a "contact" in terms of closeness and duration.). Moreover, such applications need to be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of doubt removal.

Their deployment should be accompanied by supporting measures to ensure that the information provided to the users is contextualized, and that alerts can be of use to the public health system. Otherwise, these applications might not reach their full impact.
The EDPB emphasises that the GDPR and Directive 2002/58/EC (the "ePrivacy Directive") both contain specific rules allowing for the use of anonymous or personal data to support public authorities and other actors at national and EU levels in monitoring and containing the spread of the SARS-CoV-2 virus.
In this regard, the EDPB has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users.

2. USE OF LOCATION DATA

2.1 Sources of location data

There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:

- location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service ; and
- location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).

The EDPB recalls that location data[4] collected from electronic communication providers may only be processed within the remits of articles 6 and 9 of the ePrivacy Directive. This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users,
Regarding information, including location data, collected directly from the terminal equipment, art 5(3) Of the "ePrivacy" directive applies. Hence, the storing of information on the user's device or gaining access to the information already stored is allowed only if (i) the user has given consent or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.
Derogations to the rights and obligations provided for in the "ePrivacy" Directive are however possible pursuant to Art. 15. when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives.

> As for the re-use of location data collected by an information society service provider for modelling purposes (e.g., through the operating system or some previously installed application) additional conditions must be met. Indeed, when data have been collected in compliance with 5(3) Of the ePrivacy Directive, they can only be further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23 (1) GDPR.

2.2 Focus on the use of anonymised location data

The EDPB emphasises that when it comes to using location data, preference should always be given to the processing of anonymised data rather than personal data.
Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any "reasonable" effort. This "reasonability test" must take into account both objective aspects (time, technical

means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR.
Evaluating the robustness of anonymisation relies on three criteria: (i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual).
The concept of anonymisation is prone to being misunderstood and is often mistaken for pseudonymisation. While anonymisation allows using the data without any restriction, pseudonymised data are still in the scope of the GDPR.
Many options for effective anonymisation exist', but with a caveat. Data cannot be anonymised on their own, meaning that only datasets as a whole may or may not be made anonymous. In this sense, any intervention on a single data pattern (by means of encryption, or any other mathematical transformations) can at best be considered a pseudonymisation.
Anonymisation processes and re-identification attacks are active fields of research. It is crucial for any controller implementing anonymisation solutions to monitor recent developments in this field, especially concerning location data (originating from telecom operators and/or
information society services) which are known to be notoriously difficult to anonymise.
Indeed, a large body of research has shown that *Location data thought to be anonymised* may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances.

> A single data pattern tracing the location of an individual over a significant period of time cannot be fully anonymised. This assessment may still hold true if the precision of the recorded geographical coordinates is not sufficiently lowered, or if details of the track are removed and even if only the location of places where the data subject stays for substantial amounts of time are retained. This also holds for location data that is poorly aggregated.
>
> To achieve anonymisation, location data must be carefully processed in order to meet the reasonability test. In this sense, such a processing includes considering location datasets as a whole, as well as processing data from a reasonably large set of individuals using available robust anonymisation techniques, provided that they are adequately and effectively implemented.
>
> Lastly, given the complexity of anonymisation processes, transparency regarding the anonymisation methodology is highly encouraged.

3. CONTACT TRACING APPLICATIONS

3.1 General legal analysis

> The systematic and large scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. It can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.
>
> To ensure accountability, the controller of any contact tracing application should be clearly defined. The EDPB considers that the national health authorities could

be the controllers for such application; other controllers may also be envisaged. In any cases, if the deployment of contact tracing apps involves different actors their roles and responsibilities must be clearly established from the outset and be explained to the users.

In addition, with regard to the principle of purpose limitation, the purposes must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g., commercial or law enforcement purposes). Once the objective has been clearly defined, it will be necessary to ensure that the use of personal data is adequate, necessary and proportionate.

In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default:

- contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used;
- as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;
- the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.

Regarding the lawfulness of the processing, the EDPB notes that contact tracing applications involve storage and/or access to information already stored in the terminal, which are subject to Art. 5(3) Of the "ePrivacy" Directive. If those operations are strictly necessary in order for the provider of the application to provide the service explicitly requested by the user the processing would not require his/her consent. For operations that are not strictly necessary, the provider would need to seek the consent of the user.

Furthermore, the EDPB notes that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR.

Article 6(3) GDPR clarifies that the basis for the processing referred to in article 6(i)(e) shall be laid down by Union or Members State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, Shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application. A clear specification of purpose and explicit limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing. Finally, the EDPB also recommends including, as soon as practicable, the criteria to

determine when the application shall be dismantled and which entity shall be responsible and accountable for making that determination.

> However, if the data processing is based on another legal basis, such as consent (Art. 6(1)(a)) for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met.
>
> Moreover, the use of an application to fight the COVID-19 pandemic might lead to the collection of health data (for example the status of an infected person). Processing of such data is allowed when such processing is necessary for reasons of public interest in the area of public health, meeting the conditions of art. 9(2)(i) GDPR or for health care purposes as described in Art. 9(2)(h) GDPR. Depending on the legal basis, it might also be based on explicit consent (Art. 9(2)(a) GDPR).
>
> In accordance with the initial purpose, Article 9(2)(j) GDPR also allows for health data to be processed when necessary for scientific research purposes or statistical purposes.
>
> The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates. Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only for the duration of the COVID-lg crisis. Afterwards, as a general rule, all personal data should be erased or anonymised.
>
> It is the EDPB's understanding that such apps cannot replace, but only support, manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not (e.g., when interacting with someone protected by adequate equipment — cashiers, etc. -- or not). The EDPB underlines that procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives. In particular, the task of providing advice on next steps should not be based solely on automated processing.
>
> In order to ensure their fairness, accountability and, more broadly, their compliance with the law, algorithms must be auditable and should be regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny.
>
> False positives will always occur to a certain degree. As the identification of an infection risk probably can have a high impact on individuals, such as remaining in self isolation until tested negative, the ability to correct data and/or subsequent analysis results is a necessity. This, of course, should only apply to scenarios and implementations where data is processed and/or stored in a way where such correction is technically feasible and where the adverse effects mentioned above are likely to happen.
>
> Finally the EDPB considers that a data protection impact assessment (DPIA) must be carried out before implementing such tool as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution). The EDPB strongly recommends the publication of DPIAs.

1.2 Recommendations and functional requirements

According to the principle of data minimization, among other measures of Data Protection by Design and by Default, the data processed should be reduced to the strict minimum. The application should not collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.

Data broadcasted by applications must only include some unique and pseudonymous identifiers, generated by and specific to the application. Those identifiers must be renewed regularly, at a frequency compatible with the purpose of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals.

Implementations for contact tracing can follow a centralized or a decentralized approach. Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individuals rights.

Any server involved in the contact tracing system must only collect the contact history or the pseudonymous identifiers of a user diagnosed as infected as the result of a proper assessment made by health authorities and of a voluntary action of the user. Alternately, the server must keep a list of pseudonymous identifiers of infected users or their contact history only for the time to inform potentially infected users of their exposure, and should not try to identify potentially infected users.

Putting in place a global contact tracing methodology including both applications and manual tracing may require additional information to be processed in some cases. In this context, this additional information should remain on the user terminal and only be processed when strictly necessary and with his prior and specific consent.

State-of-the-art cryptographic techniques must be implemented to secure the data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between the application and the server must also be performed.

The reporting of users as COVID-i9 infected on the application must be subject to proper authorization, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status.

The controller, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national contact tracing app in order to mitigate the risk that individuals use a third-party app.

4. CONCLUSION

The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the "ratchet effect". It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and

subject to periodic and genuine review as well as to scientific evaluation.
The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process.
For the European Data Protection Board
The Chair
(Andrea Jelinek)

ANNEX - CONTACT TRACING APPLICATIONS
ANALYSIS GUIDE

0. Disclaimer

The following guidance is neither prescriptive nor exhaustive, and its sole purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications. Other solutions than the ones described here can be used and can be lawful as long as they comply with the relevant legal framework (i.e. GDPR and the "ePrivacy" Directive).

It must also be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide.

1. Summary

In many Member States stakeholders are considering the use of *contact tracing"* applications to help the population discover whether they have been in contact with a person infected with SARS-Cov-2".

The conditions under which such applications would contribute effectively to the management of the pandemic are not yet established. And these conditions would need to be established prior to any implementation of such an app. Yet, it is relevant to provide guidelines bringing relevant information to development teams upstream, so that the protection of personal data can be guaranteed from the early design stage.

It must be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide. The purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications.

Some criteria might go beyond the strict requirements stemming from the data protection framework. They aim at ensuring the highest level of transparency, in order to favour social acceptance of such contact tracing applications.

To this end, publishers of contact tracing applications should take into account the following criteria:

- The use of such an application must be strictly voluntary. It may not condition the access to any rights guaranteed by law. Individuals must have full control over their data at all times, and should be able to choose freely to use such an application.
- Contact tracing applications are likely to result in a high risk to the rights and freedoms of natural persons and to require a data protection impact assessment to be conducted prior to their deployment.
- Information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data.
- When a user is diagnosed infected with the SARS-Cov-2 virus, only the persons with whom the user has been in close contact within the epidemiologically relevant retention period for contact tracing, should be informed.
- The operation of this type of application might require, depending on the architecture that is chosen, the use of a centralised server. In such a case and in accordance with the principles of data minimisation and data protection by design, the data processed by the centralised

server should be limited to the bare minimum:

- When a user is diagnosed as infected, information regarding its previous close contacts or the identifiers broadcasted by the user's application can be collected, only with the user's agreement. A verification method needs to be established that allows asserting that the person is indeed infected without identifying the user. Technically this could be achieved by alerting contacts only following the intervention of a healthcare professional, for example by using a special one-time code.
- The information stored on the central server should neither allow the controller to identify users diagnosed as infected or having been in contact with those users, nor should it allow the inference of contact patterns not needed for the determination of relevant contacts.

• The operation of this type of application requires to broadcast data that is read by devices of other users and listening to these broadcasts:

- It is sufficient to exchange pseudonymous identifiers between users' mobile equipment (computers, tablets, connected watches, etc.), for example by broadcasting them (e.g. via the Bluetooth Low Energy technology).
- Identifiers must be generated using state-of-the-art cryptographic processes.
- Identifiers must be renewed on a regular basis to reduce the risk of physical tracking and linkage attacks.

• This type of application must be secured to guarantee safe technical processes. In particular:

- The application should not convey to the users information that allows them to infer the identity or the diagnosis of others. The central server must neither identify users, nor infer information about them.

Disclaimer: the above principles are related to the claimed purpose of *contact tracing* applications, and to this purpose only, which only aim to automatically inform people potentially exposed to the virus (without having to identify them).The operators of the application and its infrastructure may be controlled by the competent supervisory authority. Following all or part of these guidelines is not necessarily sufficient to ensure a full compliance to the data protection framework.

2. Definitions

Contact	Parameters for duration of exposure and distance between people must be estimated by the health authorities and can be set in the application. For a contact tracing application, a contact is a user who has participated in an interaction with a user confirmed to be a carrier of the virus, and whose duration and distance induce a risk of significant exposure to the virus infection.
Location data	It refers to all data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service (as defined in the e-Privacy Directive), as well as data from potential other sources, relating to: • the latitude, longitude or altitude of the terminal equipment; • the direction of travel of the user; or • the time the location information was recorded.
Interaction	In the context of the contact tracing application, an interaction is defined as the exchange of information between two devices located in close proximity to each other (in space and time), within the range of the communication technology used (e.g. Bluetooth). This definition excludes the location of the two users of the interaction.
Virus carrier	In this document, we consider virus carriers to be users who have been tested positive for the virus and who have received an official diagnosis from physicians or health centres.

Contact tracing	People who have been in close contact (according to criteria to be defined by epidemiologists) with an individual infected with the virus run a significant risk of also being infected and of infecting others in turn. Contact tracing is a disease control methodology that lists all people who have been in close proximity to a carrier of the virus so as to check whether they are at risk of infection and take the appropriate sanitary measures towards them.

3. General

GEN-1	The application must be a complementary tool to traditional contact tracing techniques (notably interviews with infected persons), i.e. be part of a wider public health program. It must be used only up until the point manual contact tracing techniques can manage alone the amount of new infections.
GEN-2	At the latest when "return to normal" is decided by the competent public authorities, a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases (mobile applications and servers).
GEN-3	The source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and where relevant - contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data.
GEN-4	The stages of deployment of the application must make it possible to progressively validate its effectiveness from a public health point of view. An evaluation protocol, specifying indicators allowing to measure the effectiveness of the application, must bedefined upstream for this purpose.

4. Purposes

PUR-1	The application must pursue the sole purpose of contact tracing so that people potentially exposed to the SARS-Cov-2 virus can be alerted and taken care of. It must not be used for another purpose.
PUR-2	The application must not be diverted from its primary use for the purpose of monitoring compliance with quarantine or confinement measures and/or social distancing.
PUR-3	The application must not be used to draw conclusions on the location of the users based on their interaction and/or any other means.

5. Functional considerations

FUNC-1	The application must provide a functionality enabling users to be informed that they have been potentially exposed to the virus, this information being based on proximity to an infected user within a window of X days prior to the positive screening test (the X value being defined by the health authorities).
FUNC-2	The application should provide recommendations to users identified as having being potentially exposed to the virus. It should relay instructions regarding the measures they should follow, and they should allow the user to request advises. In such cases, a human intervention would be mandatory.
FUNC-3	The algorithm measuring the risk of infection by taking into account factors of distance and time and thus determining when a contact has to be recorded in the contact tracing list, must be securely tuneable to take into account the most recent knowledge on the spread of the virus.
FUNC-4	Users must be informed in case they have been exposed to the virus, or must regularly obtain information on whether or not they have been exposed to the virus, within the incubation period of the virus.
FUNC-5	The application should be interoperable with other applications developed across EU Member States, so that users travelling across different Member States can be efficiently notified.

6. Data

DATA-1	The application must be able to broadcast and receive data via proximity communication technologies like Bluetooth Low Energy so that contact tracing can be carried out.
DATA-2	This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application.
DATA-3	The risk of collision between pseudo-random identifiers should be sufficiently low.
DATA-4	Pseudo-random identifiers must be renewed regularly, at a frequency sufficient to limit the risk of re-identification, physical tracking or linkage of individuals, by anyone including central server operators, other application users or malicious third parties. These identifiers must be generated by the user's application, possibly based on a seed provided by the central server.

DATA-5	According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing
DATA-6	The application must not collect location data for the purpose of contact tracing. Location data can be processed for the sole purpose of allowing the application to interact with similar applications in other countries and should be limited in precision to what is strictly necessary for this sole purpose.
DATA-7	The application should not collect health data in addition to those that are strictly necessary for the purposes of the app, except on an optional basis and for the sole purpose of assisting in the decision making process of informing the user.
DATA-8	Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization.

7. Technical properties

TECH-1	The application should available technologies such as use proximity communication technology (e.g. Bluetooth Low Energy) to detect users in the vicinity of the device running the application.
TECH-2	The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time.
TECH-3	The application may rely on a central server to implement some of its functionalities.
TECH-4	The application must be based on an architecture relying as much as possible on users' devices.
TECH-5	At the initiative of users reported as infected by the virus and after confirmation of their status by an appropriately certified health professional, their contact history or their own identifiers should be transmitted to the central server.

8. Security

SEC-1	A mechanism must verify the status of users who report as SARS-CoV-2positive in the application, for example by providing a single-use code linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, data must not be processed.
SEC-2	The data sent to the central server must be transmitted over a secure channel. The use of notification services provided by OS platform providers should be carefully assessed, and should not lead to disclosing any data to third parties.
SEC-3	Requests must not be vulnerable to tampering by a malicious user
SEC-4	State-of-the-art cryptographic techniques must be implemented to secure exchanges between the application and the server and between applications and as a general rule to protect the information stored in the applications and on the server. Examples of techniques that can be used include for example : symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption, etc.
SEC-5	The central server must not keep network connection identifiers (e.g., IP addresses) of any users including those who have been positively diagnosed and who transmitted their contacts history or their own identifiers.
SEC-6	In order to avoid impersonation or the creation of fake users, the server must authenticate the application.
SEC-7	The application must authenticate the central server.
SEC-8	The server functionalities should be protected from replay attacks.
SEC-9	The information transmitted by the central server must be signed in order to authenticate its origin and integrity.
SEC-10	Access to all data stored in the central server and not publicly available must be restricted to authorised persons only.
SEC-11	The device's permission manager at the operating system level must only request the permissions necessary to access and use when necessary the communication modules, to store the data in the terminal, and to exchange information with the central server.

9. Protection of personal data and privacy of natural persons
Reminder: the following guidelines concern an application whose sole purpose is contact tracing.

PRIV-1	Data exchanges must be respectful of the users' privacy (and notably respect the principle of data minimisation).
PRIV-2	The application must not allow users to be directly identified when using the application.
PRIV-3	The application must not allow users' movements to be traced.
PRIV-4	The use of the application should not allow users to learn anything about other users (and notably whether they are virus carriers or not).
PRIV-5	Trust in the central server must be limited. The management of the central server must follow clearly defined governance rules and include all necessary measures to ensure its security. The localization of the central server should allow an effective supervision by the competent supervisory authority.
PRIV-6	A Data Protection Impact Assessment must be carried out and should be made public.
PRIV-7	The application should only reveal to the user whether they have been exposed to the virus, and, if possible without revealing information about other users, the number of times and dates of exposure.
PRIV-8	The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements.
PRIV-9	The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement.
PRIV-10	Requests made by the applications to the central server must not reveal anything about the virus carrier.
PRIV-11	Requests made by the applications to the central server must not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.
PRIV-12	Linkage attacks must not be possible.

PRIV-13	Users must be able to exercise their rights via the application.
PRIV-14	Deletion of the application must result in the deletion of all locally collected data.
PRIV-15	The application should only collect data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices shall be collected.
PRIV-16	In order to avoid re-identification by the central server, proxy servers should be implemented. The purpose of these *non-colluding servers is to* mix the identifiers of several users (both those of virus carriers and those sent by requesters) before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users.
PRIV-17	The application and the server must be carefully developed and configured in order not to collect any unnecessary data (e.g., no identifiers should be included in the server logs, etc.) and in order to avoid the use of any third party SDK collecting data for other purposes.

Most contact tracing applications currently being discussed follow basically two approaches when a user is declared infected: they can either send to a server the history of proximity contacts they have obtained through scanning, or they can send the list of their own identifiers that were broadcasted. The following principles are declined according to these two approaches. While these approaches are discussed here, that does not mean other approaches are not possible or even preferable, for example approaches that implement some form of E2E encryption or apply other security or privacy enhancing technologies.

1.1 **Principles that apply only when the application sends to the server a list of contacts:**

CON-1	The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action on their part.
CON-2	The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus.
CON-3	Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person.
CON-4	Except when the user detected as positive shares his contact history with the central server or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.

CON-5	Any identifier included in the local history must be deleted after X days from its collection (the X value being defined by the health authorities).
CON-6	Contact histories submitted by distinct users should not further be processed e.g. cross-correlated to build global proximity maps.
CON-7	Data in server logs must be minimised and must comply with data protection requirements

1.2 **Principles that apply only when the application sends to a server a list of its own identifiers:**

ID-1	The central server must collect the identifiers broadcast by the application of users reported as positive to COVID-19, as a result of voluntary action on their part.
ID-2	The central server must not maintain nor circulate the contact history of users carrying the virus.
ID-3	Identifiers stored on the central server must be deleted once they were distributed to the other applications.
ID-4	Except when the user detected as positive shares his identifiers with the central server, no data must leave the user's equipment or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.
ID-5	Data in server logs must be minimised and must comply with data protection requirements

REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 June 2021

on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 21(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) Every citizen of the Union has the fundamental right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give effect to them. Directive 2004/38/EC of the European Parliament and of the Council ([3]) lays down detailed rules as regards the exercise of that right.

(2) On 30 January 2020, the Director-General of the World Health Organization (WHO) declared a public health emergency of international concern over the global outbreak of severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), which causes coronavirus disease 2019 (COVID-19). On 11 March 2020, the WHO made an assessment characterising COVID-19 as a pandemic.

(3) To limit the spread of SARS-CoV-2, the Member States have adopted some measures which have had an impact on the exercise by Union citizens of their right to move and reside freely within the territory of the Member States, such as entry restrictions or requirements for cross-border travellers to undergo quarantine or self-isolation or to be tested for SARS-CoV-2 infection.

([1]) Opinion of 27 April 2021 (not yet published in the Official Journal).

([2]) Position of the European Parliament of 9 June 2021 (not yet published in the Official Journal) and decision of the Council of 11 June 2021.

([3]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

(4) On 13 October 2020, the Council adopted Recommendation (EU) 2020/1475 ([4]), which introduced a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic in the following key areas: the application of common criteria and thresholds when deciding whether to introduce restrictions to free movement, a mapping of risk areas of SARS-CoV-2 transmission based on an agreed colour code and a coordinated approach to any appropriate measures which could be applied to persons travelling to or from risk areas, depending on the level of risk of SARS-CoV-2 transmission in those areas. In view of their specific situation, the Recommendation emphasises that travellers with an essential function or need, as listed in point 19 of the Recommendation, and persons living in border regions and travelling across the border on a daily or frequent basis for the purposes of work, business, education, family, medical care or caregiving, whose lives are particularly affected by such restrictions, in particular those who exercise critical functions or who are essential for critical infrastructure, should in general be exempted from travel restrictions linked to the COVID-19 pandemic.

(5) Using the criteria and thresholds established in Recommendation (EU) 2020/1475, the European Centre for Disease Prevention and Control (ECDC) has been publishing, on a weekly basis, a map of Member States, with data on the notification, testing and test positivity rates of COVID-19, broken down by region, in order to support Member States' decision-making.

(6) Member States may, in accordance with Union law, limit the fundamental right of free movement on grounds of public health. Any restrictions to the free movement of persons within the Union that are put in place to limit the spread of SARS-CoV-2 should be based on specific and limited public interest grounds, namely the safeguarding of public health as emphasised by Recommendation (EU) 2020/1475. It is necessary for such limitations to be applied in accordance with the general principles of Union law, in particular proportionality and non-discrimination. Any measures taken should therefore be strictly limited in scope and time, in line with the efforts to restore free movement within the Union, and should not extend beyond what is strictly necessary to safeguard public health. Furthermore, such measures should be consistent with measures taken by the Union to ensure the seamless free movement of goods and essential services across the internal market, including the free movement of medical supplies and medical and healthcare personnel through the 'green lane' border crossings referred to in the Commission communication of 23 March 2020 on the implementation of the Green Lanes under the Guidelines for border management measures to protect health and ensure the availability of goods and essential services.

(7) Persons who are vaccinated or who have had a recent negative COVID-19 test result and persons who have recovered from COVID-19 in the previous six months seem to have a reduced risk of infecting people with SARS-CoV-2, according to current and still evolving scientific evidence. The free movement of persons who, according to sound scientific evidence, do not pose a significant risk to public health, for example because they are immune to and cannot transmit SARS-CoV-2, should not be restricted, as such restrictions would not be necessary to achieve the objective of safeguarding public health. Where the epidemiological situation allows, such persons should not be subject to additional restrictions to free movement linked to the COVID-19 pandemic, such as travel-related testing for SARS-CoV-2 infection or travel-related quarantine or self-isolation, unless such additional restrictions are, based on the latest available scientific evidence and in line with the precautionary principle, necessary and proportionate for the purpose of safeguarding public health, and non-discriminatory.

(8) Many Member States have launched or plan to launch initiatives to issue COVID-19 vaccination certificates. However, for such vaccination certificates to be used effectively in a cross-border context when Union citizens exercise their right to free movement, they need to be fully interoperable, compatible, secure and verifiable. A common approach is required among Member States on the content, format, principles, technical standards and the level of security of such vaccination certificates.

(9) Unilateral measures to limit the spread of SARS-CoV-2 have the potential to cause significant disruption to the exercise of the right to free movement and to hinder the proper functioning of the internal market, including the tourism sector, as national authorities and passenger transport services, such as airlines, trains, coaches and ferries, could be confronted with a wide array of diverging document formats, not only regarding certificate holders' COVID-19 vaccination, but also their test results and recovery.

(10) In its resolution of 25 March 2021 on establishing an EU strategy for sustainable tourism, the European Parliament called for a harmonised approach to tourism across the Union by means of implementing common criteria for safe travel, with a Union Health Safety protocol for testing and quarantine requirements, a common vaccination certificate, once there is sufficient scientific evidence that vaccinated persons do not transmit SARS-CoV-2, and the mutual recognition of vaccination procedures.

([4]) Council Recommendation (EU) 2020/1475 of 13 October 2020 on a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic (OJ L 337, 14.10.2020, p. 3).

(11) In their statement of 25 March 2021, the Members of the European Council called for preparations to start on a common approach to the gradual lifting of restrictions to free movement in order to ensure that efforts are coordinated when the epidemiological situation allows for an easing of existing measures and for the work on COVID-19 interoperable and non-discriminatory digital certificates to be taken forward as a matter of urgency.

(12) To facilitate the exercise of the right to move and reside freely within the territory of the Member States, a common framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) should be established. That common framework should be binding and directly applicable in all Member States. It should facilitate, whenever possible on the basis of scientific evidence, the gradual lifting of restrictions in a coordinated manner by Member States, taking into account the lifting of restrictions within their own territory. Regulation (EU) 2021/954 of the European Parliament and of the Council ([5]) extends that common framework to third-country nationals who are legally staying or residing in the Schengen area without controls at internal borders and applies as a matter of Schengen acquis, without prejudice to the specific rules on the crossing of internal borders set out in Regulation (EU) 2016/399 of the European Parliament and of the Council ([6]). Facilitating freedom of movement is one of the key preconditions for starting an economic recovery.

(13) Although this Regulation is without prejudice to Member States' competence to impose restrictions to free movement, in accordance with Union law, to limit the spread of SARS-CoV-2, it should contribute to facilitating the gradual lifting of such restrictions in a coordinated manner whenever possible, in accordance with Recommendation (EU) 2020/1475. Such restrictions could be waived in particular for vaccinated persons, in line with the precautionary principle, to the extent that scientific evidence on the effects of COVID-19 vaccination becomes increasingly available and more consistently conclusive with regard to the breaking of the transmission chain.

(14) This Regulation is intended to facilitate the application of the principles of proportionality and non-discrimination with regard to restrictions to free movement during the COVID-19 pandemic, while pursuing a high level of public health protection. It should not be understood as facilitating or encouraging the adoption of restrictions to free movement, or restrictions to other fundamental rights, in response to the COVID-19 pandemic, given their detrimental effects on Union citizens and businesses. Any verification of the certificates making up the EU Digital COVID Certificate should not lead to further restrictions to the freedom of movement within the Union or to restrictions on travel within the Schengen area. The exemptions to the restrictions of free movement in response to the COVID-19 pandemic referred to in Recommendation (EU) 2020/1475 should continue to apply and the specific situation of cross-border communities, which have been particularly affected by such restrictions, should be taken into account. At the same time, the EU Digital COVID Certificate framework is intended to ensure that interoperable certificates are also available to travellers with an essential function or need.

(15) The introduction of a common approach for the issuance, verification and acceptance of interoperable COVID-19 certificates relies upon mutual trust. The use of counterfeit COVID-19 certificates poses a significant risk to public health. Authorities in one Member State need assurance that the information included in a certificate issued in another Member State is trustworthy, that the certificate has not been forged, that the certificate belongs to the person presenting it, and that anyone verifying the certificate has access only to the minimum amount of information necessary.

(16) On 1 February 2021, Europol issued an Early Warning Notification on the illicit sales of counterfeit COVID-19 test certificates indicating a negative result. Given the availability and ease of access to technological means, such as high-resolution printers and graphics editor software, fraudsters are able to produce high-quality counterfeit COVID-19 certificates. Cases of illicit sales of counterfeit COVID-19 test certificates have been reported, which involve organised forgery rings and opportunistic individuals selling counterfeit COVID-19 certificates on and offline.

(17) It is important to make available sufficient resources to implement this Regulation and to prevent, detect, investigate and prosecute fraud and illicit practices regarding the issuance and use of the certificates making up the EU Digital COVID Certificate.

([5]) Regulation (EU) 2021/954 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID 19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID 19 pandemic (See page 24 of this Official Journal).

([6]) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

(18) To ensure the interoperability of and equal access to the certificates making up the EU Digital COVID Certificate for all Union citizens, including for vulnerable persons, such as persons with disabilities, and for persons with limited access to digital technologies, Member States should issue such certificates in a digital or paper-based format, or both. The prospective holders should be entitled to receive the certificates in the format of their choice. This would allow them to request to receive a paper copy of the certificate, or to receive it in a digital format to be stored and displayed on a mobile device, or both. The certificates should contain an interoperable, digitally readable barcode giving access only to the data relevant to the certificates. Member States should ensure the authenticity, validity and integrity of the certificates through the use of electronic seals. To ensure a high level of trust in the authenticity, validity and integrity of certificates, Member States should, where possible, prioritise the use of advanced electronic seals as defined in point (26) of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([7]). The information on the certificate should be shown in human-readable format, printed or displayed as plain text. The layout of the certificates should be easy to understand and ensure simplicity and user-friendliness. To avoid obstacles to free movement, the certificates should be issued free of charge, and Union citizens and their family members should have a right to have certificates issued to them. To prevent abuse or fraud, it should be possible to charge appropriate fees for the issuance of a new certificate in cases of repeated loss. Member States should issue the certificates making up the EU Digital COVID Certificate automatically or upon request, ensuring that they can be obtained easily and swiftly. Member States should also provide, where needed, the necessary support to allow for equal access by all Union citizens. A separate certificate should be issued for each vaccination, test result or recovery and should not contain data from previous certificates except where otherwise provided for in this Regulation.

(19) Authentic certificates making up the EU Digital COVID Certificate should be individually identifiable by means of a unique certificate identifier, taking into account that holders might be issued more than one certificate during the COVID-19 pandemic. The unique certificate identifier is composed of an alphanumeric string and Member States should ensure that it does not contain any data linking it to other documents or identifiers, such as to passport or identity card numbers, in order to prevent directly identifying the holder. The unique certificate identifier should be used only for its intended purposes, which include requests for the issuance of a new certificate if a certificate is no longer available to the holder and the revocation of certificates. In addition, the use of a unique certificate identifier avoids the need to process other personal data that would otherwise be necessary to identify individual certificates. For medical and public health reasons and in the event of fraudulently issued or obtained certificates, Member States should be able to establish and exchange with other Member States for the purpose of this Regulation certificate revocation lists in limited cases, in particular in order to revoke certificates that have been issued erroneously, as a result of fraud or following the suspension of a COVID-19 vaccine batch found to be defective. Certificate revocation lists should not contain any personal data other than unique certificate identifiers. Holders of revoked certificates should be promptly informed about the revocation of their certificates and the reasons for the revocation.

(20) The issuance of certificates pursuant to this Regulation should not lead to discrimination on the basis of the possession of a specific category of certificate.

(21) Universal, timely and affordable access to COVID-19 vaccines and tests for SARS-CoV-2 infection, which form the basis for the issuance of the certificates making up the EU Digital COVID Certificate, is crucial in the fight against the COVID-19 pandemic and essential to restore freedom of movement within the Union. To facilitate the exercise of the right to free movement, Member States are encouraged to ensure affordable and widely available testing possibilities, taking into account that not the entire population would have had the opportunity to be vaccinated before the date of application of this Regulation.

(22) The security, authenticity, validity and integrity of the certificates making up the EU Digital COVID Certificate and their compliance with Union data protection law are key to their acceptance in all Member States. It is therefore necessary to establish a trust framework laying out the rules on and infrastructure for the reliable and secure issuance and verification of COVID-19 certificates. The infrastructure should be developed, with a strong preference for the use of open-source technology, to function on different major operating systems, while ensuring that it is protected from cybersecurity threats. The trust framework should ensure that the verification of COVID-19 certificates can be carried out offline and without the issuer or any other third party being informed about the

([7]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

verification. The trust framework should be based on a public-key infrastructure with a trust chain from Member States' health authorities or other trusted authorities to the individual entities issuing the COVID-19 certificates. The trust framework should allow for the detection of fraud, in particular forgery. The eHealth Network's Outline Interoperability of Health Certificates Trust Framework of 12 March 2021 adopted pursuant to Article 14 of Directive 2011/24/EU of the European Parliament and of the Council ([8]) should form the basis for the trust framework for the EU Digital COVID Certificate.

(23) Pursuant to this Regulation, the certificates making up the EU Digital COVID Certificate should be issued to the persons referred to in Article 3 of Directive 2004/38/EC, namely Union citizens and their family members, irrespective of their nationality, by the Member State where the vaccination was administered or the test carried out, or where the recovered person is located. Where reference is made to issuance by Member States, this should be understood as also covering issuance by designated bodies on behalf of Member States, including when COVID-19 certificates are issued in overseas countries and territories or the Faroe Islands on behalf of a Member State. Where relevant or appropriate, the certificates should be issued to another person on behalf of the vaccinated, tested or recovered person, for example to the legal guardian on behalf of legally incapacitated persons or to parents on behalf of their children. The certificates should not be subject to legalisation or any other similar formalities.

(24) In accordance with Recommendation (EU) 2020/1475, Member States should pay particular attention to persons living in border regions and travelling across the border on a daily or frequent basis for the purposes of work, business, education, family, medical care or caregiving.

(25) It should be possible for the certificates making up the EU Digital COVID Certificate to be issued to nationals or residents of Andorra, Monaco, San Marino and the Vatican or Holy See.

(26) Agreements on free movement of persons concluded by the Union and the Member States, of the one part, and certain third countries, of the other part, provide for the possibility to restrict free movement on grounds of public health in a non-discriminatory manner. Where such an agreement does not contain a mechanism of incorporation of Union legal acts, COVID-19 certificates issued to beneficiaries of such agreements should be accepted under the conditions laid down in this Regulation. Such acceptance should be conditional on an implementing act to be adopted by the Commission establishing that such a third country issues COVID-19 certificates in accordance with this Regulation and has provided formal assurances that it will accept COVID-19 certificates issued by the Member States.

(27) Regulation (EU) 2021/954 applies to third-country nationals who do not fall within the scope of this Regulation and who stay or reside legally in the territory of a Member State to which that Regulation applies and who are entitled to travel to other Member States in accordance with Union law.

(28) The trust framework to be established for the purpose of this Regulation should seek to ensure consistency with global initiatives, in particular involving the WHO and the International Civil Aviation Organisation. Such consistency should include, where possible, interoperability between technological systems established at global level or by third countries with which the Union has close links and the systems established for the purpose of this Regulation to facilitate the exercise of the right to free movement within the Union, including through the participation in a public key infrastructure or the bilateral exchange of public keys. To facilitate the exercise of the right to free movement by Union citizens and their family members vaccinated or tested in third countries or in the overseas countries or territories referred to in Article 355(2) of the Treaty on the Functioning of the European Union (TFEU) and listed in Annex II thereto or the Faroe Islands, this Regulation should provide for the acceptance of COVID-19 certificates issued by third countries or by overseas countries or territories or the Faroe Islands to Union citizens and their family members where the Commission finds that those COVID-19 certificates are issued in accordance with standards that are to be considered as equivalent to those established pursuant to this Regulation.

([8]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(29) For the purpose of facilitating free movement, and to ensure that restrictions to free movement currently in place during the COVID-19 pandemic can be lifted in a coordinated manner based on the latest scientific evidence and guidance made available by the Health Security Committee established by Article 17 of Decision No 1082/2013/EU of the European Parliament and of the Council ([9]), ECDC and the European Medicines Agency (EMA), an interoperable vaccination certificate should be established. Such a vaccination certificate should serve to confirm that the holder has received a COVID-19 vaccine in a Member State and should contribute to the gradual lifting of restrictions to free movement. The vaccination certificate should contain only the information necessary to clearly identify the holder as well as the COVID-19 vaccine administered, the number of doses, and the date and place of vaccination. Member States should issue vaccination certificates to persons who have received COVID-19 vaccines that have been granted a marketing authorisation pursuant to Regulation (EC) No 726/2004 of the European Parliament and of the Council ([10]), those who have received COVID-19 vaccines that have been granted a marketing authorisation by the competent authority of a Member State pursuant to Directive 2001/83/EC of the European Parliament and of the Council ([11]), and those who have received COVID-19 vaccines the distribution of which has been temporarily authorised pursuant to Article 5(2) of that Directive.

(30) Persons who have been vaccinated before the date of application of this Regulation, including as part of a clinical trial, should also have the right to obtain a vaccination certificate in accordance with this Regulation given that the EU Digital COVID Certificate provides the mutually accepted framework to facilitate the exercise of the right to free movement. Where Union citizens or their family members are not in possession of a vaccination certificate that complies with the requirements of this Regulation, in particular because they have been vaccinated before the date of application of this Regulation, they should be given every reasonable opportunity to prove by other means that they should benefit from the waiving of relevant restrictions to free movement afforded by a Member State to holders of vaccination certificates issued pursuant to this Regulation. This should not be understood as affecting the obligation of Member States to issue vaccination certificates that comply with the requirements of this Regulation nor the right of Union citizens or their family members to receive, from Member States, such vaccination certificates. At the same time, Member States should remain free to issue proof of vaccination in other formats for other purposes, in particular for medical purposes.

(31) Member States may also issue upon request vaccination certificates to persons who have been vaccinated in a third country and who provide all necessary information, including reliable proof to that effect. This is of particular importance to allow the persons concerned to make use of an interoperable and accepted vaccination certificate when exercising their right to free movement within the Union. This should apply in particular to Union citizens and their family members vaccinated in a third country for whom the health system of a Member State allows for the issuance of an EU Digital COVID Certificate and provided that the Member State has been provided with reliable proof of vaccination. A Member State should not be required to issue a vaccination certificate where the COVID-19 vaccine concerned is not authorised for use on its territory. There is no requirement for Member States to issue vaccination certificates at consular posts.

(32) On 12 March 2021, the eHealth Network updated its Guidelines on Verifiable Vaccination Certificates - Basic Interoperability Elements. Those guidelines, in particular the preferred code standards, should form the basis for the technical specifications to be adopted for the purpose of this Regulation.

(33) Before the date of application of this Regulation several Member States already exempted vaccinated persons from certain restrictions to free movement within the Union. Where Member States accept proof of vaccination in order to waive restrictions to free movement put in place, in accordance with Union law to limit the spread of SARS-CoV-2, such as a requirement to undergo quarantine or self-isolation or to be tested for SARS-CoV-2 infection, they should be required to accept, under the same conditions, vaccination certificates issued by other Member States in accordance with this Regulation. Such acceptance should take place under the same conditions, meaning that, for example, where a Member State considers a single dose of a vaccine administered to be sufficient, it should do so

([9]) Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC (OJ L 293, 5.11.2013, p. 1).

([10]) Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Union procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency (OJ L 136, 30.4.2004, p. 1).

([11]) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

also for holders of a vaccination certificate indicating a single dose of the same vaccine. Where Member States lift restrictions to free movement on the basis of proof of vaccination, they should not subject vaccinated persons to additional restrictions to free movement linked to the COVID-19 pandemic, such as travel-related testing for SARS-CoV-2 infection or travel-related quarantine or self-isolation, unless such additional restrictions are, based on the latest available scientific evidence, necessary and proportionate for the purpose of safeguarding public health, and non-discriminatory.

(34) Regulation (EC) No 726/2004 puts in place harmonised procedures, involving all Member States, for the authorisation and surveillance of medicinal products at Union level, ensuring that only high quality medicinal products are placed on the market and administered to persons throughout the Union. As a result, the marketing authorisations granted by the Union pursuant to that Regulation, including the underlying evaluation of the medicinal product concerned in terms of quality, safety and efficacy, are valid in all Member States. In addition, efficacy follow-up and supervision procedures of medicinal products authorised pursuant to that Regulation are carried out centrally for all Member States. The assessment and approval of vaccines via the centralised procedure follow shared standards and are done in a consistent way on behalf of all Member States. Participation of Member States in the review and endorsement of the assessment is ensured through various committees and groups. The assessment also benefits from the expertise of the European medicines regulatory network. The authorisation via the centralised procedure provides the confidence that all Member States can rely on the data on efficacy and safety and on the consistency of the batches being used for vaccination. The obligation to accept, under the same conditions, vaccination certificates issued by other Member States should therefore cover COVID-19 vaccines that have been granted a marketing authorisation pursuant to Regulation (EC) No 726/2004. In order to support the work of WHO and to strive for better global interoperability, Member States are in particular encouraged to accept vaccination certificates issued for other COVID-19 vaccines that have completed the WHO emergency use listing procedure.

(35) Harmonised procedures under Regulation (EC) No 726/2004 should not prevent Member States from deciding to accept vaccination certificates issued for other COVID-19 vaccines that have been granted a marketing authorisation by the competent authority of a Member State pursuant to Directive 2001/83/EC, vaccines the distribution of which has been temporarily authorised pursuant to Article 5(2) of that Directive, and vaccines that have completed the WHO emergency use listing procedure. Where such a COVID-19 vaccine is subsequently granted a marketing authorisation pursuant to Regulation (EC) No 726/2004, the obligation to accept vaccination certificates under the same conditions would also cover vaccination certificates issued by a Member State for that COVID-19 vaccine, regardless of whether the vaccination certificates were issued before or after the authorisation via the centralised procedure.

(36) It is necessary to prevent direct or indirect discrimination against persons who are not vaccinated, for example because of medical reasons, because they are not part of the target group for which the COVID -19 vaccine is currently administered or allowed, such as children, or because they have not yet had the opportunity or chose not to be vaccinated. Therefore, possession of a vaccination certificate, or the possession of a vaccination certificate indicating a COVID-19 vaccine, should not be a pre-condition for the exercise of the right to free movement or for the use of cross-border passenger transport services such as airlines, trains, coaches or ferries or any other means of transport. In addition, this Regulation cannot be interpreted as establishing a right or obligation to be vaccinated.

(37) Many Member States have been requiring persons travelling to their territory to undergo a test for SARS-CoV-2 infection before or after arrival. At the beginning of the COVID-19 pandemic, Member States typically relied on reverse transcription polymerase chain reaction (RT-PCR), which is a nucleic acid amplification (NAAT) test for COVID-19 diagnostics considered by the WHO and the ECDC to be the most reliable methodology for the testing of cases and contacts. As the pandemic has progressed, a new generation of faster and cheaper tests has become available on the Union market, the so-called rapid antigen tests, which detect the presence of viral proteins (antigens) to detect an ongoing SARS-CoV-2 infection. Commission Recommendation (EU) 2020/1743 ([12]) sets out guidance for Member States regarding the use of such rapid antigen tests.

(38) The Council Recommendation of 21 January 2021 ([13]) sets out a common framework for the use and validation of rapid antigen tests and the mutual recognition of COVID-19 test results in the Union and provides for the development of a common list of COVID-19 rapid antigen tests. On the basis of that Recommendation, the Health Security Committee agreed, on 18 February 2021, on a common list of COVID-19 rapid antigen tests, a selection of rapid antigen tests for which Member States will mutually recognise their results and a common standardised set of data to be included in COVID-19 test certificates.

([12]) Commission Recommendation (EU) 2020/1743 of 18 November 2020 on the use of rapid antigen tests for the diagnosis of SARS-CoV-2 infection (OJ L 392, 23.11.2020, p. 63).

([13]) Council Recommendation of 21 January 2021 on a common framework for the use and validation of rapid antigen tests and the mutual recognition of COVID-19 test results in the EU (OJ C 24, 22.1.2021, p. 1).

(39) Despite those common efforts, Union citizens and their family members exercising their right to free movement still face problems when trying to have the test result obtained in one Member State accepted in another. Those problems are often linked to the language in which the test result is issued, or to a lack of trust in the authenticity of the document shown. In that context, the cost of tests also needs to be taken into account. Such problems are aggravated for persons who cannot be vaccinated yet, in particular children, for whom test results may be the only way to travel where restrictions are in place.

(40) To improve the level of acceptance of results of tests carried out in another Member State when presenting such results for the purpose of exercising the right to free movement, an interoperable test certificate should be established, containing the information necessary to clearly identify the holder as well as the type, date and result of the test for SARS-CoV-2 infection. To ensure the reliability of the test result, only the results of NAAT tests and rapid antigen tests featured in the list established on the basis of the Council Recommendation of 21 January 2021 should be eligible for a test certificate issued on the basis of this Regulation. The common standardised set of data to be included in test certificates agreed by the Health Security Committee on the basis of the Council Recommendation of 21 January 2021, in particular the preferred code standards, should form the basis for the technical specifications to be adopted for the purpose of this Regulation.

(41) The use of rapid antigen tests would serve to facilitate the issuance of test certificates on an affordable basis. Universal, timely and affordable access to COVID-19 vaccines and tests for SARS-CoV-2 infection, which form the basis for the issuance of the certificates making up the EU Digital COVID Certificate, is crucial in the fight against the COVID-19 pandemic. Among other things, easy access to inexpensive rapid antigen tests meeting quality criteria can contribute to lower costs, in particular for persons who cross borders on a daily or other frequent basis for work or education, to visit close relatives, to seek medical care, or to take care of loved ones, for other travellers with an essential function or need, for economically disadvantaged persons and for students. On 11 May 2021, the Health Security Committee adopted an updated list of rapid antigen tests, increasing the number of rapid antigen tests recognised as meeting quality criteria to 83. Before the date of application of this Regulation, several Member States already provided large-scale testing possibilities to their populations. To support the testing capacity of Member States, the Commission has mobilised EUR 100 million to purchase over 20 million rapid antigen tests. EUR 35 million were also mobilised through an agreement with Red Cross to increase testing capacity in Member States through mobile testing capacities.

(42) COVID-19 test certificates indicating a negative result issued by Member States in accordance with this Regulation should be accepted, under the same conditions, by Member States requiring proof of a test for SARS-CoV-2 infection in order to waive the restrictions to free movement put in place to limit the spread of SARS-CoV-2. Where the epidemiological situation allows, holders of test certificates indicating a negative result should not be subject to additional restrictions to free movement linked to the COVID-19 pandemic, such as additional travel-related testing for SARS-CoV-2 infection upon arrival or travel-related quarantine or self-isolation, unless such additional restrictions are, based on the latest available scientific evidence, necessary and proportionate for the purpose of safeguarding public health, and non-discriminatory.

(43) According to existing scientific evidence, it is possible for persons who have recovered from COVID-19 to continue to test positive for SARS-CoV-2 for a certain period after the onset of symptoms. Where such persons are required to undergo a test prior to exercising their right to free movement, they could therefore be effectively prevented from travelling despite no longer being infectious. For the purpose of facilitating free movement, and to ensure that restrictions to free movement currently in place during the COVID-19 pandemic can be lifted in a coordinated manner based on the latest scientific evidence available, an interoperable certificate of recovery should be established, containing the information necessary to clearly identify the person concerned and the date of a previous positive test result for SARS-CoV-2 infection. A certificate of recovery should be issued at the earliest 11 days after the date on which the person was first subject to a NAAT test which produced a positive result and should be valid for not more than 180 days. According to the ECDC, recent evidence shows that despite shedding of viable SARS-CoV-2 between ten and twenty days from the onset of symptoms, convincing epidemiological studies have failed to show onward SARS-CoV-2 transmission after ten days. The Commission should be empowered to change that period on the basis of guidance from the Health Security Committee or from ECDC, which is closely studying the evidence base for the duration of acquired immunity after recovery.

(44) Before the date of application of this Regulation, several Member States already exempted recovered persons from certain restrictions to free movement within the Union. Where Member States accept proof of recovery in order to waive restrictions to free movement put in place, in accordance with Union law, to limit the spread of SARS-CoV-2, such as a requirement to undergo quarantine or self-isolation or to be tested for SARS-CoV-2 infection, they should be required to accept, under the same conditions, certificates of recovery from COVID-19 issued by other Member States in accordance with this Regulation. On 15 March 2021, the eHealth Network, in cooperation with Health Security Committee, issued guidelines on COVID-19 citizen recovery interoperable certificates - minimum dataset. Where Member States lift restrictions to free movement on the basis of a certificate of recovery, they should not subject the recovered persons to additional restrictions to free movement linked to the COVID-19 pandemic, such as travel-related testing for SARS-CoV-2 infection or travel-related quarantine or self-isolation, unless such additional restrictions are, based on the latest available scientific evidence, necessary and proportionate for the purpose of safeguarding public health, and non-discriminatory.

(45) To be able to obtain a common position quickly, the Commission should be able to ask the Health Security Committee, the ECDC or EMA to issue guidance on the available scientific evidence on the effects of medical events documented in the certificates established in accordance with this Regulation, including the effectiveness and duration of the immunity conferred by COVID-19 vaccines, whether vaccines prevent asymptomatic infection and SARS-CoV-2 transmission, the situation of people having recovered from COVID-19, and the impacts of the new SARS-CoV-2 variants on people who have been vaccinated or already infected.

(46) In order to ensure uniform conditions for the implementation of the trust framework established by this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([14]).

(47) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating, in particular to the need to ensure a timely implementation of the trust framework, imperative grounds of urgency so require or when new scientific evidence becomes available.

(48) Regulation (EU) 2016/679 of the European Parliament and of the Council ([15]) applies to the processing of personal data carried out when implementing this Regulation. This Regulation establishes the legal ground for the processing of personal data within the meaning of point (c) of Article 6(1) and point (g) of Article 9(2) of Regulation (EU) 2016/679, necessary for the issuance and verification of the interoperable certificates provided for in this Regulation. It does not regulate the processing of personal data related to the documentation of a vaccination, a test or a recovery event for other purposes, such as for the purposes of pharmacovigilance or for the maintenance of individual personal health records. Member States may process personal data for other purposes, if the legal basis for the processing of such data for other purposes, including the related retention periods, is provided for in national law, which must comply with Union data protection law and the principles of effectiveness, necessity and proportionality, and should contain provisions clearly identifying the scope and extent of the processing, the specific purpose involved, the categories of entity that can verify the certificate as well as the relevant safeguards to prevent discrimination and abuse, taking into account the risks to the rights and freedoms of data subjects. Where the certificate is used for non-medical purposes, personal data accessed during the verification process are not to be retained, as provided for in this Regulation.

(49) Where a Member State has adopted or adopts, on the basis of national law, a system of COVID-19 certificates for domestic purposes, it should ensure for the period of application of this Regulation that certificates making up the EU Digital COVID Certificate can also be used and are also accepted for domestic purposes, in order to avoid that persons travelling to another Member State and using the EU Digital COVID Certificate are obliged to obtain an additional national COVID-19 certificate.

(50) In line with the principle of data minimisation, COVID-19 certificates should contain only the personal data strictly necessary for the purpose of facilitating the exercise of the right to free movement within the Union during the COVID-19 pandemic. The specific categories of personal data and data fields to be included in the COVID-19 certificates should be set out in this Regulation.

([14]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

([15]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (OJ L 119, 4.5.2016, p. 1).

(51) For the purposes of this Regulation, personal data on individual certificates do not need to be transmitted or exchanged across borders. In line with the public-key infrastructure approach, only the public keys of the issuers need to be transferred or accessed across borders, which will be ensured by an interoperability gateway set up and maintained by the Commission. In particular, the presence of the certificate combined with the public key of the issuer should allow for the verification of the authenticity, validity and integrity of the certificate. To prevent and detect fraud, Member States should be able to exchange lists of revoked certificates. In line with the principle of data protection by default, verification techniques not requiring transmission of personal data on individual certificates should be employed.

(52) The retention of personal data obtained from the certificate by the Member State of destination or transit or by the cross-border passenger transport services operators required by national law to implement certain public health measures during the COVID-19 pandemic should be prohibited. This Regulation does not provide a legal basis for setting up or maintaining a centralised database at Union level containing personal data.

(53) In accordance with Regulation (EU) 2016/679, the data controllers and processors of personal data are to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing.

(54) The authorities or other designated bodies responsible for issuing the certificates making up the EU Digital COVID Certificate, as controllers within the meaning of Regulation (EU) 2016/679, are accountable for how they process personal data falling within the scope of this Regulation. This includes ensuring a level of security appropriate to the risks, including by establishing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The powers of the supervisory authorities established under Regulation (EU) 2016/679 apply in full, in order to protect natural persons in relation to the processing of their personal data.

(55) To ensure coordination, the Commission and the other Member States should be informed when a Member State requires holders of certificates to undergo, after entry into its territory, quarantine or self-isolation or to be tested for SARS-CoV-2 infection, or if it imposes other restrictions on holders of such certificates.

(56) Clear, comprehensive and timely communication to the public, including holders, on the purpose, issuance and acceptance of each type of the certificates making up the EU Digital COVID Certificate is crucial to ensure predictability for travel and legal certainty. The Commission should support the efforts of Member States in this regard, for example by making available the information provided by Member States on the 'Re-open EU' web platform.

(57) A phasing-in period should be provided for, to give Member States which are unable to issue certificates in the format that complies with this Regulation from its date of application the possibility to continue issuing COVID-19 certificates which are not yet in compliance with this Regulation. During the phasing-in period, such COVID-19 certificates and COVID-19 certificates issued before the date of application of this Regulation should be accepted by Member States provided that they contain the necessary data.

(58) In accordance with Recommendation (EU) 2020/1475, any restrictions to the free movement of persons within the Union put in place to limit the spread of SARS-CoV-2 should be lifted as soon as the epidemiological situation allows. This also applies to requirements to present documents other than those required by Union law, in particular Directive 2004/38/EC, such as the certificates covered by this Regulation. This Regulation should apply for 12 months from its date of application. By four months after the date of application of this Regulation, the Commission should submit a report to the European Parliament and to the Council. At the latest three months before the end of the period of application of this Regulation, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic, the Commission should submit a second report to the European Parliament and the Council, on the lessons learned from the application of this Regulation, including on its impact on the facilitation of free movement and on data protection.

(59) In order to take into account the scientific progress in containing the COVID-19 pandemic, or to ensure interoperability with international standards, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend this Regulation by modifying or removing the data fields to be included in the EU Digital COVID Certificate regarding the identity of the holder, information about the COVID-19 vaccine, the test for SARS-CoV-2 infection, past SARS-CoV-2 infection and the certificate metadata, by adding data fields regarding information about the COVID-19 vaccine, the test for SARS-CoV-2 infection, past SARS-CoV-2 infection and certificate metadata and by amending the number of days after which a certificate of recovery is to be issued. In order to take into account guidance received, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the provisions of this Regulation with regard to the certificate of recovery by providing for its issuance on the basis of a positive rapid antigen test, antibody test, including serological testing for antibodies against SARS-CoV-2, or any other scientifically reliable method. Such delegated acts should include the necessary data fields on the categories of data laid down by this Regulation to be included in the certificate of recovery. They should also contain specific provisions on the maximum validity period, which may depend on the type of the test carried out. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([16]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(60) In accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council ([17]), the Commission is to consult the European Data Protection Supervisor when preparing delegated acts or implementing acts that impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. The Commission may also consult the European Data Protection Board where such acts are of particular importance for the protection of rights and freedoms of individuals with regard to the processing of personal data.

(61) Since the objective of this Regulation, namely to facilitate the exercise of the right to free movement within the Union during the COVID-19 pandemic by establishing a framework for the issuance, verification and acceptance of interoperable COVID-19 certificates on a person's COVID-19 vaccination, test result or recovery, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(62) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union (the 'Charter'), including the right to respect for private and family life, the right to the protection of personal data, the right to equality before the law and non-discrimination, the freedom of movement and the right to an effective remedy. Member States are to comply with the Charter when implementing this Regulation.

(63) Given the urgency of the situation related to the COVID-19 pandemic, this Regulation should enter into force on the day of its publication in the *Official Journal of the European Union*.

(64) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered a joint opinion on 31 March 2021 ([18]),

([16]) OJ L 123, 12.5.2016, p. 1.
([17]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).
([18]) Not yet published in the Official Journal.

HAVE ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation lays down a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) for the purpose of facilitating the holders' exercise of their right to free movement during the COVID-19 pandemic. This Regulation shall also contribute to facilitating the gradual lifting of restrictions to free movement put in place by the Member States, in accordance with Union law, to limit the spread of SARS-CoV-2, in a coordinated manner.

It provides for the legal ground to process the personal data necessary to issue such certificates and to process the information necessary to verify and confirm the authenticity and validity of such certificates in full compliance with Regulation (EU) 2016/679.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'holder' means a person to whom an interoperable certificate containing information about that person's COVID-19 vaccination, test result or recovery has been issued in accordance with this Regulation;

(2) 'EU Digital COVID Certificate' means interoperable certificates containing information about the vaccination, test result or recovery of the holder issued in the context of the COVID-19 pandemic;

(3) 'COVID-19 vaccine' means an immunological medicinal product indicated for active immunisation to prevent COVID-19 caused by SARS-CoV-2;

(4) 'NAAT test' means a molecular nucleic acid amplification test, such as reverse transcription polymerase chain reaction (RT-PCR), loop-mediated isothermal amplification (LAMP) and transcription-mediated amplification (TMA) techniques, used to detect the presence of the SARS-CoV-2 ribonucleic acid (RNA);

(5) 'rapid antigen test' means a test that relies on detection of viral proteins (antigens) using a lateral flow immunoassay that gives results in less than 30 minutes;

(6) 'antibody test' means a laboratory-based test aiming to detect if a person has developed antibodies against SARS-CoV-2, thus indicating that the holder has been exposed to SARS-CoV-2 and has developed antibodies, regardless of whether that person was symptomatic;

(7) 'interoperability' means the capability of verifying systems in a Member State to use data encoded by another Member State;

(8) 'barcode' means a method of storing and representing data in a visual, machine-readable format;

(9) 'electronic seal' means electronic seal as defined in point (25) of Article 3 of Regulation (EU) No 910/2014;

(10) 'unique certificate identifier' means a unique identifier given, in accordance with a common structure, to each certificate issued in accordance with this Regulation;

(11) 'trust framework' means the rules, policies, specifications, protocols, data formats and digital infrastructure regulating and allowing for the reliable and secure issuance and verification of certificates to ensure their trustworthiness by confirming their authenticity, validity and integrity, through the use of electronic seals.

Article 3

EU Digital COVID Certificate

1. The EU Digital COVID Certificate framework shall allow for the issuance, cross-border verification and acceptance of any of the following certificates:

(a) a certificate confirming that the holder has received a COVID-19 vaccine in the Member State issuing the certificate (vaccination certificate);

(b) a certificate confirming that the holder has been subject to a NAAT test or a rapid antigen test listed in the common and updated list of COVID-19 rapid antigen tests established on the basis of the Council Recommendation of 21 January 2021 carried out by health professionals or by skilled testing personnel in the Member State issuing the certificate and indicating the type of test, the date on which it was carried out and the result of the test (test certificate);

(c) a certificate confirming that, following a positive result of a NAAT test carried out by health professionals or by skilled testing personnel the holder has recovered from a SARS-CoV-2 infection (certificate of recovery).

The Commission shall publish the list of COVID-19 rapid antigen tests established on the basis of the Council Recommendation of 21 January 2021, including any updates.

2. Member States, or designated bodies acting on behalf of Member States, shall issue the certificates referred to in paragraph 1 of this Article in a digital or paper-based format, or both. The prospective holders shall be entitled to receive the certificates in the format of their choice. Those certificates shall be user-friendly and shall contain an interoperable barcode allowing for the verification of their authenticity, validity and integrity. The barcode shall comply with the technical specifications established pursuant to Article 9. The information contained in the certificates shall also be shown in human-readable form and shall be provided in at least the official language or languages of the issuing Member State and English.

3. A separate certificate shall be issued for each vaccination, test result or recovery. Such a certificate shall not contain data from previous certificates except where otherwise provided for in this Regulation.

4. The certificates referred to in paragraph 1 shall be issued free of charge. The holder shall be entitled to request the issuance of a new certificate if the personal data contained in the original certificate are not or are no longer accurate or up to date, including with regard to the vaccination, test result or recovery of the holder, or if the original certificate is no longer available to the holder. Appropriate fees may be charged for the issuance of a new certificate in cases of repeated loss.

5. The certificates referred to in paragraph 1 shall include the following text:

'This certificate is not a travel document. The scientific evidence on COVID-19 vaccination, testing and recovery continues to evolve, including with regard to new virus variants of concern. Before travelling, please check the applicable public health measures and related restrictions applicable at the point of destination.'

Member States shall provide the holder with clear, comprehensive and timely information on the issuance and purpose of vaccination certificates, test certificates, or certificates of recovery for the purposes of this Regulation.

6. Possession of the certificates referred to in paragraph 1 shall not be a precondition for exercising the right to free movement.

7. The issuance of certificates pursuant to paragraph 1 of this Article shall not lead to discrimination on the basis of the possession of a specific category of certificate as referred to in Article 5, 6 or 7.

8. Issuance of the certificates referred to in paragraph 1 shall not affect the validity of any other proof of vaccination, test result or recovery issued before 1 July 2021 or for other purposes, in particular for medical purposes.

9. Cross-border passenger transport service operators required by national law to implement certain public health measures during the COVID-19 pandemic shall ensure that the verification of the certificates referred in paragraph 1 is integrated into the operation of cross-border transport infrastructure such as airports, ports and railway and bus stations, where appropriate.

10. The Commission may adopt implementing acts establishing that COVID-19 certificates issued by a third country with which the Union and the Member States have concluded an agreement on the free movement of persons allowing the contracting parties to restrict such free movement on grounds of public health in a non-discriminatory manner and which does not contain a mechanism of incorporation of Union legal acts are equivalent to those issued in accordance with this Regulation. Where the Commission adopts such implementing acts, the certificates concerned shall be accepted under the conditions referred to in Article 5(5), Article 6(5) and Article 7(8).

Before adopting such implementing acts, the Commission shall assess whether such a third country issues certificates equivalent to those issued in accordance with this Regulation and has provided formal assurances that it will accept certificates issued by the Member States.

The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 14(2).

11. Where necessary, the Commission shall ask the Health Security Committee, the ECDC or EMA to issue guidance on the available scientific evidence on the effects of medical events documented in the certificates referred to in paragraph 1, in particular with regard to new SARS-CoV-2 variants of concern.

Article 4

Trust framework for the EU Digital COVID Certificate

1. The Commission and the Member States shall set up and maintain a trust framework for the EU Digital COVID Certificate.

2. The trust framework shall be based on a public key infrastructure and allow for the reliable and secure issuance and verification of the authenticity, validity and integrity of the certificates referred to in Article 3(1). The trust framework shall allow for the detection of fraud, in particular forgery. In addition, it may support the bilateral exchange of certificate revocation lists containing the unique certificate identifiers of revoked certificates. Such certificate revocation lists shall not contain any other personal data. The verification of the certificates referred to in Article 3(1) and, where applicable, certificate revocation lists shall not give rise to the issuer being notified of the verification.

3. The trust framework shall seek to ensure interoperability with technological systems established at international level.

Article 5

Vaccination certificate

1. Each Member State shall, automatically or upon request by the persons concerned, issue the vaccination certificates referred to in point (a) of Article 3(1) to persons to whom a COVID-19 vaccine has been administered. Those persons shall be informed of their right to a vaccination certificate.

2. The vaccination certificate shall contain the following categories of personal data:

(a) the identity of the holder;

(b) information about the COVID-19 vaccine and the number of doses administered to the holder;

(c) certificate metadata, such as the certificate issuer or a unique certificate identifier.

The personal data shall be included in the vaccination certificate in accordance with the specific data fields set out in point 1 of the Annex.

The Commission is empowered to adopt delegated acts in accordance with Article 12 to amend point 1 of the Annex by modifying or removing data fields, or by adding data fields falling under the categories of personal data referred to in points (b) and (c) of the first subparagraph of this paragraph, where such an amendment is necessary to verify and confirm the authenticity, validity and integrity of the vaccination certificate, in the case of scientific progress in containing the COVID-19 pandemic, or to ensure interoperability with international standards.

3. The vaccination certificate shall be issued in a secure and interoperable format in accordance with Article 3(2) after the administration of each dose and shall clearly indicate whether or not the vaccination course has been completed.

4. Where, in the case of newly emerging scientific evidence or to ensure interoperability with international standards and technological systems, imperative grounds of urgency so require, the procedure provided for in Article 13 shall apply to delegated acts adopted pursuant to this Article.

5. Where Member States accept proof of vaccination in order to waive restrictions to free movement put in place, in accordance with Union law, to limit the spread of SARS-CoV-2, they shall also accept, under the same conditions, vaccination certificates issued by other Member States in accordance with this Regulation for a COVID-19 vaccine that has been granted a marketing authorisation pursuant to Regulation (EC) No 726/2004.

Member States may also accept, for the same purpose, vaccination certificates issued by other Member States in accordance with this Regulation for a COVID-19 vaccine that has been granted a marketing authorisation by the competent authority of a Member State pursuant to Directive 2001/83/EC, a COVID-19 vaccine the distribution of which has been temporarily authorised pursuant to Article 5(2) of that Directive, or a COVID-19 vaccine that has completed the WHO emergency use listing procedure.

Where Member States accept vaccination certificates for a COVID-19 vaccine referred to in the second subparagraph, they shall also accept, under the same conditions, vaccination certificates issued by other Member States in accordance with this Regulation for the same COVID-19 vaccine.

Article 6

Test certificate

1. Each Member State shall, automatically or upon request by the persons concerned, issue the test certificates referred to in point (b) of Article 3(1) to persons tested for SARS-CoV-2 infection. Those persons shall be informed of their right to a test certificate.

2. The test certificate shall contain the following categories of personal data:

(a) the identity of the holder;

(b) information about the NAAT test or rapid antigen test to which the holder was subject;

(c) certificate metadata, such as the certificate issuer or a unique certificate identifier.

The personal data shall be included in the test certificate in accordance with the specific data fields set out in point 2 of the Annex.

The Commission is empowered to adopt delegated acts in accordance with Article 12 to amend point 2 of the Annex by modifying or removing data fields, or by adding data fields falling under the categories of personal data referred to in points (b) and (c) of the first subparagraph of this paragraph, where such an amendment is necessary to verify and confirm the authenticity, validity and integrity of the test certificate, in the case of scientific progress in containing the COVID-19 pandemic, or to ensure interoperability with international standards.

3. The test certificate shall be issued in a secure and interoperable format in accordance with Article 3(2).

4. Where, in the case of newly emerging scientific evidence or to ensure interoperability with international standards and technological systems, imperative grounds of urgency so require, the procedure provided for in Article 13 shall apply to delegated acts adopted pursuant to this Article.

5. Where Member States require proof of a test for SARS-CoV-2 infection in order to waive the restrictions to free movement put in place, in accordance with Union law and taking into account the specific situation of cross-border communities, to limit the spread of SARS-CoV-2, they shall also accept, under the same conditions, test certificates indicating a negative result issued by other Member States in accordance with this Regulation.

Article 7

Certificate of recovery

1. Each Member State shall issue, upon request, the certificates of recovery referred to in point (c) of Article 3(1).

Certificates of recovery shall be issued at the earliest 11 days after the date on which a person was first subject to a NAAT test which produced a positive result.

The Commission is empowered to adopt delegated acts in accordance with Article 12 to amend the number of days after which a certificate of recovery is to be issued, on the basis of guidance received from the Health Security Committee in accordance with Article 3(11) or on scientific evidence reviewed by ECDC.

2. The certificate of recovery shall contain the following categories of personal data:

(a) the identity of the holder;

(b) information about past SARS-CoV-2 infection of the holder following a positive test result;

(c) certificate metadata, such as the certificate issuer or a unique certificate identifier.

The personal data shall be included in the certificate of recovery in accordance with the specific data fields set out in point 3 of the Annex.

The Commission is empowered to adopt delegated acts in accordance with Article 12 to amend point 3 of the Annex by modifying or removing data fields, or by adding data fields falling under categories of personal data referred to in points (b) and (c) of the first subparagraph of this paragraph, where such an amendment is necessary to verify and confirm the authenticity, validity and integrity of the certificate of recovery, in the case of scientific progress in containing the COVID-19 pandemic, or to ensure interoperability with international standards.

3. The certificate of recovery shall be issued in a secure and interoperable format in accordance with Article 3(2).

4. On the basis of guidance received pursuant to Article 3(11), the Commission is empowered to adopt delegated acts in accordance with Article 12 to amend paragraph 1 of this Article and point (c) of Article 3(1) to allow for the issuance of the certificate of recovery on the basis of a positive rapid antigen test, antibody test, including a serological test for antibodies against SARS-CoV-2, or any other scientifically validated method. Such delegated acts shall also amend point 3 of the Annex by adding, modifying or removing the data fields falling under the categories of personal data referred to in points (b) and (c) of paragraph 2 of this Article.

5. Following the adoption of the delegated acts referred to in paragraph 4 the Commission shall publish the list of antibody tests on the basis of which a certificate of recovery may be issued, which is to be established by the Health Security Committee, including any updates.

6. In the report provided for in Article 16(1), the Commission shall assess the appropriateness and feasibility, in light of the available scientific evidence, of adopting the delegated acts referred to in paragraph 4 of this Article. Before submitting that report, the Commission shall seek regular guidance pursuant to Article 3(11) on the available scientific evidence and level of standardisation regarding the possible issuance of certificates of recovery based on antibody tests, including serological testing for antibodies against SARS-CoV-2,, taking into account the availability and accessibility of such tests.

7. Where, in the case of newly emerging scientific evidence or to ensure interoperability with international standards and technological systems, imperative grounds of urgency so require, the procedure provided for in Article 13 shall apply to delegated acts adopted pursuant to this Article.

8. Where Member States accept proof of recovery from SARS-CoV-2 infection in order to waive restrictions to free movement put in place, in accordance with Union law, to limit the spread of SARS-CoV-2, they shall accept, under the same conditions, certificates of recovery issued by other Member States in accordance with this Regulation.

Article 8

COVID-19 certificates and other documentation issued by a third country

1. Where a vaccination certificate has been issued in a third country for a COVID-19 vaccine that corresponds to one of the COVID-19 vaccines referred to Article 5(5) and the authorities of a Member State have been provided with all the necessary information, including reliable proof of vaccination, those authorities may, upon request, issue a vaccination certificate as referred to in point (a) of Article 3(1) to the person concerned. A Member State shall not be required to issue a vaccination certificate for a COVID-19 vaccine that is not authorised for use on its territory.

2. The Commission may adopt an implementing act establishing that COVID-19 certificates issued by a third country in accordance with standards and technological systems that are interoperable with the trust framework for the EU Digital COVID Certificate and that allow for the verification of the authenticity, validity and integrity of the certificate, and which contain the data set out in the Annex, are to be considered as equivalent to certificates issued by Member States in accordance with this Regulation, for the purpose of facilitating the holders' exercise of their right to free movement within the Union.

Before adopting such an implementing act, the Commission shall assess whether COVID-19 certificates issued by the third country fulfil the conditions set out in the first subparagraph.

The implementing act referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 14(2).

The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

3. The acceptance by the Member States of the certificates referred to in this Article shall be subject to Article 5(5), Article 6(5) and Article 7(8).

4. Where Member States accept vaccination certificates issued by a third country for a COVID-19 vaccine as referred to in the second subparagraph of Article 5(5), they shall also accept, under the same conditions, vaccination certificates issued by other Member States in accordance with this Regulation for the same COVID-19 vaccine.

5. This Article shall apply to COVID-19 certificates and other documentation issued by the overseas countries and territories referred to in Article 355(2) TFEU and listed in Annex II thereto, and by the Faroe Islands. It shall not apply to COVID-19 certificates and other documentation issued in the overseas countries and territories referred to in Article 355(2) TFEU and listed in Annex II thereto, or in the Faroe Islands on behalf of a Member State.

Article 9

Technical specifications

1. In order to ensure uniform conditions for the implementation of the trust framework established by this Regulation, the Commission shall adopt implementing acts containing the technical specifications and rules for the purpose of:

(a) securely issuing and verifying the certificates referred to Article 3(1);

(b) ensuring the security of personal data, taking into account the nature of the data;

(c) populating the certificates referred to Article 3(1), including the coding system and any other relevant elements;

(d) laying down the common structure of the unique certificate identifier;

(e) issuing a valid, secure and interoperable barcode;

(f) seeking to ensure interoperability with international standards and technological systems;

(g) allocating responsibilities among controllers and as regards processors, in accordance with Chapter IV of Regulation (EU) 2016/679.

(h) ensuring accessibility for persons with disabilities to the human-readable information contained in the digital certificate and in the paper-based certificate in accordance with the accessibility requirements under Union law.

2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 14(2).

3. On duly justified imperative grounds of urgency, in particular to ensure a timely implementation of the trust framework, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 14(3). Implementing acts adopted pursuant to this paragraph shall remain in force for the period of the application of this Regulation.

Article 10

Protection of personal data

1. Regulation (EU) 2016/679 shall apply to the processing of personal data carried out when implementing this Regulation.

2. For the purpose of this Regulation, the personal data contained in the certificates issued pursuant to this Regulation shall be processed only for the purpose of accessing and verifying the information included in the certificate in order to facilitate the exercise of the right of free movement within the Union during the COVID-19 pandemic. After the end of period of the application of this Regulation, no further processing shall occur.

3. The personal data included in the certificates referred to in Article 3(1) shall be processed by the competent authorities of the Member State of destination or transit, or by the cross-border passenger transport services operators required by national law to implement certain public health measures during the COVID-19 pandemic, only to verify and confirm the holder's vaccination, test result or recovery. To that end, the personal data shall be limited to what is strictly necessary. The personal data accessed pursuant to this paragraph shall not be retained.

4. The personal data processed for the purpose of issuing the certificates referred to in Article 3(1), including the issuance of a new certificate, shall not be retained by the issuer longer than is strictly necessary for its purpose and in no case longer than the period for which the certificates may be used to exercise the right to free movement.

5. Any certificate revocation lists exchanged between Member States pursuant to Article 4(2) shall not be retained after the end of period of the application of this Regulation.

6. The authorities or other designated bodies responsible for issuing the certificates referred to in Article 3(1) shall be considered to be controllers as defined in point (7) of Article 4 of Regulation (EU) 2016/679.

7. The natural or legal person, public authority, agency or other body that has administered a COVID-19 vaccine or carried out the test for which a certificate is to be issued shall transmit to the authorities or other designated bodies responsible for issuing the certificates the personal data necessary to complete the data fields set out in the Annex.

8. Where a controller as referred to in paragraph 6 uses a processor for the purposes referred to in Article 28(3) of Regulation (EU) 2016/679, no transfer of personal data by the processor to a third country shall take place.

Article 11

Restrictions to free movement and information exchange

1. Without prejudice to Member States' competence to impose restrictions on grounds of public health, where Member States accept vaccination certificates, test certificates indicating a negative result or certificates of recovery, they shall refrain from imposing additional restrictions to free movement, such as additional travel-related testing for SARS-

CoV-2 infection or travel-related quarantine or self-isolation, unless they are necessary and proportionate for the purpose of safeguarding public health in response to the COVID-19 pandemic, also taking into account available scientific evidence, including epidemiological data published by the ECDC on the basis of Recommendation (EU) 2020/1475.

2. Where a Member State requires, in accordance with Union law, holders of the certificates referred to in Article 3(1) to undergo, after entry into its territory, quarantine or self-isolation or to be tested for SARS-CoV-2 infection, or if it imposes other restrictions on the holders of such certificates because, for example, the epidemiological situation in a Member State or in a region within a Member State worsens quickly, in particular as a result of a SARS-CoV-2 variant of concern or interest, it shall inform the Commission and the other Member States accordingly, if possible 48 hours in advance of the introduction of such new restrictions. To that end, the Member State shall provide the following information:

(a) the reasons for such restrictions;

(b) the scope of such restrictions, specifying which certificate holders are subject to or exempt from such restrictions;

(c) the date and duration of such restrictions.

3. Member States shall inform the Commission and the other Member States of the issuance and the conditions of acceptance of the certificates referred to in Article 3(1), including the COVID-19 vaccines they accept pursuant to the second subparagraph of Article 5(5).

4. Member States shall provide the public with clear, comprehensive and timely information with regard to paragraphs 2 and 3. As a general rule, Member States shall make that information publicly available 24 hours before new restrictions come into effect, taking into account that some flexibility is required for epidemiological emergencies. In addition, the information provided by the Member States may be made publicly available by the Commission in a centralised manner.

Article 12

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 5(2), Article 6(2) and Article 7(1) and (2) shall be conferred on the Commission for a period of 12 months from 1 July 2021.

3. The delegation of power referred to in Article 5(2), Article 6(2) and Article 7(1) and (2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 5(2), Article 6(2) or Article 7(1) or (2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 13

Urgency procedure

1. Delegated acts adopted under this Article shall enter into force without delay and shall apply as long as no objection is expressed in accordance with paragraph 2. The notification of a delegated act to the European Parliament and to the Council shall state the reasons for the use of the urgency procedure.

2. Either the European Parliament or the Council may object to a delegated act in accordance with the procedure referred to in Article 11(6). In such a case, the Commission shall repeal the act immediately following the notification of the decision to object by the European Parliament or by the Council.

Article 14

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

Article 15

Phasing-in period

1. COVID-19 certificates issued by a Member State before 1 July 2021 shall be accepted by the other Member States until 12 August 2021 in accordance with Article 5(5), Article 6(5) and Article 7(8), where they contain the data set out in the Annex.

2. Where a Member State is not able to issue the certificates referred to in Article 3(1) in a format that complies with this Regulation from 1 July 2021, it shall inform the Commission and the other Member States accordingly. Where they contain the data set out in the Annex, the COVID-19 certificates issued by such a Member State in a format that does not comply with this Regulation shall be accepted by the other Member States in accordance with Article 5(5), Article 6(5) and Article 7(8) until 12 August 2021.

Article 16

Commission reports

1. By 31 October 2021, the Commission shall submit a report to the European Parliament and to the Council. The report shall include an overview of:

(a) the number of certificates issued pursuant to this Regulation;

(b) guidance requested pursuant to Article 3(11) on the available scientific evidence and level of standardisation regarding the possible issuance of certificates of recovery based on antibody tests, including serological testing for antibodies against SARS-CoV-2, taking into account the availability and accessibility of such tests; and

(c) the information received pursuant to Article 11.

2. By 31 March 2022, the Commission shall submit a report to the European Parliament and to the Council on the application of this Regulation.

The report shall contain, in particular, an assessment of the impact of this Regulation on the facilitation of free movement, including on travel and tourism and the acceptance of the different types of vaccine, fundamental rights and non-discrimination, as well as on the protection of personal data during the COVID-19 pandemic.

The report may be accompanied by legislative proposals, in particular to extend the period of application of this Regulation, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic.

Article 17

Entry into force

This Regulation shall enter into force on the day of its publication in the *Official Journal of the European Union*.

It shall apply from 1 July 2021 to 30 June 2022.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 14 June 2021.

For the European Parliament	*For the Council*
The President	*The President*
D. M. SASSOLI	A. COSTA

ANNEX

CERTIFICATE DATASETS

1. Data fields to be included in the vaccination certificate:
   (a) name: surname(s) and forename(s), in that order;
   (b) date of birth;
   (c) disease or agent targeted: COVID-19 (SARS-CoV-2 or one of its variants);
   (d) COVID-19 vaccine or prophylaxis;
   (e) COVID-19 vaccine product name;
   (f) COVID-19 vaccine marketing authorisation holder or manufacturer;
   (g) number in a series of doses as well as the overall number of doses in the series;
   (h) date of vaccination, indicating the date of the latest dose received;
   (i) Member State or third country in which the vaccine was administered;
   (j) certificate issuer;
   (k) unique certificate identifier.
2. Data fields to be included in the test certificate:
   (a) name: surname(s) and forename(s), in that order;
   (b) date of birth;
   (c) disease or agent targeted: COVID-19 (SARS-CoV-2 or one of its variants);
   (d) the type of test;
   (e) test name (optional for NAAT test);
   (f) test manufacturer (optional for NAAT test);
   (g) date and time of the test sample collection;
   (h) result of the test;
   (i) testing centre or facility (optional for rapid antigen test);
   (j) Member State or third country in which the test was carried out;
   (k) certificate issuer;
   (l) unique certificate identifier.
3. Data fields to be included in the certificate of recovery:
   (a) name: surname(s) and forename(s), in that order;
   (b) date of birth;
   (c) disease or agent from which the holder has recovered: COVID-19 (SARS-CoV-2 or one of its variants);
   (d) date of the holder's first positive NAAT test result;
   (e) Member State or third country in which test was carried out;
   (f) certificate issuer;
   (g) certificate valid from;
   (h) certificate valid until (not more than 180 days after the date of first positive NAAT test result);
   (i) unique certificate identifier.

REGULATION (EU) 2021/954 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 June 2021

on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 77(2)(c) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure ([1]),

Whereas:

(1) Under the Schengen *acquis*, third-country nationals legally staying or residing in the territories of Member States may move freely within the territories of all other Member States during a period of 90 days in any 180-day period.

(2) On 30 January 2020, the Director-General of the World Health Organization (WHO) declared a public health emergency of international concern over the global outbreak of severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), which causes coronavirus disease 2019 (COVID-19). On 11 March 2020, the WHO made an assessment characterising COVID-19 as a pandemic.

(3) To limit the spread of SARS-CoV-2, the Member States have adopted some measures which have had an impact on travel to and within the territory of the Member States, such as entry restrictions or requirements for cross-border travellers to undergo quarantine or self-isolation or to be tested for SARS-CoV-2 infection. Such restrictions have detrimental effects on persons and businesses, especially persons living in border regions and travelling across the border on a daily or frequent basis for the purposes of work, business, education, family, medical care or caregiving.

(4) On 13 October 2020, the Council adopted Recommendation (EU) 2020/1475 ([2]) which introduced a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic.

(5) On 30 October 2020, the Council adopted Recommendation (EU) 2020/1632 ([3]) in which it recommended Member States that are bound by the Schengen *acquis* to apply the general principles, common criteria, common thresholds and common framework of measures, including recommendations on coordination and communication as laid down in Recommendation (EU) 2020/1475.

(6) Many Member States have launched or plan to launch initiatives to issue COVID-19 vaccination certificates. However, for such vaccination certificates to be used effectively in connection with cross-border travel within the Union, they need to be fully interoperable, compatible, secure and verifiable. A common approach is required among Member States on the content, format, principles, technical standards and the level of security of such vaccination certificates.

([1]) Position of the European Parliament of 9 June 2021 (not yet published in the Official Journal) and decision of the Council of 11 June 2021.
([2]) Council Recommendation (EU) 2020/1475 of 13 October 2020 on a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic (OJ L 337, 14.10.2020, p. 3).
([3]) Council Recommendation (EU) 2020/1632 of 30 October 2020 on a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic in the Schengen area (OJ L 366, 4.11.2020, p. 25).

(7) Before the date of application of this Regulation several Member States already exempted vaccinated persons from certain travel restrictions. Where Member States accept proof of vaccination in order to waive travel restrictions put in place, in accordance with Union law to limit the spread of SARS-CoV-2, such as a requirement to undergo quarantine or self-isolation or to be tested for SARS- CoV-2 infection, they should be required to accept, under the same conditions, vaccination certificates issued by other Member States in accordance with Regulation (EU) 2021/953. of the European Parliament and of the Council ([4]). Such acceptance should take place under the same conditions, meaning that, for example, where a Member State considers a single dose of a vaccine administered to be sufficient, it should do so also for holders of a vaccination certificate indicating a single dose of the same vaccine.

(8) Harmonised procedures under Regulation (EC) No 726/2004 of the European Parliament and of the Council ([5]) should not prevent Member States from deciding to accept vaccination certificates issued for other COVID-19 vaccines that have been granted a marketing authorisation by the competent authority of a Member State pursuant to Directive 2001/83/EC of the European Parliament and of the Council ([6]), vaccines the distribution of which has been temporarily authorised pursuant to Article 5(2) of that Directive, and vaccines that have completed the WHO emergency use listing procedure. Where such a COVID-19 vaccine is subsequently granted a marketing authorisation pursuant to Regulation (EC) No 726/2004, the obligation to accept vaccination certificates under the same conditions would also cover vaccination certificates issued by a Member State for that COVID-19 vaccine, regardless of whether the vaccination certificates were issued before or after the authorisation via the centralised procedure. Regulation (EU) 2021/953 lays down a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic. It applies to Union citizens and third-country nationals who are family members of Union citizens.

(9) In accordance with Articles 19, 20 and 21 of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders ([7]), the third-country nationals covered by those provisions may move freely within the territories of the Member States.

(10) Without prejudice to the common rules on the crossing of internal borders by persons as laid down in Regulation (EU) 2016/399 of the European Parliament and of the Council ([8]), and for the purpose of facilitating travel within the territories of the Member States by third-country nationals who are entitled to such travel, the framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates established by Regulation (EU) 2021/953 should also apply to third-country nationals who are not already covered by that Regulation, provided that they are legally staying or residing in the territory of a Member State and are entitled to travel to other Member States in accordance with Union law.

(11) This Regulation is intended to facilitate the application of the principles of proportionality and non-discrimination with regard to travel restrictions during the COVID-19 pandemic, while pursuing a high level of public health protection. It should not be understood as facilitating or encouraging the adoption of restrictions to free movement, or restrictions to other fundamental rights, in response to the COVID-19 pandemic. In addition, any requirement for verification of certificates established by Regulation (EU) 2021/953 does not as such justify the temporary reintroduction of border control at internal borders. Checks at internal borders should remain a measure of last resort, subject to specific rules set out in Regulation (EU) 2016/399.

([4]) Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID 19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID 19 pandemic (See page 1 of this Official Journal).

([5]) Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Union procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency (OJ L 136, 30.4.2004, p. 1).

([6]) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

([7]) OJ L 239, 22.9.2000, p. 19.

([8]) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

(12) Since this Regulation applies to third-country nationals already legally staying or residing in the territories of the Member States, it should not be understood as granting third-country nationals wishing to travel to a Member State the right to an EU Digital COVID Certificate from that Member State before arrival on its territory. There is no requirement for Member States to issue vaccination certificates at consular posts.

(13) On 30 June 2020, the Council adopted Recommendation (EU) 2020/912 ([9]) on the temporary restriction on non-essential travel into the Union and the possible lifting of such restriction. This Regulation does not cover temporary restrictions on non-essential travel into the Union.

(14) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark annexed to the Treaty on European Union (TEU) and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(15) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC ([10]); Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application. In order to allow Member States to accept, under the conditions set out in Regulation (EU) 2021/953, COVID-19 certificates issued by Ireland to third-country nationals legally staying or residing in its territory for the purposes of facilitating travel within the territories of the Member States, Ireland should issue those third-country nationals with COVID-19 certificates that comply with the requirements of the EU Digital COVID Certificate trust framework. Ireland and the other Member States should accept certificates issued to third-country nationals covered by this Regulation on a reciprocal basis.

(16) This Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively, the meaning of Article 3(1) of the 2003 Act of Accession, Article 4(1) of the 2005 Act of Accession and Article 4(1) of the 2011 Act of Accession.

(17) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* ([11]) which fall within the area referred to in Article 1, point C of Council Decision 1999/437/EC ([12]).

(18) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([13]) which fall within the area referred to in Article 1, point C of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ([14]).

(19) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the

([9]) Council Recommendation (EU) 2020/912 of 30 June 2020 on the temporary restriction on non-essential travel into the EU and the possible lifting of such restriction (OJ L 208 I, 1.7.2020, p. 1).
([10]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).
([11]) OJ L 176, 10.7.1999, p. 36.
([12]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).
([13]) OJ L 53, 27.2.2008, p. 52.
([14]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).

European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([15]) which fall within the area referred to in Article 1 point C of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([16]).

(20) Since the objective of this Regulation, namely to facilitate the travel of third-country nationals legally staying or residing in the territories of the Member States during the COVID-19 pandemic by establishing a framework for the issuance, verification and acceptance of interoperable COVID-19 certificates on a person's COVID-19 vaccination, test result or recovery, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(21) Given the urgency of the situation related to the COVID-19 pandemic, this Regulation should enter into force on the day of its publication in the *Official Journal of the European Union*.

(22) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([17]) and delivered a joint opinion on 31 March 2021 ([18]),

HAVE ADOPTED THIS REGULATION:

Article 1

Member States shall apply the rules laid down in Regulation (EU) 2021/953 to third-country nationals who do not fall within the scope of that Regulation, but who are legally staying or residing in their territory and who are entitled to travel to other Member States in accordance with Union law.

Article 2

Provided that Ireland has notified the Council and the Commission that it accepts the certificates referred to in Article 3(1) of Regulation (EU) 2021/953 issued by Member States to persons covered by this Regulation, Member States shall accept, under the conditions of Regulation (EU) 2021/953, COVID-19 certificates issued by Ireland in the format that complies with the requirements of the EU Digital COVID Certificate trust framework established by Regulation (EU) 2021/953 to third-country nationals who are entitled to travel freely within the territory of the Member States.

Article 3

This Regulation shall enter into force on the day of its publication in the *Official Journal of the European Union*.

It shall apply from 1 July 2021 to 30 June 2022.

([15]) OJ L 160, 18.6.2011, p. 21.
([16]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).
([17]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).
([18]) Not yet published in the Official Journal.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels, 14 June 2021.

For the European Parliament	*For the Council*
The President	*The President*
D. M. SASSOLI	A. COSTA

France, décret n. 2020-650 du 29 mai 2020 relatif au traitement de donnée dénommé "StopCovid", Jorf n. 0131 du 30 mai 2020

Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid »

Dernière mise à jour des données de ce texte : 31 mai 2020
NOR : SSAZ2012567D
JORF n°0131 du 30 mai 2020
Le Premier ministre, Sur le rapport du ministre des solidarités et de la santé ;
Vu la directive n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;
Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, notamment son article 4 ;
Vu la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions ;
Vu le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, notamment son article 9 ;
Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 25 mai 2020 ;
Le Conseil d'Etat (section sociale) entendu, Décrète :

Article 1

I. - Il est créé un traitement de données dénommé StopCovid, dont le responsable est le ministre chargé de la santé (direction générale de la santé). Ce traitement de données à caractère personnel est mis en œuvre dans le cadre d'une mission d'intérêt public conformément au e du paragraphe 1 de l'article 6 du règlement (UE) du 27 avril 2016 susvisé, et pour les motifs d'intérêt public mentionnés au i du paragraphe 2 de l'article 9 de ce même règlement.
Il repose sur une application mobile, un serveur central dédié à l'information des utilisateurs ayant été en contact avec un utilisateur diagnostiqué ou dépisté positif au covid-19 et un serveur central distinct dédié à l'information des utilisateurs ayant fréquenté un lieu dans lequel s'est trouvée, au même moment, une personne diagnostiquée ou dépistée positive au covid-19.
II. - Ce traitement a pour finalités :
1° D'informer les personnes utilisatrices de l'application qu'il existe un risque qu'elles aient été contaminées par le virus du covid-19 en raison du fait qu'elles se sont trouvées à proximité d'un autre utilisateur de cette application ayant été diagnostiqué ou dépisté positif à cette pathologie. Les personnes exposées à ce risque sont désignées ci-après comme contacts à risque de contamination ;
2° De sensibiliser les personnes utilisatrices de l'application, notamment celles identifiées comme contacts à risque de contamination, sur les symptômes de ce virus, les mesures barrières et la conduite à adopter pour lutter contre sa propagation ;
3° De recommander aux contacts à risque de contamination de s'orienter vers les acteurs de santé compétents aux fins que ceux-ci les prennent en charge ;
4° De réaliser des analyses statistiques à partir des données anonymes issues de l'application

afin d'adapter les mesures de gestion nécessaires pour faire face à l'épidémie et d'améliorer les performances de l'application ;
5° D'informer les personnes utilisatrices de l'application qu'il existe un risque qu'elles aient été contaminées par le virus du covid-19 en raison du fait qu'elles ont fréquenté un lieu dans lequel se trouvait au même moment une personne ayant été diagnostiquée ou dépistée positive au covid-19. Les personnes exposées à ce risque sont désignées ci-après comme " contacts à risque de contamination " ;
6° De permettre aux personnes utilisatrices, sur présentation du statut " contact à risque de contamination " dans l'application, de bénéficier d'un examen ou test de dépistage dans des conditions de réalisation prioritaire, au même titre que les autres personnes à risque d'infection ;
7° D'informer les personnes utilisatrices de l'application sur la situation sanitaire nationale et locale, ainsi que sur des mesures ou actions de promotion, de prévention et d'éducation pour la santé ou de les orienter vers des applications ou des sites internet mis en œuvre pour la gestion de l'épidémie de covid-19 et de leur fournir des informations sur les données d'utilisation de l'application ;
8° De permettre aux personnes utilisatrices de l'application de stocker des données à caractère personnel sur leur téléphone mobile en vue de générer des justificatifs requis par les autorités publiques.
III. - L'application StopCovid est installée librement et gratuitement par les utilisateurs. Ceux-ci ont la faculté d'activer ou non la fonctionnalité de l'application permettant de constituer l'historique de proximité mentionné au 5° du I de l'article 2. En cas de diagnostic clinique positif au virus du covid-19 ou de résultat positif à un examen de dépistage à ce virus, les utilisateurs de l'application sont libres de notifier ou non ce résultat dans l'application et de transmettre au serveur l'historique de proximité mentionné au 6° du I de l'article 2. L'application peut être désinstallée à tout moment.
IV. - Le code source mis en œuvre dans le cadre de StopCovid est rendu public et est accessible à partir des sites internet du ministre des solidarités et de la santé www.tousanticovid.gouv.fr.
NOTA : Conformément à l'article 2 du décret 2021-157 du 12 février 2021 : Les dispositions du a, du b et du deuxième alinéa du f du 2° de l'article 1er, les dispositions des c, e et g du 3° de l'article 1er et les dispositions du b du 4° de l'article 1er entrent en vigueur le seizième jour suivant la publication du présent décret.

Article 2

I. - Pour la mise en œuvre du traitement mentionné à l'article 1er, sont traitées les données suivantes :

1° Une clé d'authentification partagée entre l'application et le serveur central, générée par ce serveur lors du téléchargement de l'application, qui sert à authentifier les messages de l'application ;
2° Un identifiant unique associé à chaque application téléchargée par un utilisateur, qui est généré de façon aléatoire par le serveur central et n'est connu que de ce serveur, où il est stocké ;
3° Les codes pays, générés par le serveur central ;
4° Des pseudonymes aléatoires et temporaires, qui sont transmis chaque jour par le serveur central à l'application lorsqu'elle se connecte à ce dernier ;
5° L'historique de proximité d'un utilisateur, constitué des pseudonymes aléatoires et temporaires émis via la technologie Bluetooth par les applications installées sur des téléphones mobiles d'autres utilisateurs qui se trouvent, pendant une durée déterminée, à une distance de son téléphone mobile telle qu'il existe un risque suffisamment significatif qu'un utilisateur qui serait positif au virus du covid-19 contamine l'autre. Les pseudonymes aléatoires et temporaires sont collectés et enregistrés par l'application sur le téléphone mobile de l'utilisateur.

Les critères de contact entre deux téléphones permettant de considérer que leurs utilisateurs se trouvent dans une situation présentant un risque de contamination par le virus du covid-19 sont définis par l'Agence nationale de santé publique et sont rendus publics ;
6° L'historique de proximité des utilisateurs déclarés positifs, correspondant aux pseudonymes aléatoires et temporaires enregistrés par l'application dans les quarante-huit heures qui précèdent la date de début des symptômes ainsi que dans la période comprise entre cette date et la date de transfert de l'historique de proximité au serveur central ou, à défaut de renseignement de la date de début des symptômes par la personne diagnostiquée ou dépistée positive, aux pseudonymes aléatoires et temporaires enregistrés par l'application dans les sept jours qui précèdent la date du diagnostic ou du prélèvement positif ainsi que dans la période comprise entre cette date et la date de transfert de l'historique de proximité au serveur central ou, à défaut de renseignement de la date du diagnostic ou du prélèvement positif, aux pseudonymes aléatoires et temporaires enregistrés par l'application pendant les quinze jours qui précèdent le transfert de l'historique de proximité. Ces données sont transmises par les utilisateurs diagnostiqués ou dépistés positifs au virus du covid-19 qui le souhaitent au serveur central. Elles sont alors stockées sur ce serveur et sont notifiées aux applications des personnes identifiées comme contacts à risque de contamination à l'occasion de leur connexion quotidienne au serveur. Ces personnes identifiées comme contacts à risque de contamination reçoivent alors, par l'intermédiaire de l'application, la seule information selon laquelle elles ont été à proximité, au cours d'une période donnée de trois jours, d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du covid-19 ;
6° bis Pour chaque contact à risque de contamination, la date de la remontée de l'historique de proximité de l'utilisateur déclaré positif et la date de la dernière notification du statut " contact à risque de contamination " ;
7° Les périodes d'exposition des utilisateurs à des personnes diagnostiquées ou dépistées positives au virus du covid-19 et une date déterminée aléatoirement entre la date du dernier contact avec l'une de ces personnes, cette date moins un jour et cette date plus un jour. Ces données sont collectées et enregistrées par l'application sur le téléphone mobile de l'utilisateur et stockées sur le serveur central en cas de partage par l'utilisateur de l'historique de proximité des contacts à risque de contamination par le virus du covid-19 ;
8° Les données renseignées dans l'application par les personnes diagnostiquées ou dépistées positives au virus du covid-19 qui décident d'envoyer au serveur l'historique de proximité de leurs contacts à risque :

a) La date de début des symptômes si l'utilisateur est en mesure de donner cette information ou la date du prélèvement positif si la personne est asymptomatique ou n'est pas en mesure de donner la date de début des symptômes ;

b) Le code aléatoire à usage unique donné par un médecin traitant à son patient suite à un diagnostic clinique positif au virus du covid-19 ou un code aléatoire à usage unique sous forme de QR-code émis par le traitement mentionné à l'article 8 du décret n° 2020-551 du 12 mai 2020 susvisé en cas d'examen de dépistage positif au virus du covid-19, en application de l'article 9 de ce même décret, afin que l'utilisateur de l'application soit autorisé par le serveur à partager son historique de proximité ;

9° Le statut «contacts à risque de contamination» de l'identifiant de l'application, qui est retenu dès lors qu'un utilisateur de l'application a été, conformément aux critères définis par l'arrêté mentionné au 5°, à proximité d'un autre utilisateur, ultérieurement dépisté ou

diagnostiqué positif au virus du covid-19. Cette donnée est stockée par le serveur central, lorsqu'elle lui a été communiquée par l'utilisateur qui accepte de lui transmettre son historique de proximité des contacts à risque de contamination par le virus du covid-19 ;
10° La date des dernières interrogations du serveur central ;
11° Le pseudonyme, le type d'activité, la superficie et la plage horaire de fréquentation des lieux mettant un QR-code à disposition des utilisateurs de l'application. Ces informations sont stockées sur un serveur central en vue d'informer les utilisateurs qu'ils ont fréquenté, au cours d'une période donnée de trois jours, un lieu où se trouvait, pendant tout ou partie de la même plage horaire, une personne diagnostiquée ou dépistée positive au covid-19 ;
12° Le code postal renseigné dans l'application par l'utilisateur pour obtenir des informations locales sur la situation sanitaire. Cette donnée ne fait l'objet d'aucun traitement sur le serveur central ;
13° Les données à caractère personnel renseignées par l'utilisateur permettant de générer le QR-code lui permettant de disposer d'une attestation de déplacement dérogatoire.
II. - Les données permettant l'identification du téléphone mobile, de son détenteur ou de son utilisateur ne peuvent être collectées ni enregistrées dans le cadre du traitement.
Les données à caractère personnel renseignées par l'utilisateur lorsqu'il accède à d'autres sites ou applications via l'application TousAntiCovid ne peuvent être ni collectées ni enregistrées dans le cadre du traitement de données TousAntiCovid.

Les données à caractère personnel renseignées pour générer les justificatifs mentionnés au 9° du II de l'article 1er du présent décret ne peuvent être enregistrées que par l'utilisateur, s'il le souhaite, aux fins d'être conservées localement sur le téléphone mobile.

III. - Les sous-traitants auxquels le responsable du traitement peut recourir dans les conditions prévues à l'article 28 du règlement (UE) 2016/679 du 27 avril 2016 susvisé sont accédants ou destinataires des données du traitement strictement nécessaires à l'exercice de leurs missions.
NOTA :
Conformément à l'article 2 du décret 2021-157 du 12 février 2021 : Les dispositions du a, du b et du deuxième alinéa du f du 2° de l'article 1er, les dispositions des c, e et g du 3° de l'article 1er et les dispositions du b du 4° de l'article 1er entrent en vigueur le seizième jour suivant la publication du présent décret.
Article 3
Le traitement est mis en œuvre jusqu'au 31 décembre 2021.
La clé d'authentification partagée et l'identifiant aléatoire permanent sont conservés jusqu'à ce que l'utilisateur désinstalle l'application StopCovid, et au plus tard pour la durée mentionnée au premier alinéa.
Les données de l'historique de proximité enregistrées par l'application sur le téléphone mobile sont conservées quinze jours à compter de leur enregistrement par cette application.
Lorsqu'elles ont été partagées sur le serveur central, les données de l'historique de proximité des contacts à risque de contamination sont conservées sur ce serveur quinze jours à compter de leur enregistrement par l'application du téléphone mobile de la personne dépistée ou diagnostiquée positive au virus du covid-19.
Les données mentionnées au 8° du I de l'article 2 ne sont pas conservées. Elles ne sont traitées qu'une seule fois afin que l'utilisateur de l'application soit autorisé par le serveur à partager son historique de proximité.
Les actions réalisées par les administrateurs dans le traitement font l'objet d'un

enregistrement, qui est conservé pendant une durée maximale de six mois à compter de la fin de l'état d'urgence sanitaire. Cet enregistrement comporte l'identification de l'administrateur, les données de traçabilité, notamment la date, l'heure et la nature de l'intervention dans le traitement.
Les données mentionnées au 11° du I de l'article 2 sont conservées sur le serveur central et sur le téléphone de l'utilisateur pendant quinze jours à compter de leur enregistrement sur ce téléphone. L'utilisateur a la possibilité, depuis son terminal, de supprimer de son historique tout lieu visité.
La donnée mentionnée au 12° du I de l'article 2 n'est pas conservée.
Le QR-code mentionné au 13° du I de l'article 2 ne peut être conservé plus de 24 heures à compter de sa date et heure de validité.
NOTA :
Conformément à l'article 2 du décret 2021-157 du 12 février 2021 : Les dispositions du a, du b et du deuxième alinéa du f du 2° de l'article 1er, les dispositions des c, e et g du 3° de l'article 1er et les dispositions du b du 4° de l'article 1er entrent en vigueur le seizième jour suivant la publication du présent décret.

Article 4

Modifié par Décret n°2021-157 du 12 février 2021 - art. 1

En application de l'article 11 et du i du paragraphe 1 de l'article 23 du règlement (UE) du 27 avril 2016 susvisé, les droits d'accès, de rectification ainsi que le droit à la limitation prévus aux articles 15, 16 et 18 de ce même règlement ne peuvent s'exercer auprès du responsable de traitement.

Les personnes concernées sont informées des principales caractéristiques du traitement et de leurs droits, conformément aux dispositions des articles 13 et 14 du règlement (UE) du 27 avril 2016 susvisé, au moment de l'installation de l'application StopCovid. Elles sont en outre prévenues qu'en cas de partage de leur historique de proximité sur le serveur central avant le seizième jour suivant la publication du décret n° 2021-157 du 12 février 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé " StopCovid ", les personnes identifiées comme leurs contacts à risque de contamination seront informées qu'elles auront été à proximité, au cours des quinze derniers jours, d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du covid-19 et qu'en cas de partage de leur historique de proximité ou de lieux fréquentés sur le serveur central à compter du quinzième jour suivant la publication du même décret, les personnes identifiées comme leurs contacts à risque de contamination seront informées qu'elles auront, au cours d'une période donnée de trois jours, été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du covid-19, ou fréquenté un même lieu au même moment qu'au moins une personne diagnostiquée ou dépistée positif au virus du covid-19. Elles sont également informées de la possibilité limitée d'identification indirecte susceptible d'en résulter lorsque ces personnes ont, au cours de cette période, eu un très faible nombre de contacts ou fréquenté des lieux où se trouvaient au même moment un faible nombre de personnes.

Des mentions d'information sont également publiées sur le site internet www.tousanticovid.gouv.fr. et sur la page https://bonjour.tousanticovid.gouv.fr/privacy.html, et apposées à proximité des QR-codes situés devant ou dans les lieux qui en sont équipés.

Article 5

Modifié par Décret n°2021-157 du 12 février 2021 - art. 1

Le responsable de traitement rend public un rapport sur le fonctionnement de StopCovid

dans les trente jours suivant le terme de la mise en œuvre de l'application.
Article 6
A modifié les dispositions suivantes
Modifie Décret n°2020-551 du 12 mai 2020 - art. 9 (M)
Article 7
Le ministre des solidarités et de la santé, le ministre de l'économie et des finances ainsi que le secrétaire d'Etat chargé du numérique sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait le 29 mai 2020.

Edouard Philippe Par le Premier ministre :
Le ministre des solidarités et de la santé, Olivier Véran

Le ministre de l'économie et des finances, Bruno Le Maire
Le secrétaire d'Etat auprès du ministre de l'économie et des finances, chargé du numérique, Cédric O

Germany, Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an den Bundesminister für Gesundheit zur Frage, welche Zwecke einer «Corona App» einer gesetzlichen Regelung bedürfen, 13.05.2020.

GESCHÄFTSZ.
13-401/008#0090
Gesetzliche Regelung einer „Corona App"

Sehr geehrter Herr Minister Spahn,
im Rahmen der derzeit diskutierten Maßnahmen zur Bekämpfung der Corona-Pandemie mehren sich im politischen Raum Stimmen, die eine gesetzliche Regelung für die von der Bundesregierung angedachte „Corona-Warn-App" fordern. Zu der damit verbundenen grundsätzlichen Frage, ob eine solche App einer gesetzlichen Regelung bedarf oder aber insoweit eine freiwillige und informierte Einwilligung der Bürgerinnen und Bürger ausreichend ist, möchte ich auf folgendes hinweisen:

Soweit beim Angebot einer derartigen App die Verarbeitung personenbezogener Daten in der mir derzeit bekannten Form erfolgt, die App in Kenntnis der beabsichtigten Datenverarbeitung freiwillig aus einem App Store heruntergeladen wurde, und deren Zweck allein die Aufdeckung potenzieller Infektionskontakte für die nutzende Person selbst ist, gehe ich davon aus, dass dies seine Rechtsgrundlage in Artikel 9 Absatz 2 lit. a) in Verbindung mit Artikel 6 Absatz 1 lit. a) Datenschutz-Grundverordnung (DSGVO), d.h. in der Einwilligung des Nutzers der App, findet. Dies ergibt sich auch deshalb, da der Zweck der Datenverarbeitung, in die eingewilligt wird, eng begrenzt ist. Für die Verarbeitung dieser Daten bedarf es daher keiner weiteren gesetzlichen Regelung.

Auch die Nutzung dieser Daten für Zwecke der epidemiologischen Forschung, die nach Artikel 5 Absatz 1 lit. b) DSGVO vereinbar mit dem ursprünglichen Zweck der App wäre, könnte im Rahmen einer (zusätzlichen) Einwilligungslösung möglich sein. Soweit der Forschungszweck zum Zeitpunkt der Nutzung der Daten noch nicht vollständig feststeht, sieht Erwägungsgrund 33 der Datenschutz-Grundverordnung unter den dort genannten engen Voraussetzungen ausnahmsweise die Möglichkeit einer Einwilligung zu Nutzung von Daten in diese noch nicht präziser zu bezeichnenden Forschungszwecke vor (sog. breite Einwilligung «broad consent») . Außerhalb der im Erwägungsgrund 33 festgelegten Grenzen kommt hingegen eine Verarbeitung der durch die App generierten Daten für Zwecke der epidemiologischen Forschung auf Grundlage einer Einwilligung nicht in Betracht.

Wenn eine über den ursprünglichen Zweck hinausgehende Verarbeitung von Gesundheitsdaten im Sinne des Artikels 9 Absatz 1 DSGVO erfolgen soll, insbesondere wenn die Nutzung seiner Daten für den Nutzer der App nicht absehbar ist, hielte ich die Verarbeitung der mit der Corona-Warn-App gesammelten Daten aufgrund einer Einwilligung nicht für ausreichend legitimiert. Dann bedürfte es einer gesetzlichen Regelung, bei der der Gesetzgeber insbesondere die Verhältnismäßigkeit und damit auch die Erforderlichkeit sowie die Geeignetheit der Datenverarbeitung zu einem legitimen Zweck darzulegen hat.

Eine verbleibende kritische Fragestellung ist die potenzielle Nutzung der Corona- Warn-App durch Minderjährige. Hier stellt sich das Problem, dass vor allem jüngere Kinder

rechtlich nicht wirksam in die Datenverarbeitung einwilligen können, so dass es für sie Einwilligungserklärungen der Erziehungsberechtigten bedürfte. Dies wiederum macht es erforderlich, weitere technisch-organisatorische Maßnahmen vorzusehen, um eine ordnungsgemäße Dokumentation der Einwilligungen sicherzustellen. Wir sind dazu mit den Entwicklern der Corona-Warn-App im Gespräch. Eine alternative Lösung könnte in einer rechtlichen Legitimation der Datenverarbeitung durch eine zu schaffende gesetzliche Grundlage sein. Diese müsste so ausgestaltet werden, dass sie die Freiwilligkeit der App-Nutzung voraussetzt und die elterlichen Rechte unberührt lässt. In diesem Fall bedürfte es keiner Einwilligung nach Artikel 9 Absatz 2 lit. a) in Verbindung mit Artikel 6 Absatz 1 lit. a) Daten- schutz-Grundverordnung (DSGVO).

Soweit der Gesetzgeber auf eine gesetzliche Regelung der Verarbeitung von durch die Corona-Warn-App gewonnener Daten verzichten möchte, ergeben sich im Übrigen die Rechte der Betroffenen, insbesondere auf Auskunft, Löschung, Einschränkung der Verarbeitung etc., im Wesentlichen unmittelbar aus der Datenschutz-Grundverordnung sowie den allgemeinen staatlichen Gesetzen, aber auch aus den durch die Gerichte des Bundes und der Länder aufgestellten Vorgaben.

Sollte der Gesetzgeber hingegen eine Regelung der Nutzung der Corona-Warn-App in einer Rechtsvorschrift für geboten halten, müsste beispielsweise geregelt werden, zu welchen Zwecken welche Daten der App-Nutzer und -Nutzerinnen von welcher Stelle verarbeitet werden. Zudem wären die datenschutzrechtlichen Verantwortlichen eindeutig zu benennen, die Betroffenenrechte auszugestalten, Löschpflichten und -fristen vorzusehen sowie die datenschutzrechtlich erforderlichen technischen und organisatorischen Maßnahmen vorzugeben . Weitere mögliche Regelungsgegenstände wären aus meiner Sicht u. a. , Dritten zu untersagen, Bürgerinnen und Bürger zu verpflichten, sich eine entsprechende App aus einem App-Store herunterzuladen und ihnen die Ergebnisse eines möglichen Kontaktes mit einem Infizierten zu offenbaren. Hintergrund ist u.a. die an mich herangetragene Befürchtung, dass beispielsweise Arbeitgeber ihre Beschäftigten verpflichten könnten, eine entsprechende App zu nutzen und möglicherweise auch Ergebnisse der App-Nutzung dem Arbeitgeber zu offenbaren. Dies würde aber einer freiwilligen Nutzung und damit auch der Akzeptanz einer „Corona-Warn-App“ zuwiderlaufen. Ich rege an, für den Fall einer gesetzlichen Regelung ein solches unzulässiges Verhalten mit einer Strafandrohung zu versehen.

Ein weiterer Aspekt, der im Falle einer gesetzlichen Regelung bedacht werden solle, wäre eine Regelung über ein Verbot des Zugriffs von Strafverfolgungsbehörden, eines Beschlagnahme- und Verwertungsverbots im Strafverfahren. Derartige Regelungen würden zudem die Akzeptanz der Corona-Warn-App weiter erhöhen.

Mit freundlichen Grüßen,
Ulrich Kelber

Italy, Decreto Legge 30 aprile 2020, n. 28, Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché 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. (20G00046)

Capo I - Misure urgenti in materia di intercettazioni di conversazioni e comunicazioni, di ordinamento penitenziario e disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 77 e 87 della Costituzione;

Visto il decreto legislativo 29 dicembre 2017, n. 216, recante «Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103»;

Visto il decreto-legge 30 dicembre 2019, n. 161, convertito, con modificazioni, dalla legge 28 febbraio 2020, n. 7;

Ritenuta la straordinaria necessità ed urgenza di differire l'entrata in vigore della nuova disciplina delle intercettazioni telefoniche ed ambientali come dettata dal decreto legislativo n. 216 del 2017 e rimodulata dal decreto-legge n. 161 del 2019 per le esigenze di adeguamento delle strutture, il cui processo in corso è stato rallentato dalla grave emergenza epidemiologica da COVID-19 in atto;

Ritenuta la necessità ed urgenza di integrare la disciplina dell'ordinamento penitenziario in materia di rinvio dell'esecuzione della pena in detenzione domiciliare e permessi nel caso di detenuti per reati gravi o sottoposti al regime previsto dall'articolo 41-bis del medesimo ordinamento, nonché' di introdurre con urgenza le necessarie disposizioni di coordinamento e adeguamento della disciplina sulla sospensione dei termini processuali per contrastare l'emergenza epidemiologica da COVID-19, nonché' disposizioni integrative e di coordinamento in materia di giustizia amministrativa e contabile;

Considerata la necessità e l'urgenza di introdurre misure urgenti per l'introduzione del sistema di allerta Covid-19;

Acquisito sull'articolo 6 il parere del Garante per la protezione dei dati personali, reso nell'adunanza del 29 aprile 2020;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 29 aprile 2020;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri per l'innovazione tecnologica e la digitalizzazione, della salute e dell'economia e delle finanze;

Emana il seguente decreto-legge:

(…)

Capo II Misure urgenti per l'introduzione del sistema di allerta Covid-19

Art. 6 Sistema di allerta Covid-19

1. Al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19, è istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile. Il Ministero

della salute, in qualità di titolare del trattamento, si coordina, sentito il Ministro per gli affari regionali e le autonomie, anche ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, con i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, e con i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché' con l'Istituto superiore di sanità e, anche per il tramite del Sistema Tessera Sanitaria, con le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID 19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanità pubblica e di cura. Le modalità operative del sistema di allerta tramite la piattaforma informatica di cui al presente comma sono complementari alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale. Il Ministro della salute e il Ministro per gli affari regionali e le autonomie informano periodicamente la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano sullo stato di avanzamento del progetto.

2. Il Ministero della salute, all'esito di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'articolo 35 del Regolamento (UE) 2016/679, adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, sentito il Garante per la protezione dei dati personali ai sensi dell'articolo 36, paragrafo 5, del medesimo Regolamento (UE) 2016/679 e dell'articolo 2-quinquiesdecies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, assicurando, in particolare, che:

a) gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati;

b) per impostazione predefinita, in conformità all'articolo 25 del Regolamento (UE) 2016/679, i dati personali raccolti dall'applicazione di cui al comma 1 siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, individuati secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure di cui al presente comma, nonché' ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti;

c) il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati; è esclusa in ogni caso la geolocalizzazione dei singoli utenti;

d) siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché' misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento;

e) i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute e specificata nell'ambito delle misure di cui al presente comma; i dati sono cancellati in modo automatico alla scadenza del termine;

f) i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679 possano essere esercitati anche con modalità semplificate.

3. I dati raccolti attraverso l'applicazione di cui al comma 1 non possono essere trattati per finalità diverse da quella di cui al medesimo comma 1, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca

scientifica, ai sensi degli articoli 5, paragrafo 1, lettera a) e 9, paragrafo 2, lettere i) e j), del Regolamento (UE) 2016/679. Al solo fine indicato al comma 1, previa valutazione d'impatto ai sensi dell'articolo 35 del regolamento (UE) 2016/679, è consentita l'interoperabilita' con le piattaforme che operano, con le medesime finalità, nel territorio dell'Unione europea.
4. Il mancato utilizzo dell'applicazione di cui al comma 1 non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento.
5. La piattaforma di cui al comma 1 è di titolarità pubblica ed è realizzata dal Commissario di cui all'articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite dalla società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. I programmi informatici di titolarità pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione di cui al medesimo comma 1 sono resi disponibili e rilasciati sotto licenza aperta ai sensi dell'articolo 69 del decreto legislativo 7 marzo 2005, n. 82.
6. L'utilizzo dell'applicazione e della piattaforma, nonché' ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione delle esigenze di protezione e prevenzione sanitaria, legate alla diffusione del COVID-19 anche a carattere transfrontaliero, individuata con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della salute, e comunque entro il 31 dicembre 2021, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi.
7. Agli oneri derivanti dall'implementazione della piattaforma di cui al presente articolo, nel limite massimo di 1.500.000 euro per l'anno 2020, si provvede mediante utilizzo delle risorse assegnate per il medesimo anno al Commissario straordinario di cui all'articolo 122 del decreto-legge 17 marzo 2020, n. 18 con delibera del Consiglio dei Ministri a valere sul Fondo emergenze nazionali di cui all'articolo 44 del decreto legislativo 2 gennaio 2018, n. 1.

Capo III Disposizioni finanziarie e finali

Art. 7 - Disposizioni finanziarie
1. Dall'attuazione degli articoli del presente decreto, ad eccezione di quanto previsto all'articolo 6, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le Amministrazioni interessate provvedono agli adempimenti connessi mediante l'utilizzazione delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

(…)

Art. 8 - Entrata in vigore
1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana e sarà presentato alle Camere per la conversione in legge.

Luxembourg, Loi du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant : 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

Mémorial : A624
Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,
Notre Conseil d'État entendu ;
De l'assentiment de la Chambre des Députés ;
Vu la décision de la Chambre des Députés du 16 juillet 2020 et celle du Conseil d'État du 17 juillet 2020 portant qu'il n'y a pas lieu à second vote ;
Avons ordonné et ordonnons : (…)

Chapitre 3 - Traitement des informations
Art. 10.
(1) En vue de suivre l'évolution de la propagation du virus SARS-CoV-2 et les effets des vaccins contre la maladie Covid-19, sont autorisés des traitements de données à caractère personnel au travers de la mise en place d'un système d'information pour les finalités suivantes :
1° détecter, évaluer, surveiller et combattre la pandémie de Covid-19 ;
1°bis acquérir les connaissances fondamentales sur la propagation et l'évolution de cette pandémie, y inclus au travers de suivis statistiques, d'études et de recherche ;
2° garantir aux citoyens l'accès aux soins et aux moyens de protection contre la maladie Covid-19 ;
2°bis suivre et évaluer de manière continue l'efficacité et la sécurité des vaccins contre la Covid-19 ainsi que l'évolution de l'état de santé des personnes vaccinées ;
2°ter suivre et évaluer le programme de dépistage à grande échelle et le programme de vaccination ;
3° créer les cadres organisationnel et professionnel requis pour surveiller et combattre la pandémie de Covid-19 ;
4° répondre aux demandes d'informations et aux obligations de communication d'informations provenant d'autorités de santé européennes ou internationales.
(1*bis*) La Direction de la santé est responsable des traitements visés au paragraphe 1 er, à l'exception de l'identification des catégories de personnes à inviter dans le cadre des programmes de dépistage à grande échelle et de vaccination qui relève de la responsabilité de l'Inspection générale de la sécurité sociale.
(2) Les traitements prévus au paragraphe 1 er portent sur les données à caractère personnel suivante :
1° les données collectées en vertu de l'article 5 ;
2° les données collectées en vertu des articles 3 à 5 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique.
2°bis
Pour le programme de dépistage à grande échelle, en vue de l'identification des catégories de personnes à inviter :
a) les données socio-démographiques (âge, sexe, composition du ménage, localité de résidence) ;
b) les données sur l'emploi (secteur d'activité professionnelle et employeur) ;

c) l'historique des dépistages Covid-19.

Pour le programme de vaccination, en vue de l'identification des catégories de personnes à inviter :

a) les données socio-démographiques (âge, sexe, composition du ménage, localité de résidence) ;

b) les données sur l'emploi (secteur d'activité professionnelle et employeur) ;

c) la date de rendez-vous pour la vaccination ;

d) si le vaccin a été administré.

3°

les données collectées dans le cadre du programme de vaccination :

a)

pour le vaccinateur :

i) les données d'identification (nom, prénoms, date de naissance, sexe) ;

ii) les coordonnées de contact (numéro de téléphone et adresse électronique) ;

iii) la désignation de l'organisme de sécurité sociale et le numéro d'identification ;

b)

pour la personne à vacciner :

i) les données d'identification (nom, prénoms, date de naissance, sexe) de la personne et de ses éventuels représentants légaux ;

ii) les coordonnées de contact (numéro de téléphone et adresse électronique) ;

iii) le numéro d'identification ;

iv) le critère d'allocation du vaccin (âge, profession, secteur d'activité professionnelle ou vulnérabilité) ;

v) les données permettant de déterminer la présence éventuelle de contre-indications, la présence de problèmes de santé ou d'autres facteurs de risque, et la présence d'effets indésirables ;

vi) les données d'identification du vaccinateur ;

vii) la décision sur l'administration (décision, date, et raisons) ;

viii) les caractéristiques de la vaccination (site d'administration, marque, numéro de lot, numéro d'administration et date de péremption).

c)

Les nom, prénoms et numéro d'identification des personnes vulnérables en raison d'un état de santé préexistant transmises par un médecin, sur demande de cette dernière ou de ses représentants légaux, au directeur de la santé ou à son délégué.

Ces données sont traitées exclusivement en vue d'inviter les personnes visées à l'alinéa 1er. Elles sont anonymisées au plus tard trois semaines après la date de l'envoi de l'invitation à se faire vacciner.

4°

Les données à caractère personnel visées au point 3° a) sont anonymisées au plus tard à l'issue d'une durée de deux ans après leur collecte. Les données à caractère personnel visées au point 3° b) sont anonymisées au plus tard à l'issue d'une durée de vingt ans après leur collecte, à l'exception des données énoncées au point 3° b) i) et ii) qui sont anonymisées au plus tard à l'issue d'une durée de deux ans après leur collecte et des données énoncées au point 3° b) v) qui sont anonymisées au plus tard à l'issue d'une durée de dix ans après leur collecte.

Par dérogation à l'alinéa 1er :

a) en cas de réfutation de l'indication de la vaccination par le vaccinateur, les données à caractère personnel visées au point 3° b), dans la mesure où elles sont collectées, sont anonymisées au plus tard à l'issue d'une durée de deux ans après leur collecte.
b) en cas de retrait de l'accord à se faire vacciner par la personne à vacciner ou par son représentant légal, les données à caractère personnel visées au point 3° b), dans la mesure où elles sont collectées, sont anonymisées au plus tard à l'issue d'une durée de trois mois après leur collecte.

5° Les vaccinateurs ou les personnes placées sous leur responsabilité enregistrent sans délai les données visées au point 3° a) et b).
(3) Seuls les médecins et professionnels de la santé ainsi que les fonctionnaires , employés ou les salariés mis à disposition du ministre ayant la Santé dans ses attributions en application de l'article L. 132-1 du Code du travail ou toute autre personne , nommément désignés à cet effet par le directeur de la santé, sont autorisés à accéder aux données relatives à la santé des personnes infectées ou à haut risque d'être infectées. Ils accèdent aux données relatives à la santé dans la stricte mesure où l'accès est nécessaire à l'exécution des missions légales ou conventionnelles qui leur sont confiées pour prévenir et combattre la pandémie de Covid-19 et sont astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 458 du Code pénal.
(3*bis*) Sans préjudice du paragraphe 2, 2° *bis* et 3° c), l'Inspection générale de la sécurité sociale est destinataire des données traitées qu'elle pseudonymise pour les fins énoncées au paragraphe 6.
(4) Les personnes infectées ou à haut risque d'être infectées ne peuvent pas s'opposer au traitement de leurs données dans le système d'information visé au présent article tant qu'elles ne peuvent pas se prévaloir du résultat d'un test de dépistage négatif de l'infection au virus SARS-CoV-2. Pour le surplus, les droits des personnes concernées prévus par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après désigné comme « règlement (UE) 2016/679 », s'exercent auprès de la Direction de la santé.
(5) Sans préjudice du paragraphe 2, point 3° et des paragraphes 3 *bis* et 5, de l'article 5, paragraphe 2 *bis*, alinéa 3, paragraphe 3, point 2° et paragraphe 3 *bis*, les données à caractère personnel traitées sont pseudonymisées au plus tard à l'issue d'une durée de six mois après leur collecte pour une période de trois ans à l'issue de laquelle elles sont anonymisées. Les données de journalisation qui comprennent les traces et logs fonctionnels permettant la traçabilité des accès et actions au sein du système d'information suivent le même cycle de vie que les données auxquelles elles se rapportent. Les accès et actions réalisés sont datés et comportent l'identification de la personne qui a consulté les données ainsi que le contexte de son intervention.
Par dérogation à l'alinéa 1er, les données des personnes sont anonymisées avant leur communication aux autorités de santé européennes ou internationales.
(6) Les données peuvent être traitées à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions prévues par le règlement (UE) 2016/679 précité et par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, sous réserve d'être pseudonymisées au sens de l'article 4, paragraphe 5, du règlement (UE) 2016/679 précité.

Luxembourg, Commission nationale pour la protection des données, Délibération n° 13/2020 du 8 juin 2020

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19) et modifiant 1. la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2. la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments. Délibération n° 13/2020 du 8 juin 2020

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1 er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») « conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».
En date du 4 juin 2020, Madame la Ministre de la Santé a saisi la Commission nationale à se prononcer sur le projet n°7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19) et modifiant 1. la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2. la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après le « projet de loi »). Dans ledit courrier Madame la Ministre a précisé que le projet en cause devra entrer en vigueur au plus tard le 24 juin 2020, date de la levée de l'état de crise, et que partant, elle nous prie de lui faire parvenir notre avis endéans les plus brefs délais. La CNPD tient à souligner que son avis a ainsi été élaboré et adopté uniquement sur base des informations dont elle dispose et sous réserve d'éventuelles considérations futures non connues à ce jour. Le présent projet de loi a pour objet de créer un cadre légal se rapportant à des mesures prises à l'égard des personnes physiques pour continuer la lutte contre le Covid-19 en limitant la propagation du SARS-CoV-2 sur le territoire du Grand-Duché de Luxembourg moyennant un catalogue limité de mesures bien circonscrites. Il ressort de l'exposé des motifs qu'à côté des mesures centrées sur les personnes physiques, le projet de loi s'articule autour des trois axes suivants :

- la limitation de la liberté de rassemblement ;
- l'application de mesures de protection ainsi que l'identification, le suivi et la mise à l'écart rapide des personnes infectées et susceptibles d'être infectées ;
- l'instauration de « certaines garanties autour du traitement des données nécessaires au suivi des personnes et à la lutte contre la pandémie. »

La Commission nationale tient à souligner à titre préliminaire que la protection des données personnelles n'est pas à considérer comme obstacle à la mise en place d'un traitement de données à caractère personnel dans le cadre de la lutte contre l'épidémie Covid-19, tant que les principes fondamentaux prévus par le RGPD sont respectés. Elle entend ainsi limiter ses

observations aux dispositions du projet de loi ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel, et plus précisément à son article 9.

Ad article 9 du projet de loi n°7606

L'article 9 du projet de loi n°7606 vise la création d'un système d'information par la Direction de la santé, afin de surveiller l'évolution de la situation liée au Covid-19 et de formuler des recommandations dans l'intérêt de la santé publique à l'attention du Gouvernement (ci-après : le « système d'information »). Le commentaire de l'article précise qu'à cette fin, un système de monitoring avec différents indicateurs et types de données est mis en place, incluant tant des données à caractère personnel que des données à caractère non personnel qui doivent obligatoirement être transmises à l'autorité de santé publique. En vertu du paragraphe (2) de l'article 9 du projet de loi, différentes données à caractère personnel concernant les personnes infectées ou présumées infectées au Covid-19 sont à transmettre à la Direction de la Santé par les établissements hospitaliers, les structures d'hébergement et les réseaux de soins en vue de détecter, évaluer, surveiller et combattre le Covid-19. Ces données sont énumérées aux articles 3 et 4 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique. Étant donné que le projet de loi ne définit pas d'autres catégories de données individuelles à fournir que celles énumérées aux articles 3 et 4 susmentionnées, la Commission nationale estime que le présent article est à lire restrictivement et que nonobstant le fait que l'énumération des données à collecter comprend la précision « au moins », elle ne doit pas être élargie en l'espèce, sinon il faudrait le préciser. La Commission nationale comprend donc qu'il s'agit plus spécifiquement du nom, prénom, adresse, date de naissance, diagnostic médical, date des 1ers symptômes et date du diagnostic médical, date de prélèvement et origine du prélèvement, pays où la maladie a été contractée et la source d'infection si connue. Il est donc indéniable que des catégories particulières de données à caractère personnel, dites données « sensibles », seront traitées à travers ce système d'information. Ces données, incluant les données concernant la santé, sont spécifiquement réglementées par l'article 9 du RGPD. Par principe, il est interdit de traiter des données sensibles, sauf si une des dix conditions prévues au paragraphe (2) de l'article 9 du RGPD est remplie. Sous réserve des commentaires qui suivent et face à la déclaration du 30 janvier 2020 de l'Organisation mondiale de la santé (OMS) que l'apparition du coronavirus SARS-CoV-2 (Covid-19) constitue une « urgence sanitaire mondiale », ainsi qu'à la déclaration subséquente de l'état de crise sur base de l'article 32 paragraphe 4 de la Constitution luxembourgeoise par règlement grand- ducal du 18 mars 2020[10], la CNPD considère que l'exception prévue à l'article 9 paragraphe 2) lettre i) du RGPD est applicable en l'espèce. Ladite disposition prévoit plus précisément que le traitement de données sensibles peut être effectué lorsqu'il est « nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel. »

Le considérant (46) du RGPD précise dans ce contexte que certains types de traitements peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire pour suivre des épidémies et leur propagation.

[10] Il s'agit du règlement grand-ducal du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19.

En sus de l'article 9 du RGPD, le traitement de données à caractère personnel envisagé par la Direction de la santé doit se baser sur un des critères de licéité prévus à l'article 6 du RGPD. Sur base des mêmes considérations, la CNPD estime que ledit traitement est à considerer comme étant « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (article 6 paragraphe (1) lettre e) du RGPD).
Le considérant (54) du RGPD énonce dans ce contexte que le « traitement des categories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. »
La base légale de l'intérêt public sur laquelle repose donc le traitement en question[11] rend applicable l'ensemble des droits prévus par le RGPD au bénéfice des personnes concernées, à l'exclusion du droit à la portabilité. Le projet de loi n°7606 prévoit néanmoins en son article 9 paragraphe (4) que les personnes infectées ou présumées infectées ne peuvent pas s'opposer au traitement de leurs données dans le système d'information visé audit article. Par cette exclusion du droit d'opposition, il apparaît que les auteurs du projet de loi font usage de la faculté offerte par l'article 23 paragraphe (1) lettre e) du RGPD de limiter les droits des personnes pour garantir, notamment, des objectifs importants de santé publique.
Sans préjudice de ses remarques sous le point 2. concernant la durée de conservation des données, la CNPD peut a priori comprendre que cette limitation du droit d'opposition des personnes infectées, ainsi que des personnes présumées infectées et dont le test s'avère positif, est obligatoire afin de pouvoir suivre l'évolution de ce virus encore très peu connu par le monde scientifique, surtout qu'à « ce stade il est prématuré d'affirmer avec certitude que la présence d'anticorps équivaut à une immunité contre l'infection, voire de se prononcer sur la durée éventuelle de cette protection. Donc, à l'heure actuelle, un résultat positif d'un test sérologique ne garantit pas une immunité. »[12].
Néanmoins, la CNPD ne disposant pas des compétences scientifiques et épidémiologiques nécessaires, elle n'est pas en mesure d'évaluer, sans explications supplémentaires et plus précises de la part des auteurs du projet de loi, si la restriction absolue du droit d'opposition des personnes présumées infectées, mais dont le test s'avère négatif, est vraiment nécessaire dans le cadre de la lutte contre le Covid-19.

Par ailleurs, en vertu du paragraphe (2) de l'article 23 du RGPD, chaque mesure législative qui vise à limiter les droits des personnes concernées doit obligatoirement contenir un certain nombre de dispositions spécifiques y énumérées. Afin d'évaluer si le texte du projet de loi n°7606 respecte les dispositions du RGPD et répond plus particulièrement aux exigences de l'article 9 paragraphe (2) lettre i) du RGPD et dudit article 23 paragraphe (2) du RGPD, la CNPD analysera successivement les finalités du traitement et les catégories de données à caractère personnel (1.), la durée de conservation des données (2.), les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites (3.), ainsi que le droit des personnes d'être informées (4.).
1. Quant aux finalités du traitement et aux catégories de données à caractère personnel

[11] Par l'article 6 paragraphe (1) lettre e) tout comme l'article 9 paragraphe 2) lettre i) du RGPD.
[12] Communiqué de presse du 22 mai 2020 du Ministère de la Santé et du Ministère de l'Enseignement supérieur etde la recherche : « COVID-19 - Une stratégie de test ambitieuse et au service de la santé publique », disponible sous : https://gouvernement.lu/dam-assets/documents/actualites/2020/05-mai/Communique-de-presse-depistage-2252020-.pdf.

L'article 9 paragraphe (1) du projet de loi n°7606 énumère quatre différentes finalités poursuivies par la mise en place du système d'information dont la Direction de la santé est à considérer comme responsable du traitement conformément au sens de l'article 4 point 7) du RGPD. En vertu de l'article 5 paragraphe (1) lettre b) du RGPD, les finalités d'un traitement de données doivent être déterminées, explicites et légitimes. La CNPD considère que les finalités, telles que décrites actuellement à l'article 9 du projet de loi n°7606, peuvent paraître assez larges, ce qu'elle peut a priori comprendre vu que les conséquences et le développement futur du Covid-19 n'ont pas encore pu être analysés en détail par la Direction de la santé. Néanmoins, au vu de l'ampleur du traitement et de la sensibilité des données qui y seront traitées, la Commission nationale rappelle que ces finalités doivent s'entendre strictement et que tout usage des données qui ne s'inscrirait pas dans celles-ci ne respecterait pas le principe de la limitation des finalités inscrit dans le RGPD. En ce qui concerne les catégories de données à caractère personnel, la CNPD s'interroge sur les catégories de personnes concernées dont les données sont traitées. La stratégie de test liée au Covid-19 présentée par Madame la Ministre de la Santé le 22 mai 2020[13] comporte trois différentes manières dont les tests de diagnostic PCR[14] sont utilisés au Luxembourg : de manière réactive en présence de symptômes, de manière active au profit de certaines catégories de personnes particulièrement à risque, ainsi que de manière préventive par échantillons représentatifs (« cluster prevalence studies ») pour accompagner le déconfinement.

Selon la compréhension de la CNPD de la configuration du système d'information, ce dernier contiendra les données relatives à deux différentes catégories de personnes concernées :

- Les personnes infectées, donc celles qui ont été testées positives au virus SARS- CoV-2, soit suite à un test prescrit par un médecin en présence de symptômes, soit suite à un test ayant eu lieu de manière active au profit de certaines catégories de personnes particulièrement à risque ou de manière préventive pour accompagner le déconfinement (les « cluster prevalence studies », le projet d'étude CON-VINCE et le « large scale testing »).
- La CNPD comprend qu'en combinant les dispositions de loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique, ainsi que l'article 9 paragraphe (2) du projet de loi n°7606, les médecins, les médecins-dentistes, les responsables de laboratoires d'analyses médicales, les établissements hospitaliers, les structures d'hébergement et les réseaux de soins sont obligés de transmettre les données relatives aux personnes infectées ou présumées infectées au Covid-19 à la Direction de la Santé. Néanmoins, pour des raisons de clarté, elle propose d'énumérer de manière exhaustive les différentes sources de données dans le corps du texte de l'article 9 paragraphe (2) du projet de loi n°7606.
- Les personnes présumées infectées, c'est-à-dire celles visées par une des situations prévues à l'article 2 point 4[15] du projet de loi n°7606. Dans ce contexte, la CNPD se pose une question concernant le système du « contact tracing » qui, à l'heure actuelle, est effectué de manière manuelle au Luxembourg. Il ressort des explications contenues sur le site du

[13] Communiqué de presse du 22 mai 2020 du Ministère de la Santé et du Ministère de l'Enseignement supérieur et de la recherche : « COVID-19 - Une stratégie de test ambitieuse et au service de la santé publique », disponible sous: https://gouvernement.lu/dam-assets/documents/actualites/2020/05-mai/Communique-de-presse-depistage-2252020-.pdf.

[14] Test de diagnostic (qRT-PCR) (real-time polymerase chain reaction) utilisé au Luxembourg et reposant sur un prélèvement par écouvillon réalisé au niveau nasal (naso-pharyngé) ou par la bouche (oro-pharyngé), à la recherche du matériel génétique du virus à partir du prélèvement.

[15] Visant les différentes situations quand une personne devient une « personne présumée infectée ».

gouvernement luxembourgeois dédié au Corona virus[16] que l'objectif poursuivi par ledit système de traçage est de s'assurer que les personnes qui ont eu des contacts à haut risque avec une personne dont l'infection est confirmée, donc les personnes présumées infectées, se mettent en auto-quarantaine afin de tenter de rompre la chaine de transmission du virus. La Commission nationale se demande néanmoins quelle est la source des données à caractère personnel des personnes présumées infectées et comment celles-ci auront connaissance de leur obligation de se mettre en quarantaine. Est-ce que la personne infectée communique les données d'identification (nom, prénom, n° de téléphone, etc.) des personnes présumées infectées à la Direction de la santé qui les insérera dans le système d'information et les contactera par la suite ? Ou est-ce que, par contre, la personne infectée contactera directement les personnes présumées infectées, ces dernières étant dans ce cas obligées de se manifester de leur propre gré auprès de la Direction de la santé qui insérera qu'à ce moment-là leurs données dans le système d'information afin de pouvoir les suivre? Dans le cas de figure où la source est la personne infectée qui transmet les données à la Direction de la santé, la CNPD constate que cette source n'est pas énumérée au paragraphe (2) de l'article 9 du projet de loi. Le cas échéant, il y aurait lieu de rajouter au texte la personne infectée comme source, tout comme il faudrait rajouter, le cas échéant, le numéro de téléphone à la liste des données qui peuvent être traitées, dans la mesure où cette donnée est la plus efficace et la plus rapide pour contacter les personnes.

La CNPD part de l'hypothèse que les données de tous les individus dont le test a été négatif, hormis la catégorie des personnes présumées infectées, ne sont pas transmises à la Direction de la Santé par les établissements hospitaliers, les structures d'hébergement et les reseaux de soins et ne devraient, a fortiori, pas se retrouver dans le système d'information. Au cas où le système d'information contiendra néanmoins lesdites données, la Commission nationale se demande quelle serait la finalité poursuivie par ce traitement. A priori, elle est d'avis qu'aucune des finalités mentionnées à l'article 9 paragraphe (1) du projet de loi n°7606 ne permet l'enregistrement et la conservation dans le système d'information des données d'individus don't le test a été négatif (hormis de nouveau la catégorie des personnes présumées infectées). Si la finalité poursuivie est la réalisation d'études scientifiques, statistiques et/ou d'appui à la politique, et dans la mesure où il ne serait pas possible de réaliser ces traitements à partir de données anonymisées, la CNPD estime que dans ces hypothèses précises une collecte de données pseudonymisées devrait s'avérer suffisante.

Sous ces conditions, la CNPD estime que la liste des catégories de données à caractère personnel énumérées ci-dessus[17] n'est pas excessive au regard des finalités du traitement et respecte le principe de minimisation des données qui doit conduire à ne collecter que les données strictement nécessaires (article 5 paragraphe (1) lettre c) du RGPD). Par ailleurs, ladite liste de données à transférer (en plus du numéro de téléphone, le cas échéant) par les établissements hospitaliers, les structures d'hébergement et les réseaux de soins (en plus de la personne infectée comme source, le cas échéant) à la Direction de la Santé doit être considérée comme exhaustive et ne pourra pas excéder les catégories de données y mentionnées.

[16] https://coronavirus.gouvernement.lu/fr/citoyens.html.

[17] Nom, prénom, adresse, date de naissance, diagnostic médical, date des 1ers symptômes et date du diagnostic médical, date de prélèvement et origine du prélèvement, pays où la maladie a été contractée et la source d'infection si connue.

2. Quant à la durée de conservation
L'article 5 paragraphe (1) lettre (e) du RGPD prévoit que les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ». Il ressort par ailleurs du considérant (45) du RGPD que lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il devrait appartenir au droit de l'Union ou au droit d'un Etat membre d'établir, entre autres, la durée de conservation des données. De plus, comme déjà susmentionné, l'article 5 paragraphe (1) lettre (b) du RGPD prévoit que les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ».
Ainsi, la durée de conservation doit être déterminée en fonction de l'objectif ayant conduit à la collecte des données en cause. Une fois cet objectif atteint, ces données devraient être supprimées ou anonymisées (afin notamment de produire des statistiques).
L'article 9 paragraphe (5) du projet de loi n°7606 dispose que les données à caractère personnel des personnes infectées ou présumées infectées seront conservées dans le système d'information sous une forme permettant l'identification des personnes pendant « la durée nécessaire pour prévenir et combattre le Covid-19 et les données sont anonymisées au plus tard six mois après que la loi cesse de produire ses effets. »
A priori, la loi en projet sous examen entrera en vigueur le lendemain de sa publication au Journal officiel du Grand-Duché de Luxembourg pour une durée d'un mois (article 13 du projet de loi n°7606). Les auteurs du projet de loi expliquent dans l'exposé des motifs que la particularité du projet de loi repose sur son applicabilité dans le temps et qu'elle produira des effets a priori uniquement du 25 juin 2020, fin de l'état de crise, au 25 juillet 2020.
Dans le commentaire de l'article 13 du projet de loi il est précisé que « la situation sanitaire en relation avec la propagation du Covid-19 est en constante évolution ce qui explique la durée d'application limitée de la présente loi. » La Commission nationale comprend dès lors que l'état de la crise sanitaire sera réévalué avant le 24 juillet 2020 et en fonction des résultats, elle suppose que la Chambre des députés pourra, le cas échéant, décider de prolonger l'applicabilité de la loi en cause.
Il ressort de ce qui précède qu'il y a un double délai de conservation des données : le premier délai étant celui de la fin d'applicabilité de la loi (a priori le 24 juillet 2020 mais en fonction des circonstances, ce délai pourrait être étendu comme susmentionné) et le deuxième délai se situe six mois après la fin du premier délai.
Le commentaire de l'article 9 du projet de loi n°7606 précise dans ce contexte qu'« eu égard aux finalités du système d'information, la durée de conservation des données nominatives contenues dans le système est limitée à la durée de la gestion de la pandémie, augmentée d'une durée de six mois pour traiter d'éventuelles demandes de traitement de données provenant d'autorités de santé étrangères ou européennes ainsi que pour traiter d'éventuelles demandes liées à la recherche scientifique, historique ou à des fins statistiques. »
La Commission nationale tient à souligner tout d'abord qu'elle ne dispose pas de l'expertise scientifique et épidémiologique nécessaire, afin d'évaluer si la conservation même des données dans le système d'information des personnes présumées infectées, mais dont le test s'avère négatif, est vraiment nécessaire dans le cadre de la lutte contre le Covid-19. En l'absence d'explications plus précises par les auteurs du projet de loi, elle ne peut pas apprécier si d'éventuels argumentations d'experts scientifiques et épidémiologiques permettent de justifier

pourquoi ces données devraient être conservées pendant un certain laps de temps.
Au regard du RGPD, il est nécessaire et primordial de définir une durée de conservation des données au sein du système d'information de la Direction de la santé qui soit proportionnée au regard de la finalité poursuivie. Partant, il est nécessaire de définir des critères objectifs permettant de justifier une durée de conservation adéquate.
Au risque de se répéter, la CNPD n'étant pas experte en matière de santé et de gestion d'épidémies, il est difficile pour elle d'évaluer s'il est proportionné, afin de combattre l'expansion du Covid-19, que les données à caractère personnel des personnes infectées et présumées infectées seront conservées dans le système d'information pendant un nombre déterminé de mois. Elle se demande néanmoins quelles sont les raisons sanitaires et/ou scientifiques qui ont amené les auteurs du projet de loi à insérer dans l'article 9 paragraphe (5) du RGPD une durée de conservation spécifique de 6 mois après que la future loi cessera de produire ses effets.
A titre de comparaison, la loi française n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions contient une disposition a priori similaire au texte proposé par le législateur luxembourgeois. En effet, l'article 11 dispose « qu'aux seules fins de lutter contre la propagation de l'épidémie de covid-19 et pour la durée strictement nécessaire à cet objectif ou, au plus, pour une durée de six mois à compter de la fin de l'état d'urgence sanitaire déclaré par l'article 4 de la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, des données à caractère personnel concernant la santé relatives aux personnes atteintes par ce virus et aux personnes ayant été en contact avec elles peuvent être traitées et partagées, le cas échéant sans le consentement des personnes intéressées, dans le cadre d'un système d'information créé par décret en Conseil d'Etat et mis en œuvre par le ministre chargé de la santé. »
Or, l'alinéa 2 de l'article 11 précité contient une précision importante, dans la mesure où « les données à caractère personnel collectées par ces systèmes d'information à ces fins ne peuvent être conservées à l'issue d'une durée de trois mois après leur collecte ». Ainsi, même si le système français en lui-même pourra fonctionner jusqu'au plus tard six mois après la fin de l'état d'urgence sanitaire, les données à caractère personnel devraient régulièrement être supprimées, voir anonymisées, trois mois après qu'elles ont été collectées.
En Belgique, l'arrêté royal n°25 du 28 mai 2020 modifiant l'arrêté royal n°18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19, est entré en vigueur le 5 juin 2020. Comme l'arrêté royal n°18 du 4 mai 2020 cessait déjà ses effets le 4 juin 2020, il a été décidé de le proroger jusqu'au 30 juin 2020. Dans le rapport au roi, la Ministre des Affaires sociales et de la Santé publique belge a précisé que « le délai pour l'effacement des données à caractère personnel serait ajusté en conséquence (le 5 juillet 2020 au lieu du 9 juin 2020) », soit une durée de conservation des données de cinq jours après la fin de validité de l'arrêté en cause.
Pour conclure, la CNPD ne peut que constater que les législateurs des pays voisins du Luxembourg ont opté dans ce contexte pour des durées de conservation beaucoup plus courtes. Or, comme susmentionné, la Commission nationale n'a pas les éléments et explications nécessaires à sa disposition pour se prononcer sur la proportionnalité d'un délai de conservation des données des personnes infectées et présumées infectées de six mois après que la loi cessera de produire ses effets.
Afin de garantir que les données ne soient pas conservées plus longtemps que nécessaire, des délais devraient être fixés soit pour leur effacement, soit pour un examen périodique. Ainsi, une alternative serait de prévoir qu'en fonction de l'évolution du Covid-19, la pertinence d'une durée de conservation a priori plus brève que six mois, fasse l'objet d'une évaluation régulière,

surtout qu'à l'heure actuelle, il n'est pas possible de prédire combien de fois et pendant quel laps de temps l'applicabilité de la loi en projet sera prolongée.

3. Quant aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites
La Commission nationale rappelle que, quel que soit le contexte d'urgence, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être apportées. L'encadrement des accès à des données de santé est essentiel dans ce contexte au regard des exigences prévues par l'article 9 paragraphe 2 lettre i) du RGPD.
En vertu de l'article 9 paragraphe (3) du projet de loi sous revue, « seuls les médecins et professionnels de la santé, nommément désignés et habilités dans le cadre de la présente loi par le directeur de la santé ou de son délégué pour détecter, évaluer, surveiller et combattre le Covid-19 sont autorisés à accéder aux données relatives à la santé des personnes infectées ou présumées infectées. » Ledit paragraphe continue en limitant l'accès aux données relatives à la santé dans la stricte mesure où il « est nécessaire à l'exécution des missions légales ou conventionnelles qui leur sont confiées pour prévenir et combattre le Covid-19. »

Etant donné le caractère sensible des données relatives à la santé, la Commission nationale ne peut qu'approuver que le cercle des personnes pouvant accéder aux données liées à la santé et le contexte dans lequel ils y accèdent est circonscrit. Il ressort de l'article 9 paragraphe (3) du projet de loi que toutes les personnes que le directeur de la santé peut habiliter à accéder au système d'information sont soumises au secret professionnel prévu à l'article 458 du Code pénal, comme il est par ailleurs exigé par l'article 9 paragraphe 2 lettre i) précité du RGPD.
L'article 9 paragraphe (5) du projet de loi requiert en plus que les « données sont traitées dans des conditions permettant d'en garantir la sécurité, la confidentialité et l'intégrité. » Au vu de la nature et du volume des données traitées ainsi que des risques pour les personnes en cas d'atteinte à la sécurité des données, la CNPD estime incontournable que des mesures de sécurité technique et organisationnelle adéquates soient mises en place afin de garantir un niveau de sécurité à l'état de l'art du secteur de la santé.
A cet égard, la CNPD tient à souligner l'importance de l'obligation de sécurité prévue à l'article 5 paragraphe (1) lettre f) et à l'article 32 du RGPD, exigeant que des mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, soient mises en place. Elle considère que la mise en œuvre du traitement de données à caractère personnel contenues dans le système d'information devra en particulier garantir le recours à une authentification forte des personnes ayant accès et ledit système devrait être doté d'un traçage (journalisation) individuel des accès pendant une durée de cinq ans à partir de l'enregistrement du log, ce qui constitue une garantie supplémentaire en matière de protection des données à caractère personnel. Il est également primordial que les données soient détruites irréversiblement après l'expiration du délai de conservation.

4. Quant aux droits des personnes concernées
Le paragraphe (4) de l'article 9 du projet de loi précise que « les droits des personnes concernées prévus par le règlement général sur la protection des données (UE) 2016/679 s'exercent auprès de la Direction de la santé ». Pour ce qui est de la limitation du droit d'opposition, la CNPD renvoie à ses observations ci-avant.
En vertu des articles 13 et 14 du RGPD, le responsable du traitement est obligé de fournir aux personnes concernées certaines informations lorsque des données à caractère personnel

sont collectées directement auprès d'elles ou indirectement à travers un tiers. Une information précise et adaptée devra donc être apportée aux personnes concernées dans un context sanitaire particulier.
Ainsi, en vertu de l'article 14 du RGPD, la Direction de la santé est obligée de fournir ces informations à la personne infectée, ces données provenant a priori d'un tiers (les établissements hospitaliers, les structures d'hébergement et les réseaux de soins). En ce qui concerne les données à caractère personnel relatives aux personnes présumées infectées dans le contexte du « contact tracing », il n'est pas clair si cette collecte s'effectue de manière directe par la Direction de la santé ou de manière indirecte (par exemple via la personne infectée elle-même). Dans les deux hypothèses, le droit à l'information desdites personnes est à respecter par la Direction de la santé.
Finalement, la CNPD tient à préciser qu'au moment où une personne effectue un test, elle devrait en principe déjà être informée du fait qu'en cas de résultat positif, ses données à caractère personnel seront transférées vers la Direction de la santé et y enregistrées dans leur système d'information.

Ainsi décidé à Esch-sur-Alzette en date du 8 juin 2020.
La Commission nationale pour la protection des données

United Kingdom, House of Commons and House of Lords, Joint Committee on Human Rights. Human rights and the Government's Response to Covid-19: Digital Contact tracing, 7th May 2020.

House of Commons and House of Lords, Joint Committee on Human Rights. Human rights and the Government's Response to Covid-19: Digital Contact tracing. Third Report of Session 2019-21
Report, together with formal minutes relating to the report
Ordered by the House of Commons to be printed 6 May 2020
Joint Committee on Human Rights
The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders.
The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

Current membership
House of Commons
Ms Harriet Harman QC MP (*Labour, Camberwell and Peckham*) (Chair)
Fiona Bruce MP (*Conservative, Congleton*)
Ms Karen Buck MP (*Labour, Westminster North*)
Joanna Cherry QC MP (*Scottish National Party, Edinburgh South West*)
Mrs Pauline Latham MP (*Conservative, Mid Derbyshire*)
Dean Russell MP (*Conservative, Watford*)
House of Lords
Lord Brabazon of Tara (*Conservative*)
Lord Dubs (*Labour*)
Baroness Ludford (*Liberal Democrat*)
Baroness Massey of Darwen (*Labour*)
Lord Singh of Wimbledon (*Crossbench*)
Lord Trimble (*Conservative*)

Powers
The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Committee staff
The current staff of the Committee are Miguel Boo Fraga (Senior Committee Assistant), Samantha Granger (Deputy Counsel), Shabana Gulma (Specialist Assistant), Zoe Grunewald (Media Officer), Katherine Hill (Committee Specialist), Eleanor Hourigan (Counsel), Lucinda Maer (Commons Clerk), and George Webber (Lords Clerk).

Contents

Summary

The Covid-19 pandemic presents significant challenges for governments across the world. In addressing the virus, the Government is required to protect the right to life, guaranteed by Article 2 of the European Convention on Human Rights (EHCR). The UK, like many countries, has sought to protect the right to life by enforcing "lockdowns" which have placed severe restrictions on individuals' movements, with significant and wide-ranging implications for human rights.

The UK Government now has plans to release a contact tracing app as part of its strategy to "test, track and trace to minimise the spread of Covid-19 and move towards safely reducing lockdown measures."1 The app would notify individuals who may have been exposed to the virus to take the appropriate action such as to self-isolate or to get tested. If effective, a contact tracing app could pave the way out of current lockdown restrictions, enabling individuals to move around more freely whilst helping to prevent the spread of the virus.

However, any such app will have an impact on the right to private and family life, protected under Article 8 of the ECHR. If a contact tracing app enables people to move around freely and safely, and is accompanied with the sufficient protections, then the risk to privacy could be a more proportionate interference with individuals' human rights than current restrictions imposed by the lockdown. However, there are significant concerns about a tracking app being rolled out at speed with the potential longer-term effects on personal freedoms and concerns around surveillance encroaching on people's everyday lives. Such an app must not be rolled out nationally unless strong safeguards and protections are in place. It is not clear that the current legal and regulatory arrangements provide satisfactory, indeed the necessary, legal oversight required. State-controlled apps that enable the mass

surveillance of personal data, and that could then enable the (proportionate or otherwise) violation of fundamental rights are novel. The introduction of such an app is an innovative apparatus of state interaction with its citizens. The implications of such an app are so widespread, significant, and, as yet, subject to limited public examination, that they should be subject to the in-depth scrutiny of Parliament at the earliest opportunity. The Committee is concerned that this has not happened to date.

Previous extensions of state powers of surveillance and data collection for the purposes of terrorism prevention have been legitimised by legislation scrutinised by Parliament; and so, it should be for public health purposes.

Having a carefully considered legislative basis for this app would better engender public trust and participation.

Legislation would require a formal human rights assessment to take place. This degree of formal rights balancing is lacking at present, being left to the NHSX team and its advisory bodies. In particular, Parliamentary scrutiny would allow for consideration as to whether the use of a centralised system, as opposed to a decentralised system, is reasonable and proportionate. The implementation and oversight of this app must, in our view, be urgently placed on a legislative footing; if rolled out without being governed by a clear legislative framework it risks not complying with the provisions of the ECHR.

In our view, a contact tracing app must not be rolled out nationally unless there are guarantees with respect to:

- Efficacy and proportionality: Unless the efficacy and benefits of the app are clear, the level of data being collected will be not be justifiable and it will therefore fall foul of data protection law and human rights protections. The Science and Technology Committee has been focussing on this and our Committee will focus on the necessary privacy protections. However, the app will not be as effective if uptake is low and uptake is likely to be lower without user confidence in privacy protections—so we consider that the privacy protections are themselves key to the effectiveness of the app.

- Primary legislation: The Government's assurances about intended privacy protections do not carry any weight unless the Government is prepared to enshrine these protections in law. Any data gathering by the app must be accompanied with the appropriate guaranteed protections for personal data to ensure the impact on privacy is minimised as far as possible. Privacy protections applicable to the contact tracing app must be placed on a legislative footing. This would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app; increase uptake; and therefore improve the efficacy.

- Oversight: There should be an independent body to oversee the use, effectiveness and privacy protections of the app and any data associated with this contact tracing. The independent monitoring body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how the app is working. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions.

- Child safeguarding: In all aspects of usage of the app, children under 18 must be given protection and support as expressed in the UN Convention on the Rights of the Child (UNCRC), the ECHR and in domestic legislation.2 Children and parents should be given information and training in the use of the app and reassurances about safety.

- Efficacy review: The Health Secretary must undertake a review every 21 days of the app's efficacy, as well as the safety of the data and how privacy is being protected in the use of

any such data. The Health Secretary must report to Parliament on the conclusions of each review.

• Transparency: The Government and health authorities must at all times be transparent about how the app, and data collected through it, is being used, including publishing ethics reviews and sufficient technical specification information relating to the app and to data security.

Introduction

What is contact tracing?

1.Covid-19 emerged in late 2019 in the city of Wuhan in Hubei province, China. Its origins are yet to be confirmed. It spread quickly through the population in Wuhan and to slow transmission the Chinese Government implemented a strict "lockdown" of the city and later the province. As the virus spread internationally, other countries introduced their own lockdowns, although the restrictiveness of the measures varied and few matched the intensity of the Chinese approach.

2.South Korea avoided imposing a blanket lockdown through a mass testing regime and tracing the contacts of those who had been infected so they could self-isolate and break the chain of transmission. This included the use of a contact tracing app but was combined with extensive manual contact tracing. With just 255 deaths as of 5 May 2020, and daily life largely proceeding as normal, it is widely recognised that much can be learnt from South Korea's response.

3.The Government announced on 5 May 2020 that the UK had passed 29,000 confirmed deaths from Covid-19, a similar amount to Italy and second only behind the United States in terms of the total death toll. The privacy concerns about the contact tracing app are certainly pertinent to human rights, especially Article 8, which protects the right to private and family life. However, Governments also have a responsibility to protect Article 2 ECHR, the right to life. If the app demonstrably protects lives and can help to ease the constraints of a lockdown, then this is a very relevant factor in assessing the proportionality of any interference with the right to a private life under article 8 ECHR. However, any contact tracing must only interfere with the right to privacy to the strict extent necessary to achieve its objectives of combatting the disease, so robust privacy protections will be important and where exactly the line is drawn is a matter of debate.

4.Contact tracing is one way of trying to control and track the spread of the virus. It involves notifying individuals when they have come into contact with others who may have been exposed to the Covid-19 virus and giving them appropriate advice, for example to get tested and or to self-isolate, in order to minimise the further spread of the virus. Several countries are using smartphones to speed up the process of contact tracing.

5.Digital contact tracing generally works by an app on a user's smartphone registering and storing details of another smartphone when it is within a defined distance for a certain period of time and if a user tests positive for (or is suspected of having) the virus, the app notifies these contacts that they may themselves be affected. There are a number of different approaches to digital contact tracing which have been discussed at length by academics in recent weeks. Some of the key differences, which have implications for privacy, are discussed briefly below.Different models/approaches which exist

A centralised or decentralised approach?

6.A major area of discussion around the development of the app has been whether the

NHSX should adopt a "centralised" or "decentralised" approach to data storing and sharing. The two models are explained briefly below:

- Decentralised models: most data is stored locally on an individual's phone and as little data as possible is shared with the NHS.
- Centralised models: data is shared with a central server managed by the authority which carries out data processing and/or storage.3

The Information Commissioner's Office, privacy experts and organisations, as well as the European Parliament and the European Data Protection Board (EDPB) have indicated a preference for a decentralised approach.4 It is considered that this would provide greater protection against the abuse of people's data than apps which pull data into centralised pots and have a higher risk of security breaches as well as being much more invasive into the private lives of individuals. There are heightened risks with centralised models with their "potential to de-anonymise data and develop profiles of individuals' social interactions."5 However, it is asserted that a centralised approach has "public health advantages," in that, it allows health authorities to analyse how the virus is spreading. In turn that allows them to help prevent the spread of the virus (and therefore deaths caused by it), to allow hospitals in virus hotspots to prepare for a surge in cases, and to lessen the invasive nature of the lockdown provisions to the extent possible. It also allows them to improve the efficacy of the app in future versions.

7.The developers of the NHS tracking app have stated that the purpose for choosing a centralised database model over the more data-secure and private de-centralised model is that it allows for greater data analysis. It is not clear that the additional functionality of a centralised data system outweighs the risks inherent in such a model. Such risks may include:

- Less secure data storage (privacy) due to a centralised server.
- Greater incentives to hack centralised databases.
- Identifier numbers are permanent records of one individual, unlike in most de-centralised systems.
- The functionality of a centralised model, if preferred for the benefit of increased analysis, could encourage more data being requested from users in the future, 'mission creep'.Issues with compatibility with de-centralised systems (notably the Republic of Ireland) used in the majority of other countries, as recognised by NHSX.

8.It has been noted that the UK is an outlier. While giving evidence to the Committee, Matthew Gould and Dr Michael Veale, lecturer in Digital Rights and Regulation, University College London, both accepted that the technical difficulties of switching the current model to a de-centralised system were manageable.7 The NHS tracking app asks for post code area information. In some parts of England there are less than 10,000 people in a post code area. Three or four 'bits' of information can be can enough to identify individuals. If NHSX were to add location data to the current model, could easy and consistent individual identification become possible, especially with a centralised data system? The Committee expresses concern that the centralised model is being proposed without there having been the opportunity for Parliamentary debate and consideration of the alternative.

Self-reporting or diagnoses and testing?

9.Another difference between approaches is how to notify the app of an infection. This could be done via self-reporting into the app; by uploading confirmation of an approved

test; or health authorities themselves uploading results onto the app server. Relying upon self-reporting alone may carry the risk of false alerts, thereby impacting on other people's rights if they have to isolate unnecessarily.

Voluntary or mandatory

10.Another area of discussion has been around whether a contact tracing app should be voluntary or mandatory to use. The Information Commissioner, the European Data Protection Board (EDPB) and other privacy experts have indicated that the use of contact tracing applications should be voluntary.8 The EDPB have said that this would imply that "individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all."9 Some academics in the UK have called for protection for groups who do not have access to smartphones to ensure that they are not penalised for not using the app.

The UK's plan to release a contact tracing app

11.The UK Government is going ahead with its plans to release a contact tracing app. A Government press release dated 4th May 2020 contained details of the first phase of the Government's "test, tack and trace programme," which includes roll out of the NHS Covid-19 App in the Isle of Wight. The Government's intention is to use the app as a tool to "minimise the spread of Covid-19 and move towards safely reducing lockdown measures."11

12.We took evidence from Matthew Gould, CEO of the NHSX, the Information Commissioner, Dr Orla Lynskey and Dr Michael Veale and others on the UK's plan to release a contact tracing app.12 We are grateful for their evidence. We were also assisted by a specialist advisor Adam Wagner with this inquiry.

NHSX's current approach to the app

13.The NHSX app will use the centralised model for data storage and sharing. It will work by logging the distance between an individual's phone and other phones nearby that also have the app installed using Bluetooth Low Energy. Unless a user becomes ill, this log will be stored on an individual's phone and the data deleted every 28 days. Matthew Gould, Chief Executive of NHSX, told us that users who become ill will then have the choice to upload the information from the app onto the central server. Users will also be able to give their anonymous contacts to the central database which will identify which contacts are at risk and notify them accordingly. It will also allow the NHS to use the anonymised data to understand how the virus is spreading.

Concerns with the current approach

14.While a recent poll has shown that 65% of people in the UK are in favour of having an app to track the virus, a number of privacy concerns remain with the approach being adopted by the UK. The main concerns with the NHSX's current approach are outlined below:

- Efficacy and proportionality—there is a lack of evidence that a contact tracing app would be an effective tool in suppressing the virus.14 Concerns have been expressed as to whether the contact tracing app will work on a technical level. Moreover there are significant concerns around interoperability with other countries systems, with particular concerns on the interoperability of systems on the island of Ireland. If it interferes with privacy rights but is too ineffective to fulfil its objective, then the interferences with the right to private life will not be proportionate.
- Mission creep—there are concerns that given NHSX's plans to upgrade the app in "future releases", there will be a risk of creating systems that can be changed incrementally, thus

changing the privacy protections upon which the data was initially collected and shared. If that happens, vital privacy protections, and safeguards might be undermined. The capacity to include location data is a concern as it could reveal sensitive information, including relating to third parties.

• Purpose of data use and data retention—Matthew Gould has noted that the "data will only ever be used for NHS care, management, evaluation and research". There are concerns that this is a broad and unclear purpose and may extend beyond preventing the spread of Covid-19.15 Matthew Gould in evidence said data shared with the NHS 'can be retained for research in the public interest or for use by the NHS for planning and delivering services', the latter potentially opening the way for sharing a) within government beyond the NHS and b) with private companies. Matthew Gould also said in evidence that data submitted to the NHS database will not be deleted and could be used in an anonymised form for research purposes. If data is held indefinitely even in an anonymised form, then this raises data protection concerns not least due to data reconstruction risks (i.e. that 'anonymised' data is used to identify individuals) and is likely to affect uptake of the app. The risk of data reconstruction may be enhanced by the fact that users of the app will be required to enter the first half of their postcode. Need for legislation and oversight—Several academics and organisations have called for legislation to provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. There are also calls for proper oversight mechanisms to monitor efficacy, impact on privacy and other rights.

• Human rights framework

15.The overall Government response to Covid-19 raises core human rights considerations. In addressing the virus, the Government is required to protect the right to life, guaranteed by Article 2 of the European Convention on Human Rights (EHCR). In doing so, many countries, including the UK have placed severe restrictions on individuals' movements by enforcing "lockdowns", which themselves have wide ranging implications for human rights. The lockdown measures are a significant interference with the right to family and private life, (Article 8 of ECHR), the right to free movement (Article 12 International Covenant on Civil and Political Rights 1966), freedom of assembly and association (Article 11 ECHR), freedom of religion or belief (Article 9 ECHR), the peaceful enjoyment of possessions (Article 1 of Protocol 1 ECHR) and the right to education (Article 2 of Protocol 1 ECHR). One way of easing lockdown restrictions is to seek to contain the virus through a variety of other techniques including digital contact tracing, which itself will interfere with the right to private life (Article 8 ECHR) as well as requiring a very careful analysis of compatibility with data protection and privacy law.

16.In the UK privacy law is protected by Article 8 ECHR, the common law duty of confidence, the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (which has equivalent protections to the GDPR under the "UK GDPR" that will succeed the GDPR after Brexit transition).

17.The seven data protection principles under the GDPR (and mirrored by the UK GDPR) provide a basis for considering the issues which need to be addressed before an app is released:

a)Data minimisation: The processing of personal data should be limited to what is necessary.

b)Purpose limitation: organisations need to be clear about the purposes for processing data from the start of data processing and collection. This must be specified in privacy information provided to individuals.

c)Storage limitation: Personal data must not be kept for longer than is necessary for the purposes for which the personal data is processed.
d)Integrity and confidentiality: Appropriate security measures must be in place to protect personal data e.g. from accidental breaches.
e)Lawfulness, fairness and transparency: Personal data must be processed in a transparent manner and data organisations must be clear about how they will use personal data.
f)Accountability and accuracy: Organisations must take responsibility for what they do with personal data and must take all reasonable steps to ensure that personal data held is not incorrect.19

Our proposals
Efficacy and proportionality
18.The lockdown itself constitutes an interference in the human rights of individuals and is currently justified by the need to protect human life. It is appropriate that the Government is exploring options to save lives and to ease the restrictions caused by lockdown. The app's contribution to reducing the severity of the lockdown and to helping to prevent the spread of Covid-19 must be demonstrated and improved at regular intervals for the collection of the data to be reasonable. This is the basis on which any discussion around the privacy concerns must proceed: if the digital contact tracing system does not work, or only has a minimal effect, the collection of huge amounts of data is indefensible.
19.The amount of data the contact tracing app requires on the private and family lives of individuals is not justifiable if the app does not contribute meaningfully to the easing of lockdown restrictions and the combatting of Covid-19. Digital contact tracing will not be as effective if uptake is low. Uptake will be lower without user confidence in privacy protections—therefore robust privacy protections are themselves key to effectiveness of the app and the digital contact tracing system. Interoperability with other countries' systems will also be relevant to efficacy, not least to ensure that there is interoperability of systems in use on the island of Ireland. The Republic of Ireland has elected to use a decentralised app and if a centralised app is in use in Northern Ireland, there are risks that the two systems will not be interoperable which would be most unfortunate.
Privacy and other Human Rights Protections
20.The Heath Secretary has informed us that he has appointed an independent Ethics Advisory Board. That is welcome but insufficient. There needs to be established by law and with sufficient powers a Digital Contact Tracing Human Rights Commissioner who would not only exercise oversight with the appropriate powers but also be able to deal with any complaints from the public and report to Parliament.
21.The Government must not roll out the contact tracing app nationally unless the following protections are in place:
a)Primary legislation: Government assurances about intended privacy protections for any data collected do not carry any weight unless the Government is prepared to enshrine these protections in legislation. A Bill would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app, increase uptake, and improve efficacy.
b)Oversight: There should be an independent body, such as a Digital Contact Tracing Human Rights Commissioner, to oversee the use, effectiveness and privacy protections of the app and any data associated with digital contact tracing. The independent monitoring

body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how data collected is being used and protected. To guard against mission creep it cannot be left to the Information Commissioner's Office to be the only body with powers of oversight or sanction; such an Office is not designed to monitor the significant rights-based implications that app based surveillance raises and, in addition, the Information Commissioner has been involved in the development of the app. Matthew Gould in his evidence to the Committee stated "However, we do not yet know exactly how it will work; we do not know all the consequences. There will be unintended consequences and there will certainly be some things that we have to evolve." In light of this, the speed of piloting and intended roll out, it is imperative that an independent oversight body be established immediately. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions.

c)Child Safeguarding: Particular safeguards should be applied to children under 18. Children's use must be monitored in relation to data collection and use of data. Misuse must be identified and rectified promptly. Interviews with children and parents (where appropriate) must take place in order to support children and act on any concerns.

d)Efficacy review: The Health Secretary must undertake a review every 21 days on the digital contact tracing system. Such reviews must cover efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data. The Health Secretary must report to Parliament every 21 days on the findings of such reviews.

e)Transparency: The Government and health authorities must be transparent about how the app, and data collected through it, is being used. The Data Protection Impact Assessment must be made public and updated as digital contact tracing progresses.

f)Time-limited: Any digital contact tracing (and data associated with it) must be permanently deleted when no longer required and in any event may not be kept beyond the duration of the public health emergency.

Legislation

22.Once the app's utility is demonstrated, we recommend that the data and other human rights protections should be placed on a legislative footing. This would further improve efficacy by increasing uptake.

23.The current data protection framework is contained in a number of different documents and it is nearly impossible for the public to understand what it means for their data which may be collected by the digital contact tracing system. Government's assurances around data protection and privacy standards will not carry any weight unless the Government is prepared to enshrine these assurances in legislation. Such a Bill must include the following provisions and protections:

a)Set out the clear and limited purposes of this app for data processing: Personal data may only be collected and processed for the purpose of preventing the spread of Covid-19. No personal data collected through the digital contact tracing app may be accessed for any other purpose. No personal data collected through the digital contact tracing app may be shared with third parties. There should be prohibition against data use for certain purposes such as legal proceedings, to support or deny benefits, data sharing with employers.

b)Unless an individual has notified that they have Covid-19 (or have suspected Covid-19) and has chosen to upload their data, all personal data should only be held locally on the user's device and must be automatically deleted entirely from the app every 28 days.

c)Any personal data held centrally (e.g. following a diagnosis of Covid-19 or suspected Covid-19) must be subject to the highest security protections and standards.
d)Limit who has access to data and for what purpose: Data held centrally may not be accessed or processed without specific statutory authorisation, for the purpose of combatting Covid-19 and provided adequate security protections are in place for any systems on which this data may be processed.
e)Data held centrally may not be used for data reconstruction (i.e. where different pieces of anonymised personal data are combined to reconstruct information about an individual through piecing together multiple data sets).
f)Data held centrally must be deleted where a user so requests and may not be held for longer than is required and in any event for no longer than 2 years. All data collected must be deleted once the public health emergency is over.
g)The Minister must undertake a review and report to Parliament on the efficacy and privacy protections relating to digital contact tracing every 21 days.
h)Powers for a Digital Contact Tracing Human Rights Commissioner to ensure that authority has sufficient powers, staff and resources to oversee the roll-out of digital contact tracing, to look into individual complaints, to make binding recommendations on data protection, collection, storage, safety and use.
24.Furthermore the introduction of this app raises issues that go beyond data protection and privacy. Other human rights which are protected under the Human Rights Act 1998 (HRA) and ECHR are engaged, for example, the right to non-discrimination in employment and immigration matters. The declaration of compatibility with the HRA which would be required to accompany legislation would put the framework for the app on a firmer rights-based footing and ensure protection of all the rights engaged.
25.There might be concerns that legislating could entail delays which would be undesirable since a key objective is to safely ease the lockdown as soon as possible. But legislation enshrining assurances in law is perfectly viable in time for the national roll out in the middle of this month. Parliament was able quickly to agree to give the Government sweeping new powers in the Coronavirus Act. If Parliament is able to swiftly enact legislation to confer powers it can do so to circumscribe them. The parties were able to agree that legislation and it should be possible to agree legislation to describe and circumscribe the contact tracing app expeditiously. The law could provide flexibility for any future changes which become necessary by enshrining the principles in primary legislation and the particulars in secondary legislation, which are easier to change but which still have the force of law.

Conclusions and recommendations

Efficacy and Proportionality

1.The amount of data the contact tracing app requires on the private and family lives of individuals is not justifiable if the app does not contribute meaningfully to the easing of lockdown restrictions and the combatting of Covid-19. Digital contact tracing will not be as effective if uptake is low. Uptake will be lower without user confidence in privacy protections—therefore robust privacy protections are themselves key to effectiveness of the app and the digital contact tracing system. Interoperability with other countries' systems will also be relevant to efficacy, not least to ensure that there is interoperability of systems in use on the island of Ireland. The Republic of Ireland has elected to use a decentralised app and if a centralised app is in use in Northern Ireland, there are risks that the two systems will not be interoperable which would be most unfortunate. (Paragraph 19)

Privacy and Other Human Rights Protections
2.There needs to be established by law and with sufficient powers a Digital Contact Tracing Human Rights Commissioner who would not only exercise oversight with the appropriate powers but also be able to deal with any complaints from the public and report to Parliament. (Paragraph 20)
3.*The Government must not roll out the contact tracing app nationally unless the following protections are in place*:
a)*Primary legislation: Government assurances about intended privacy protections for any data collected do not carry any weight unless the Government is prepared to enshrine these protections in legislation. A Bill would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app, increase uptake, and improve efficacy*.
b)*Oversight: There should be an independent body, such as a Digital Contact Tracing Human Rights Commissioner, to oversee the use, effectiveness and privacy protections of the app and any data associated with digital contact tracing. The independent monitoring body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how data collected is being used and protected. To guard against mission creep it cannot be left to the Information Commissioner's Office to be the only body with powers of oversight or sanction; such an Office is not designed to monitor the significant rights-based implications that app based surveillance raises and, in addition, the Information Commissioner has been involved in the development of the app. Matthew Gould in his evidence to the Committee stated "However, we do not yet know exactly how it will work; we do not know all the consequences. There will be unintended consequences and there will certainly be some things that we have to evolve." In light of this, the speed of piloting and intended roll out, it is imperative that an independent oversight body be established immediately. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions*.
c)*Child Safeguarding: Particular safeguards should be applied to children under 18. Children's use must be monitored in relation to data collection and use of data. Misuse must be identified and rectified promptly. Interviews with children and parents (where appropriate) must take place in order to support children and act on any concerns*.
d)*Efficacy review: The Health Secretary must undertake a review every 21 days on the digital contact tracing system. Such reviews must cover efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data. The Health Secretary must report to Parliament every 21 days on the findings of such reviews*.
e)*Transparency: The Government and health authorities must be transparent about how the app, and data collected through it, is being used. The Data Protection Impact Assessment must be made public and updated as digital contact tracing progresses*.
f)*Time-limited: Any digital contact tracing (and data associated with it) must be permanently deleted when no longer required and in any event may not be kept beyond the duration of the public health emergency*. (Paragraph 21)
Legislation
4.The current data protection framework is contained in a number of different documents and it is nearly impossible for the public to understand what it means for their data which may be collected by the digital contact tracing system. Government's assurances around data protection and privacy standards will not carry any weight unless the Government is prepared to enshrine these assurances in legislation. *Such a Bill must*

include the following provisions and protections:
a)*Set out the clear and limited purposes of this app for data processing: Personal data may only be collected and processed for the purpose of preventing the spread of Covid-19. No personal data collected through the digital contact tracing app may be accessed for any other purpose. No personal data collected through the digital contact tracing app may be shared with third parties. There should be prohibition against data use for certain purposes such as legal proceedings, to support or deny benefits, data sharing with employers*.
b)*Unless an individual has notified that they have Covid-19 (or have suspected Covid-19) and has chosen to upload their data, all personal data should only be held locally on the user's device and must be automatically deleted entirely from the app every 28 days*.
c)*Any personal data held centrally (e.g. following a diagnosis of Covid-19 or suspected Covid-19) must be subject to the highest security protections and standards*.
d)*Limit who has access to data and for what purpose: Data held centrally may not be accessed or processed without specific statutory authorisation, for the purpose of combatting Covid-19 and provided adequate security protections are in place for any systems on which this data may be processed*.
e)*Data held centrally may not be used for data reconstruction (i.e. where different pieces of anonymised personal data are combined to reconstruct information about an individual through piecing together multiple data sets)*.
f)*Data held centrally must be deleted where a user so requests and may not be held for longer than is required and in any event for no longer than 2 years. All data collected must be deleted once the public health emergency is over*.
g)*The Minister must undertake a review and report to Parliament on the efficacy and privacy protections relating to digital contact tracing every 21 days*.
h)*Powers for a Digital Contact Tracing Human Rights Commissioner to ensure that authority has sufficient powers, staff and resources to oversee the roll-out of digital contact tracing, to look into individual complaints, to make binding recommendations on data protection, collection, storage, safety and use*. (Paragraph 23)

United Kingdom Information Commissioner's Opinion (ICO), Apple and Google joint initiative on Covid-19 contact tracing technology 2020/01, 17 April 2020

Summary

The Information Commissioner (the Commissioner) has previously provided guidance to organisations and to individuals regarding aspects of personal data processing and COVID-19.

This Opinion sets out the Commissioner's current thinking regarding a joint initiative by Apple and Google (which we are calling the Contact Tracing Framework (CTF)) to enable the use of Bluetooth technology to help governments and public health authorities (PHAs) reduce the spread of the virus.

Key messages

- The proposals for the CTF itself appear aligned with the principles of data protection by design and by default. This is based on the understanding that the CTF is designed to:

only generate a limited amount of data from the user's device, that is then made available via the CTF application programming interface (API). This data includes periodically-generated cryptographic tokens (we have used the term 'tokens' for clarity, noting that the Apple and Google documentation calls these numbers 'identifiers') created on that device, and stored tokens collected from nearby devices via Bluetooth. Tokens are not associated with other data that may further identify or locate the device user; and

support the use of these tokens as part of a specific methodology for contact tracing, through their upload from a COVID-19 diagnosed user to a central server and subsequent notification to other app users from that server, with this process only matching tokens stored on a particular device (with the match only occurring on the device), if it had been in the proximity of the diagnosed user's device.

- The CTF is therefore intended to support the development of apps that protect their users' identities, both before any risk of infection has been identified and when a COVID-19 infection notification is made via the app.
- However, it will be possible for those developing COVID-19 contact tracing apps — anticipated to be whitelisted PHAs and similar organisations — to design apps that use the CTF but also collect other data and use other techniques beyond those envisaged by the CTF.
- Organisations designing contact tracing apps are responsible for ensuring the app complies with data protection law where it processes personal data and the organisations are the controllers for that data. This is especially important because individuals may believe that the data protection by design and by default principles used in the development of the CTF extend to all aspects of a contact tracing app that is built to use the CTF, which may not necessarily be the case. If the app processes data outside the CTF's intended scope, then the controller should ensure it assesses the data protection implications of this processing (along with any undertaken by way of the CTF) and ensure that the processing is fair and lawful. It is also crucial that the processing is transparent.
- The Commissioner notes that the CTF's underlying principles are similar to the proposed 'Decentralized Privacy-Preserving Proximity Tracing' ('DP-3T') system. While this Opinion is about the CTF, where these similarities exist the Commissioner's views are equally applicable to the DP-3T proposals.

- This is a fast moving and highly complex situation. Apple and Google have stated that they acknowledge the CTF initiative is an ongoing project, that will doubtless evolve over time. There are also plans for a 'Phase 2' of the work that could see additional functionality. The Commissioner will remain engaged in this work as it continues.
- The Commissioner is pleased that the hard work, innovation and collaboration of many different parties is enabling these vitally important contact tracing solutions to be developed, while supporting data protection compliance and good practice. She agrees that apps should espouse robust security (including the use of encryption, and covering each stage of the data processing), data minimisation, transparency and user control, and that any supporting technology, including centralised processing to support contact tracing, should follow the same principles. She believes this work to be evidence that innovation and data protection are complementary concepts. The Commissioner will continue to promote and support data protection best practice across all initiatives seeking to address the COVID-19 pandemic.

About this Opinion

What is the status of this Opinion?

Section 115(3)(b) of the Data Protection Act 2018 (DPA 2018) allows the Commissioner to issue Opinions to Parliament, Government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

The Commissioner can issue Opinions on her own initiative or on request.

The Opinion represents the Commissioner's view at the time of publication. It is based on the publicly available information about the CTF and the joint communications made by Apple and Google on 10 April 2020 (see Further Reading at the end of this Opinion), and only pertains to 'Phase 1' of the project as outlined in those documents.

The Commissioner reserves the rightto make changes, publish new Opinions or form a different view based on further findings or other changes in circumstances.

Who is this Opinion for?

This Opinion is primarily for organisations involved in the CTF's development, as well as organisations developing apps that may use the CTF and other stakeholders that wish to understand the Commissioner's position on this initiative. It may also be of interest to those involved in other contact tracing initiatives.

What is the purpose of this Opinion?

This Opinion summarises the Commissioner's view of the joint initiative by Apple and Google to enable the use of Bluetooth technology to help governments and health agencies use contact tracing to reduce the spread of COVID-19.

Background
COVID- 19 contact tracing
Contact tracing techniques seek to ascertain whether any individual has been in contact with an infected person during the time they were possibly infectious. Contact tracing could be used to support prompt communications with individuals who may be at risk of infection to ensure they:

- are aware of the risk;
- are provided with the appropriate information;
- take the appropriate steps to protect themselves and others; and
- receive any other support they may need.

Contact tracing has the potential to be used effectively as part of a package of measures and policies to manage social distancing and social or professional gatekeeping. It may therefore enable any potential measures that would support the easing of lockdown or other restrictions (eg immunity verification or immunity passport proposals).
The Commissioner understands that a number of these proposals are being advanced, and recommends that there is transparency around initiatives that link to COVID-19 tracing apps and that any solution is privacy-preserving in nature.
Contact tracing may be undertaken manually, relying on information provided by the infected person and others regarding their movements and interactions, during the time they may have been infectious.
Recently, there has been substantial focus on the possibility of supporting traditional contact tracing using automated tools, including the functionality available to many people on their mobile devices (eg their smart phone), as a means of addressing the COVID-19 pandemic.

The Google and Apple initiative
On 10 April, Apple and Google announced they would be launching:

'a comprehensive solution that includes application programming interfaces (APIs) and operating system -level technology to assist in enabling contact tracing [...] in May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These official apps will be available for users to download via their respective app stores.'

The CTF is not itself a contact tracing app, and Google and Apple are not yet proposing to build such an app, although they have indicated that they intend to develop more functionality into their solution. For now, the aim is to enable third parties, such as PHAs, to create contact tracing apps that exchange information via Bluetooth Low Energy between devices.
A simple explanation of how an app is envisaged to work has been provided by Google and Apple. (The Commissioner notes that this explanation includes Google's terminology for the proposals, which slightly differs from the terminology in this Opinion).

Discussion
The first part of the following discussion deals with the CTF itself and the second with contact tracing apps that may be developed using the CTF.

Assessment of the CTF
Data minimisation

The CTF appears, based on this initial review, to comply with the data minimisation principle. Our review suggests:

- the exchange of information between devices does not include personal data such as account information or usernames;
- matching processes take place on-device and are notundertaken by the app host or with the involvement of any other third party; and
- the information required for the core functionality of contact tracing apps built using CTF does not use location data, either in the exchange between devices, the upload to the app host or subsequent notifications to other users from the app host.

However, the CTF provides the possibility for app developers to process more information than may be required for contact tracing purposes. This is discussed below.

User control over apps built using the CTF

The Commissioner notes that in the contact tracing proposals seen so far, app installation is voluntary and the post-diagnosis upload of stored tokens to the app developer requires a separate consent process.

Any app built using the CTF will be provided via the applicable mobile Operating System (OS) app store, and is subject to the same requirements as any other app within that app store. In addition, users have the ability to remove or disable the app. However we understand that in the 'Phase 2' plans the CTF API will form part of each mobile device's OS. This means that even a mobile device user who removes or disables an app will not be able to easily refuse or remove OS updates that continue to provide the CTF API, which enables apps to use this data. The Commissioner is not suggesting that they need to, but that this should be noted.

The user can also disable Bluetooth on their device. The Commissioner observes that, with regard to the possible development of Phase 2 of the CTF, and also with regard to the development of contact tracing apps in general, and as with other cases where the onus is on a user to protect against being tracked, a user should not have to take action to prevent tracking.

Additionally, the Commissioner notes that more general considerations are required regarding the implications for individual rights and freedoms if the user chooses to not disable Bluetooth (or indeed uninstalls, or does not install, the apps envisioned here), particularly in terms of future proposals for immunity testing and immunity passports or access to services.

Security

As for the security principle, it appears that under the CTF, the exchange of information between devices and the upload of information to the app host incorporate a number of security measures. The CTF documentation indicates the use of appropriate cryptographic functions with additional safeguards. Cryptographic techniques are a means of mitigating risks to the security of the data being processed, for example:

- the generation of tokens takes place on the device and is not under the

control of the contact tracing app utilising the API, using cryptographic techniques to ensure that information broadcast to other devices is not directly related to an identifiable individual. The exchange of tokens between devices do not indicate COVID-19 status, therefore the device-to-device level exchange of information does not directly result in app users knowing who has been diagnosed. While there may be circumstances where an individual could determine the identity of a diagnosed user (eg if they had only been in recent contact with a few people they know), these measures address risks about identification in circumstances such as public spaces;

- if a user is diagnosed they can voluntarily upload the stored tokens on their device to the app host (eg a PHA) via an encrypted communications channel. The app host in turn lets other app users know that they may be at risk because they had recently been in close proximity to the diagnosed user, but this does not directly identify the diagnosed individual. While this is not intended to enable users to look up the tokens of COVID-19-positive users, the Commissioner understands that this may be possible, but only for a technically advanced attacker in specific circumstances, meaning this risk appears low;
- the second-stage transfer of data to the app host is likely to be undertaken via transport layer security (TLS), as is the case with most other contact tracing proposals, particularly given the requirements of the two mobile operating systems; and
- no persistent user ID is broadcast. Instead, a sequence of pseudo-random tokens representing changing user IDs are broadcast.This means that the risk of identifying a user from the interaction between phone A and phone B in the moment is likely to be low.

This analysis is limited to the information provided so far; the Commissioner may provide additional assessment of the security measures of any cloud-based infrastructure in due course.

Purpose limitation and risks of scope creep

Purpose limitation is a core principle of data protection internationally. It is about limiting use of personal data to the purpose for which it was collected or purposes compatible with that purpose. As indicated earlier, the CTF is a very new initiative and there are already signs that it will continue to evolve. Third-party app developers may also develop functionality that involves collection of additional data or new uses of existing data. This risks expanding the use of CTF-enabled apps beyond the stated purpose of contact tracing for COVID-19 pandemic response efforts. The Commissioner will monitor all developments, with an eye to ensuring that this purpose does not expand outward, in the phenomenon known as scope creep.

Current alignment with the proposed DP-3T system

The CTF is a joint initiative of Apple and Google and is not directly associated with the DP-3T initiative of a separate expert group. However, the underlying principles of the CTF appear to be similar to those proposed in the DP-3T protocol. The similarities between the two projects give the Commissioner further comfort that these approaches to contact tracing app solutions are generally aligned with the principles of data protection by design and by default.

The Commissioner has not undertaken a detailed technical review of the proposed DP-3T system. As noted above, the review of the CTF is based on the information made available on 10 April 2020. As such, there may be differences in the detailed approach undertaken by the two proposals. In addition, as the two initiatives have different stakeholders and governance, they may further diverge over time. However, at the date of publication of this Opinion the Commissioner believes that a number of the points included in this Opinion regarding the CTF are equally applicable to the DP-3T protocol.

Observations about contact tracing apps that use the CTF

This part of the Opinion offers observations about key issues raised by third-party development of tracing apps using CTF as the API foundation. These observations are not exhaustive and, as noted elsewhere, the Commissioner will consider the facts of each case in assessing compliance.

Roles of the app developer and the body controlling the contact tracing scheme, as controllers

The CTF as a technical matter enables development of apps that process more information than may be necessary for contact tracing purposes.

The CTF documentation says that while the 'standard' means of operation does not use location data, it may be possible for app developers to do so, but that 'any use of location data is completely optional to the schema'.

The Commissioner acknowledges that the processing of additional data by apps that use the CTF may be legitimate and permissible. This may be needed to support the public health utility of a tracing app, and would need to be assessed on a case-by-case basis. For example, it may be necessary to process data to restrict the uploading of diagnosis keys by users, to ensure the system is not flooded with false positives. A more expansive example of where additional functionality beyond contact tracing could be sought would be to assess compliance with isolation.

Where additional data processing takes place, a separate assessment of data protection considerations will need to be made by the controller, which may involve a separate data protection impact assessment if the threshold criteria are met.

Privacy information, lawful basis and consent management

While the existence of multiple different actors within the mobile app ecosystem likely means that data protection obligations rest upon multiple parties, the primary responsibility for providing privacy information rests with app developers (who create apps; this may include organisations, who outsource the actual app design to a third party) and app stores (who make apps available to users), particularly where app developers are also controllers. This is however no different to normal apps.

While Google and Apple's app stores mandate specific requirements for the privacy information that apps must provide, it is at present not clear whether this would mean contact tracing apps utilising the CTF must include information relating to the CTF.

As stated above, the Commissioner understands that most current proposals for contact tracing apps would rely on consent as the lawful basis for processing any personal data, and that installation of the apps is also voluntary. However, the Commissioner also notes that at the present time some matters remain unclear and must be addressed before being rolled out.

First, it is not yet clear how the CTF will facilitate the collection of consent for the upload of stored tokens to the app host, although we are advised that the CTF will require the specific consent of the user at this point.
Second, it is not clear how an app utilising the CTF will manage this consent signal and how the CTF and an app may between them provide control to users. Last, it is unclear what impact consent withdrawal may have both on the effectiveness of contact tracing solutions and any notifications provided to other app users once an individual is diag nosed. Each of these matters will have to be addressed moving forward.

User awareness and perception

It is possible that many users of a contact tracing app will have neither the time nor the expertise to determine that the CTF is facilitating the collection of some data from their devices, or that any app using it was designed by another party.
There is a risk that individuals believe that the data protection by design and by default principles incorporated by the CTF extend to all aspects of a contact tracing app that uses the CTF. If the app processes data outside the scope of what the CTF intends to cover, then the controller should ensure it has also assessed the data protection implications of this processing (along with the processing it undertakes using the CTF), ensuring that the processing is fair, lawful and transparent.
However, the responsibility cannot solely be placed on the user. While the Commissioner welcomes the transparency already shown by Google and Apple in this proposal, use of the CTF by apps must be documented and auditable, and any controller processing personal data has to comply with data protection law.
The Commissioner is a reasonable and pragmatic regulator, and does not operate in isolation from matters of serious public concern. Regarding compliance with data protection, the Commissioner will take into account the compelling public interest in the current health emergency.
Controllers should refer to the ICO's guidance on COVID-19 that reflects this position.

Considerations outside of the scope of this Opinion

The scope of this Opinion is limited to consideration of the design of the CTF. A range of other concerns and considerations may arise pertaining to the broader area of COVID-19 contact tracing. For example, there may be more components of a contact tracing scheme that could give rise to other concerns for controllers, such as the association of other data generated by an app with centralised data held by the PHA or others, or measures taken by the PHA or Government to encourage or mandate use of the app. These will need consideration on a case by case basis as they arise.

Conclusions

The CTF is aligned with the principles of data protection by design and by default
The Commissioner has considered the concerns and considerations regarding the CTF, and believes the CTF is aligned with the principles of data protection by design and by default, including design principles around data minimisation and security.

Contact tracing apps that use the CTF should align with the principles of data protection by design and by default whenever personal data is processed
At present, the CTF is limited to the development of APIs and technical specifications for Apple and Google's mobile operating systems to facilitate the development of

contact tracing apps on both platforms. Such apps may process other sets of personal data to support additional functionality. Each controller designing an app is responsible for ensuring the app is compliant with law and regulation.

Clarification is needed for app users around who is responsible for data processing
Many users of a contact tracing app will have neither the time nor the expertise to understand that the CTF is facilitating the collection of some data from the device, but that the app itself was designed by another party.
There is a risk that individuals believe that the data protection by design and by default principles being utilised by the CTF extend to all aspects of a contact tracing app utilising the CTF. If the app processes data outside the CTF's intended scope, however, the controller responsible must ensure it has also assessed the data protection implications of this processing (along with any it undertakes using the CTF), and ensure that it is compliant. It is equally important that this controller be transparent with potential and actual app users, noting the data protection principles of transparency and accountability.

Further questions are likely to arise over time

The COVID-19 pandemic continues to pose unique and urgent challenges to all aspects of society. This is a fast moving and complex situation, and it is likely that additional questions regarding the use of technology and data for contact tracing will arise over time. This much is clear given the acknowledgement by Apple and Google that the CTF is will likely evolve over time. There are indications, for example, of a Phase 2 of the work that would see additional functionality. Moreover, other contact tracing proposals exist, such as the proposed DP-3T system. As noted above, third parties are likely to develop contact tracing apps that use the CTF and may also separately process personal data.
Development of these apps may give rise to broader questions, such as around additional functionality within the app itself or the use of other personal data sets to promote or mandate usage of a particular contact tracing app. Existing ICO guidance will be sufficient to address many questions that developers and controllers may have, but the Commissioner will continue to identify ways to support controllers with questions about the processing of personal data during the COVID-19 pandemic.

Next steps

As suggested earlier, the Commissioner will carefully consider developments in this area, and may choose to issue further Opinions or other statements to address aspects of personal data processing during the COVID-19 pandemic.

United Kingdom Information Commissioner's Opinion (ICO), COVID-19 Contact tracing: data protection expectations on app development, Statement, 4th May 2020

COVID-19 Contact tracing: data protection expectations on app development

Purpose

This document sets expectations on how contact tracing solutions may be developed in line with the principles of data protection by design and default, and includes a series of best practice recommendations.

Audience

The expectations outlined below have been developed to support technical design teams (architects, product managers, designers, engineers) in understanding how to apply information rights and data protection by design and default approaches to the technical development lifecycle of COVID-19 contact tracing apps. Risk management professionals, including those working in privacy and data protection, information security, compliance and operational risk may also benefit from this document.

Scope

This is a discussion document that has been provided by the Information Commissioner's Office (ICO) to supplement ongoing conversations between the ICO and NHSX regarding its planned contact tracing app and associated activities.

The ICO recognises the importance of the app as one part of a package of measures in the UK's fight against the COVID-19 pandemic, while recognising that an app cannot be used to address all the challenges of supporting citizens appropriately, especially those who don't have smartphones, or members of society that may be vulnerable or disadvantaged.

Our role as an independent regulator is to act in the public interest, and our approach has always been to be a pragmatic and proportionate regulator. We appreciate the effort NHSX has made to maintain a dialogue with the ICO whilst having to move at speed in addressing complicated technological and epidemiological challenges.

This document provides further detail on our understanding of privacy and data protection considerations around contact tracing apps, and our articulation of best practice recommendations in this area.

For the purposes of this document, a contact tracing app is considered to be a mobile application which functions to notify users when they have been in recent proximity with another user who has confirmed symptoms of COVID-19 (whether via official or self-diagnosis). It uses 'proximity data' which consists of identifiers broadcast by pairs of devices that have been close to each other (possibly including how close they were, and for how long). One typical approach involves generating identifiers and the matching process taking place on-device, while another involves these processes being driven by the backend infrastructure. In popular parlance these have become known as 'decentralised' and 'centralised' approaches, although both may include a server.

Any additional functions or features, such as recording/communicating the location in which contact has taken place, or collection of additional data that may support other functions (such as epidemiological research) is considered beyond the core functionality needed for contact tracing via proximity detection, notwithstanding the value additional functionality may offer medical professionals in combatting COVID-19, and will need to be assessed on a case-by-case basis.

This document has been drafted to support our ongoing conversation with NHSX. We appreciate this is a fast moving project; we are happy to discuss any aspect of this document with NHSX and its stakeholders.

Compliance with data protection law

Any assessment of the data protection implications of a contact tracing app must be undertaken on a case-by-case basis and therefore the specific implementations may require additional measures and considerations beyond the scope of these recommendations.

The ICO considers that a Data Protection Impact Assessment (DPIA) is required for contact tracing solutions prior to implementation, given that the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA may also need to iterate over time, particularly in accordance with any Product or Project roadmaps and functionality/scope updates and releases. The principles and expectations below therefore do not replace a DPIA, however they can be used to support its completion.

Principles

The following principles should guide the development of your contact tracing app. They are linked to the core principles and provisions of data protection law and are designed to support your design decisions and key considerations for documentation, accountability and auditability.

You should consider how to apply these principles throughout the lifecycle of the contact tracing app or service.

1. Be transparent about the purpose: Explain if the purpose is only proximity notification or if the purpose is broader, or is likely to expand in accordance with any development roadmap. Explain any additional purposes clearly and make sure you assess the necessity and proportionality of the processing the app undertakes. Ensure your considerations address all relevant parties - for example, build core requirements into your notices, user experience (UX) design and other appropriate in-app transparency mechanisms, but also provide more detailed information about your app's development outside of the app itself.
2. Be transparent about your design choices: Be clear about the system's architectural design decisions, how they were made and what risks the approach poses to individual rights. Use the least privacy intrusive approach possible to achieve your purpose and ensure you justify the design choices you make. Make the service requirements and objectives available to users and other parties.
3. Be transparent about the benefits: Be clear about the benefits and outcomes your app seeks to achieve, from both your perspective and that of the user. Where benefits for different parties may be the subject of tension, ensure that you are clear on how you have managed these in the data protection context. As part of assessing necessity and proportionality, clearly define these parties and clarify how your solution addresses each in line with data protection requirements.

4. Collect the minimum amount of personal data necessary: Minimise the data your solution processes to that which is necessary to achieve your purposes. Begin by considering whether you can generate and match identifiers on-device. Where this approach is available, feasible, and enables you to achieve your purposes, then you should use it. If you decide to use an alternative approach, you must be able to explain why it is necessary to do so, as well as the steps you will take to ensure you will not introduce unnecessary risks to the user. Contact tracing apps should

only collect or otherwise process information that is required for the core purpose (e.g. excluding location data, other device identifiers beyond any that are strictly necessary for the purpose, and personal data such as user account information, etc.). As noted above the collection and processing of personal data for other purposes will need to be assessed on a case-by-case basis.

5. Protect your users: Ensure your app uses pseudonymous identifiers, which are renewed regularly as appropriate to your purposes, and are generated in such a way that risks of reidentification and tracking are reduced.

6. Give users control: Ensure your users can exercise their rights via your app, where these rights apply. Provide controls while onboarding and during use, e.g. via a dedicated privacy control panel or dashboard.

7. Keep data for the minimum amount of time, and, where appropriate, ensure the user has control over this: Store data for the minimum amount of time necessary for your purposes. Explain what that period will be and why. Avoid gathering, augmenting or correlating user data without express permission.

8. Securely process the data: Apply appropriate cryptographic/security techniques to secure the data, both at rest (in servers and apps) and in transit (between apps and the server). Ensure confidentiality, integrity and availability has been engineered into the service.

9. Ensure the user can opt in or opt out without any negative consequences: App use, from installation to sharing of information, should be voluntary with no negative consequences for individuals if they do not take action. Functions should be de-coupled to allow the user to benefit from one function without being compelled to provide data for other functions.

10. Strengthen privacy, don't weaken it: Ensure the design of the app does not introduce additional privacy and security risks for the user (for example requiring the phone to be unlocked, or location to be identified).

Consider how to test functional and non-functional requirements or use cases and user journeys that are being developed against these principles on a continuous development basis - for example including testing against these principles to determine the impact on the user, as part of any sprint planning and retrospectives.

Best practice recommendations

The following best practice recommendations are grouped under a development lifecycle. While these (and any references to document types) may not align with the process your organisation uses, the key point to recognise is that there are data protection obligations during the ideation and design phase, when on boarding and operating any service, when iterating any service, and when decommissioning any service.

It may also be the case that different parties may be responsible for specific aspects of the processing. For example, developers of a contact tracing app may only be responsible for collecting information from the user, while a different party may be responsible for its analysis. However, even in these circumstances it is incumbent upon the developers of a contact tracing service, particularly where acting on behalf of a public health authority, to take steps to ensure that:

- data is not used for analysis or for other purposes in ways that may detrimentally affect information rights and privacy; and
- data use does not lead to other significant decisions about the user without the

user's permission or understanding that this is the case.
This responsibility can be met in part through the design of privacy protections into the technical approach of the service, including clear privacy and security objectives and controls, and by ensuring that all involved parties are clear on their respective responsibilities.
While this document comprises good practice recommendations, from a design perspective the key words 'must', 'must not', 'required', 'shall', 'shall not', 'should', 'should not', 'recommended', 'may' and 'optional' are to be interpreted as described in RFC 2119. These are used to aid translation of the requirements of data protection law.

Scope, requirements and design

1. Contact tracing app initiatives must describe the objectives they seek to achieve. This must include articulating if the benefit is directly for the user and/or if the benefit is for a broader societal purpose. Being transparent on the objectives, requirements and future plans will help to build trust amongst all stakeholders, especially users.

a. Within any product roadmap or description of objectives and requirements (epics, stories) articulate how the user will understand, e.g. through the experience and interface design, that their privacy has been engineered into the project. Make sure your design choices enable you to clearly tell your users about any uses of their data that may be unexpected or could have significant effects on them, and if there are any residual privacy risks.

b. Publish the product roadmap and user needs/journeys, as well as any supporting documentation, code or collateral that explains the requirements, scope, approach and risk management controls.

2. Contact tracing apps must exclude further processing for purposes unrelated to the primary aim, as explained to the user. The purposes must be specific enough to exclude other unrelated purposes. Personal data beyond that necessary for contract tracing purposes must not be processed merely because it may become useful in the future.

a. Describe how you have assessed what the minimum amount of data (and types of data) are that you have to collect and process to enable proximity detection.

b. Detail the technical and design controls you will put in place to ensure data collection doesn't expand during any further development without user engagement.

3. Contact tracing apps may develop roadmaps for additional functionality involving personal data; in such cases, a documented re-assessment of the data protection implications is required.

a. Describe the product roadmap in a way the user can understand, both in general and with specific reference to any implications for their privacy rights. Ensure any technical or policy decisions are explained to the user in an accessible way.

b. Describe as part of the development of the roadmap how features could lead to privacy challenges and what control measures have been considered.

c. Consider how to functionally decouple features. Ensure users are not compelled to share additional data to access existing features or new features, and to allow any features to be rolled back or deprecated.

4. Processing of personal data may be based on consent or an alternative lawful basis where this is more appropriate, such as performance of a task in the public interest (particularly where an app is developed by or on behalf of a public health authority). For the latter, the processing must be necessary; if you could reasonably

perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply. The voluntary use of an app does not mean that processing has to be consent-based. However, where the processing is based on consent, that consent must be collected in line with the requirements of data protection law.

5. The consent requirement of Regulation 6 of the Privacy and Electronic Communications Regulations 2003 ('PECR') does not apply in relation to storage of information, or access to information stored, on user devices where this is strictly necessary for the provision of a contact tracing service the user requests (e.g. exchange of proximity data and receipt of push notifications). Where storage and access is not strictly necessary, valid consent must be obtained. Consideration of this requirement must take place on a case-by-case basis.

a. Consider how to separate out storage/access to user devices that is strictly necessary from that which is not, where this applies. Where strictly necessary, establish how you will obtain prior consent from the user.

6. App developers should break down the processing operations involved in their proposed contact tracing apps into their individual components and assess necessity and proportionality, the lawful basis and user impact, of each one. Design should incorporate the ability to functionally decouple each discrete process.

a. Consider how to offer proximity notification to a user as a minimum product feature, with any other features layered on top with simple mechanisms for the user to opt in or out without feeling compelled.

b. Consider architecting your data model and data pipelines to allow clear separation between processing that is taking place, and to clearly link the functional (experience) layer with the data and processing enabling it.

c. Document and demonstrate how you have achieved this, and what technical and policy controls have been put in place to validate the separation of processing and experience.

7. Source code must be open to allow scrutiny and review.

a. Consider how you will implement established code management and publication principles, such as those in the GDS Service Manual (or other relevant guidelines as appropriate).

8. The design stage must consider the most appropriate architectural design to achieve the purpose from the user's perspective. As a general rule, the decentralised approach allows most readily for best practice compliance with the data minimisation principle.

a. How might you separate out elements of the service that rely on personal data so that they are developed and deployed using a decentralised model, especially if this is sufficient to achieve the core purpose of proximity notification?

b. As the technology and modelling capability of end point devices evolves, how might you transition the product roadmap from a centralised approach to a decentralised approach – where the decentralised approach offers greater privacy protections?

9. A DPIA must be completed prior to the commencement of the processing, and updated at all relevant stages of your app's development. Where a DPIA identifies risks to users that you cannot mitigate, you must submit it to the ICO for prior consultation. The ICO

will expedite the consultation process for any such DPIA we receive.
a. Consider how to ensure the technical development lifecycle and product updates trigger the right thresholds for refreshing the DPIA, and what you can do to build this into the sprint cycle.

Development, deployment, onboarding and operation

10. Contact tracing apps should adopt a user centric design approach, even if the circumstances of the current pandemic mean the development lifecycle is compressed.
a. Consider how to test for different user needs, taking special consideration for different societal groups that may be vulnerable, disadvantaged, or require accessibility support.
b. Consider how to build technical and policy controls to ensure users, especially children, vulnerable adults, and other at risk members of society are treated fairly.
11. Contact tracing apps must not involve or require the processing of location data, or the tracking of the location of users either directly or by inference. Proximity data must be used; as contact tracing apps do not require location data to fulfil their purpose, any processing of this data is therefore not necessary and poses additional privacy risks. The app and backend infrastructure must not directly identify users or process other information from the device such as call logs, device identifiers (beyond any that are strictly necessary for the purpose), IP addresses and any other information (including personal data), as this is not required for contact tracing purposes.
12. An interoperability framework may be considered (e.g. for efficient notification of users travelling outside the UK). Data processed must be for the sole purpose of interoperability and must be limited to that which is strictly necessary for the purpose and be undertaken in accordance with applicable law.
a. Consider how your technical and design controls will mitigate the risks of personal data being shared with other third party app controllers.
b. Ensure the app only collects data transmitted by interoperability equivalent applications.
13. Use of coding libraries, frameworks, APIs, SDKs and other software components, including those within the mobile operating system, must be understood and clarified. Collection of data by third parties for other purposes must be avoided.
14. In general, information should remain on the user's device as far as is reasonably practicable. Backend infrastructure should only collect that which is strictly necessary in the context of the functions it provides.
a. What data retention technical controls are in place to manage data stored locally on the device and centrally?
15. Proximity data must comprise pseudonymous identifiers that are refreshed at regular intervals as appropriate for the purpose of the processing, as a means of limiting the risk of reidentification and of tracking individuals.
a. These pseudonymous identifiers should be generated on the device if possible. If they are generated by the backend infrastructure, you must explain why you have decided this is necessary and how you have assessed the risks of this approach.
b. Ensure that any underlying smartphone operating system APIs, e.g. for processing data via Bluetooth, are used in accordance with relevant developer documentation, app store guidelines and terms of use.
16. Retention periods must relate to the purpose of the processing and must not be disproportionate. They should be based on scientific or epidemiological considerations

(e.g. period of infection). Personal data must only be processed for the duration of the COVID-19 crisis. Afterwards, as a general rule, it should be erased or anonymised. The purposes for the use of anonymised data (e.g. future research value) must be documented. Appropriate measures must be in place to address the risk of re-identification.
a. Where a research purpose may deliver value in the public interest, any such use case should be assessed in the DPIA and discussed with the ICO.
19. Apps and servers must authenticate with each other at the transport layer, and other security protections must be considered to ensure the exchange of data protects the privacy of the user.
20. If self diagnosis is necessary, appropriate measures should be in place to mitigate the risks of false positives and the impact on the rights of those notified. For reporting test results, a separate authentication must be made e.g. a one-time password linked to the medical professional that made the diagnosis.
21. Processes must be in place to test the effectiveness of the security measures as well as to respond to any security issues, with actions taken where necessary, to ensure the security of the processing is maintained. Appropriate consideration and action must be taken to ensure common security threats are assessed and mitigated, both in respect of the backend infrastructure and the mobile app environment.
22. App developers should break down the processing operations involved in their proposed contact tracing apps into their individual components and assess necessity and proportionality, the lawful basis, and the user impact of each one. Design should incorporate the ability to functionally decouple each discrete process.
a. Consider how to offer proximity notification to a user as a minimum product feature, with any other features layered on top with simple mechanisms for the user to opt in or out without feeling compelled.
23. Processes involved in matching identifiers must be developed to mitigate risks of false positives and false negatives. Any algorithms or models deployed must be auditable and subject to regular review (e.g., by independent experts) and any necessary changes.
24. The identities, roles, and responsibilities of all parties that process personal data as part of the contract tracing solution must be clarified, documented, and made clear to the user.
25. Users must be provided with clear and comprehensive information about the data your app processes before the processing takes place. Privacy information may be made available in different ways, as appropriate to the circumstances and the reasonable expectations of individuals - including app store information, information within the app itself, user interface design, just-in-time notifications, etc.
a. How might you design simple and accessible engagement moments to explain to the user the purpose and outcome from the use of their data?
26. Collection of personal data relating to health shall be allowed only where the processing is either based on explicit consent, is necessary for reasons of public interest in the area of public health, is for health care purposes, or is necessary for scientific research or statistical purposes.
27. Apps must be designed in such a way as to enable users to access their rights as set out in the GDPR, including rights of access, erasure, restriction and rectification, as applicable.
28. Backend infrastructure must not attempt to identify infected or potentially

infected users. Access to data on the central server must be restricted to authorised individuals.
a. Develop technical, procedural and policy controls to avoid data sharing outside the operational boundary of the PHA.
b. Limit APIs, database analytics or other data exchange mechanisms to parties that are directly supporting proximity notification delivery. Where access is required for epidemiological reasons for trend/pattern analysis then consider earlier points about purpose limitation and refreshing the DPIA.

Decommissioning

29. Assessment must be made about how the functionality of the app and the backend infrastructure, and any data processed, will be deprecated once the pandemic ends. This should be made at the design stage, or alternatively may take place as part of development roadmaps.
a. How will you incorporate decommissioning into your roadmap?
b. Consider whether your app/infrastructure should be designed to dismantle itself once the crisis ends and people cease using the app, or whether specific processes are necessary.
c. What steps will be taken to erase or anonymise the data once the contact tracing purposes are no longer relevant?
d. How will you ensure your decommissioning process is independently verifiable and auditable, including to the ICO?

30. Decommissioning considerations should cover not only the 'general' retirement of the service as described above, but instances where an individual ceases to use the application.
a. Consider how you will make the decommissioning a matter of public record, and how you will inform your users (e.g. by providing messages to delete the app from their device).

31. The decommissioning process must consider the possible future use of personal data and/or any models derived for legitimate research purposes (e.g. developing responses to future outbreaks, development of models or inferences to understand epidemiological impact). Any consideration of use of data for research purposes is undertaken in accordance with data protection law, with appropriate safeguards in place.

32. Consideration should be taken after, or as part of, the decommissioning process to analyse the privacy issues raised, how risks were managed, and what lessons can be learned for the future. This can act as an overarching safeguard.
a. Consider undertaking this analysis through relevant governance groups in order to fully understand the efficacy of the approach.

The ICO will keep these recommendations under review, taking into account how the COVID-19 pandemic develops and the particular proposals under development to respond to the crisis. The ICO is open to any conversation regarding these recommendations in order to help technical teams build data protection by design and default into their service, because this is the best way to promote trust and confidence in any solution.

Bibliography

World Wide

Abeler, J., Bäcker, M., Buermeyer, U., & Zillessen, H., *COVID-19 contact tracing and data protection can go together*, in *JMIR mHealth and uHealth*, *8*(4), 2020.

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., & Al, *A survey of covid-19 contact tracing apps,* in *IEEE Access*, 2020, 8, 134577-134601.

Akinbi, A., Forshaw, M., & Blinkhorn, V., *Contact tracing apps for the COVID-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies*, in *Health Information Science and Systems*, *9*(1),2021, 1 – 15.

Alanoca, S., Guetta-Jeanrenaud, N., Ferrari, I., Weinberg, N., Çetin, R. B., & Miailhe, N. *Digital contact tracing against COVID-19: a governance framework to build trust*, in *International Data Privacy Law*, *11*(1), 2021, 3 – 17.

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., & Al *Acceptability of app-based contact tracing for COVID-19: Cross-country survey study,* in *JMIR mHealth and uHealth*, 2020, 8(8), e19857.

Amariles, D. R., *Towards Computational Indicators: Internet of Things, Data Analytics and Encoding in COVID-19 Contact Tracing Apps,* in Nelken, D., et al., *COVID-19 and the social role of indicators: a preliminary assessment,* EUI Working Paper LAW, 17, 2020, 37-45.

Arakpogun, E., et al. *Digital Contact-Tracing in a Pandemic… We Need One with a Blended Aproach*, *Available at SSRN 3639056*, 2020.

Arakpogun, E. O., Elsahn, Z., Prime, K. S., Gerli, P., & Olan, F. *Digital contact-tracing and pandemics: Institutional and technological preparedness in Africa*, in *World development*, *136*, 2020, 105105.

Ayres, I., Romano, A., Sotis, C., *How to Make COVID-19 Contact Tracing Apps work: Insights From Behavioral Economics,* available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3689805.

Bengio, Y. et al., *The need for privacy with public digital contact tracing during the COVID-19 pandemic*, in *The Lancet Digital Health*, 2 (7), 2020, e342-e344.

Berman, G., Carter, K., Herranz, M. G., & Sekara, V., *Digital Contact Tracing and Surveillance during COVID-19: General and Child-specific Ethical Issues*, Innocenti Working Papers, Unicef, 2020.

Brian, R.,Bambauer, J., *Privacy and Digital Contact Tracing*, in *Law Faculty Articles and Essays*, 2021, 1181.

Castelluccia, C., et al., *ROBERT: ROBust and privacy-presERving proximity Tracing*, in HAL Id: hal-02611265; URL: https://hal.inria.fr/hal-02611265.

Cho, H., Ippolito, S. et al., *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-off s,* (2020), https://arxiv.org/abs/2003.11511.

Clarke, L., *PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear*, IN *NS Tech*, Apr. 20, 2020; http://tech.newstatesman.com/security/pepp-ptvs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear.

Cofone, I., *Immunity Passports and Contact Tracing Surveillance,* in Stan. Tech. L. Rev., 24, 2021, 354 ss.

Dubov, A., & Shoptawb, S. *The value and ethics of using technology to contain the COVID-19 epidemic,* in *The American Journal of Bioethics*, 2020, 20(7), W7-W11.

Epifani, S., *Pedinamento digitale e democrazia della sorveglianza,* in Crampi A. (a cura di), *Dopo. Come la pandemia può cambiare la politica, l'economia, la comunicazione e le relazioni internazionali,* Rubbettino Editore, 2020, 59-69.

Ferretti, L., Wymant, C., et al., *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing,* in *Science* 10.1126/science. abb6936 (2020).

Floridi, L., Mind *the App - Considerations on the Ethical Risks of COVID-19 Apps*, in *Philosophy & Technology*, 33, 167 – 172, 2020.

Greenwood, D., et al., *Commentary on COVID-19 Contact Tracing Privacy Principles,* in *MIT Computational Law Report,* 2020.

Hatamian, M., Wairimu, S., Momen, N., & Fritsch, L., *A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps*, in *Empirical Software Engineering*, *26*(3), 2021, 1 – 51.

Hoffman, A. S., Jacobs, B., van Gastel, B., Schraffenberger, H., Sharon, T., & Pas, B., *Towards a seamful ethics of Covid-19 contact tracing apps?*, in *Ethics and Information Technology*, 2020, 1-11.

Ivers, L.C., & Weitzner, D.J., *Can digital contact tracing make up for lost time?,* in *The Lancet Public Health*, *5*(8), 2020, e417-e418.

Jalabneh, Rawan and Zehra Syed, Haniya and Pillai, Sunitha and Hoque Apu, Ehsanul and Hussein, Molla Rashied and Kabir, Russell and Arafat, S.M. Yasir and Azim Majumder, Md. Anwarul, *Use of Mobile Phone Apps for Contact Tracing to Control the COVID-19 Pandemic: A Literature Review*, July 1, 2020, Doi.org/10.1016/j.arcmed.2020.05.015, Available at SSRN: https://ssrn.com/abstract=3641961 or http://dx.doi.org/10.2139/ssrn.3641961.

Joo, J., & Shin, M.M. *Resolving the tension between full utilization of contact tracing app services and user stress as an effort to control the COVID-19 pandemic*, in *Service Business*, *14*(4), 2020, 461-478.

Kahn, J., Hopkins, J., *Project on Ethics and Governance of Digital Contact Tracing Technologies. Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance,* Johns Hopkins University Press, 2020.

Klar, R., & Lanzerath, D., *The ethics of COVID-19 tracking apps–challenges and voluntariness,* in *Research Ethics*, 2020, 16(3-4), 1-9.

Kleinman, R. A., & Merkel, C. *Digital contact tracing for COVID-19*, in *CMAJ*, *192*(24), 2020, E653-E656.

Klenk, M., & Duijf, H. *Ethics of digital contact tracing and COVID-19: who is (not) free to go?*, in *Ethics and information technology*, 2020, 1-9.

Kritikos, M., *Ten technologies to fight coronavirus,* EPRS, Brussels, 2020.

Kuner, C., *Data Crossing Borders,* in *Verfassungsblog.de,* 15-4-2020.

Laudato, S., et al., *Intelligenza artificiale e* Big Data*: l'arma in più contro il Covid-19?,* in *Oltre la Pandemia. Società, salute, economia e regole nell'era* post *Covid 19,* G. Palmieri (a cura di), Editoriale Scientifica, 2020, vol. II, 1617-1632.

Lawson-Tancred, H., Price, H.C.W., Provetti, A., *COVID-19 Contact Tracing: Eight Privacy Questions Explored A Reply to de Montjoye et al.,* May 20, 2020, Available at SSRN: https://ssrn.com/abstract=3607089 or http://dx.doi.org/10.2139/ssrn.3607089.

LI, J., Guo, X., *Global Deployment Mappings and Challenges of Contact-tracing Apps for COVID-19,* May 24, 2020, Available at SSRN: https://ssrn.com/abstract=3609516 or http://dx.doi.org/10.2139/ssrn.3609516.

Liu, J.K., et al., *Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach,* in *IACR Cryptol. ePrint Arch.*, 2020, 528.

Lucivero, F., Hallowell, N., Johnson, S., Prainsack, B., Samuel, G., & Sharon, T. *Covid-19 and Contact Tracing Apps: Ethical challenges for a social experiment on a global scale*, in *Journal of bioethical inquiry*, 2020, 17(4), 835-839.

Marhold, K., Fell, J., *Format Wars Hampering Crisis Response – The Case of Contact Tracing Apps During COVID-19*, May 16, 2020, Available at SSRN: https://ssrn.com/abstract=3598143 or http://dx.doi.org/10.2139/ssrn.3598143.

Mbunge, E., Fashoto, S. G., Batani, J., *COVID-19 Digital Vaccination Certificates and Digital Technologies: Lessons from Digital Contact Tracing Apps*, 2021). Available at SSRN: https://ssrn.com/abstract=3805803 or http://dx.doi.org/10.2139/ssrn.3805803.

McGregor, L., *Contact-tracing Apps and Human Rights,* in *Ejiltalk.org,* 30 April 2020.

Melosi, L., Rottner, M., *Pandemic Recessions and Contact Tracing*, FRB of Chicago Working Paper No. 2020-31, 2020, Available at SSRN: https://ssrn.com/abstract=3734491.

Monroe, C., Tazi, F., & Das, S. *Location Data and COVID-19 Contact Tracing: How Data Privacy Regulations and Cell Service Providers Work In Tandem*, in *Proceedings of the Workshop on Usable Security and Privacy (USEC),* 2021.

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. *Ethical guidelines for COVID-19 tracing apps,* in *Nature,* 582 (7810), 2020.

Munzert, S., Selb, P., Gohdes, A., Stoetzer, L.F., & Lowe, W., *Tracking and promoting the usage of a COVID-19 contact tracing app,* in *Nature Human Behaviour*, 2021, *5*(2), 247-255.

Narayanan, H.T.S., *Contact Tracing with Bluetooth LE - A Status Review*, in *International Journal of Latest Trends in Engineering and Technology*, 15 (5), 2020.

Nesterova, I., *The global flood of COVID-19 contact tracing apps: sailing with human rights and data protection standards against the wind of mass surveillance,* in *SHS Web of Conferences,* 92, 2021, 01035.

Nijsingh, N., van Bergen, A., & Wild, V. *Applying a precautionary approach to mobile contact tracing for Covid-19: The value of reversibility*, in *Journal of Bioethical Inquiry*, *17*(4), 2020, 823 – 827.

Oliva, Jennifer, *Surveillance, Privacy, and App Tracking*, in Burris, S., de Guia, S., Gable, L., Levin, D.E., Parmet, W.E., Terry, N.P. (Eds.), Assessing Legal Responses to COVID-19, Boston: Public Health Law Watch, 2020.

Parker, M.J., Fraser, C., Abeler-Dörner, L., & Bonsall, D., *Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic,* in *Journal of Medical Ethics*, 2020, 46 (7), 427 – 431.

Raman, R., Achuthan, K., Vinuesa, R., & Nedungadi, P., *COVIDTAS COVID-19 Tracing App Scale—An Evaluation Framework*, in *Sustainability*, 2021, 13(5), 2912.

Ranisch, R., et al., *Digital contact tracing and exposure notification: ethical guidance for trustworthy pandemic management*, in *Ethics and information technology*, 2020, 1-10.

Resta, G., *Data and Territory. The impact of the "local" in the regulation of digital technologies and algorithmic decision-making,* in Essays in Honour of Mads Andenas, forthcoming.

Restrepo-Amariles, D., *From Computational Indicators to Law into Technologies: The Internet of Things, Data Analytics and Encoding in COVID-19 Contact Tracing Apps*, in *International Journal of Law in Context* (Forthcoming), 2021, Available at SSRN: https://ssrn.com/abstract=3751126.

Rowe, F., *Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world*, in *International Journal of Information Management*, *55*, 2020, 102178.

Sato, M., *Why some countries suspended, replaced, or relaunched their covid apps*, in MIT Technology Review, December 23, 2020; https://www.technologyreview.com/2020/12/23/1015557/covid-apps-contact-tracing-suspended-replaced-or-relaunched/.

Savona, M., *The Saga of the Covid-19 Tracing Apps: What Lessons for Data Governance?,* SPRU Working paper series, n. 10/2020, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3645073.

Scassa, T., Millar, J., Bronson, B., *Privacy, Ethics, and Contact-tracing Apps*, in C.M. Flood, V. MacDonnell, J. Philpott, S. Thériault and S. Venkatapuram, (eds.), *Vulnerable: The Law and Policy of COVID-19*, Ottawa Faculty of Law Working Paper, 23, 2020.

Sharon, *T. Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers*, in *Ethics and Information Technology*, 2020, 1 – 13.

Shubina, V., Ometov, A., Basiri, A., & Lohan, E. S. *Effectiveness modelling of digital contact-tracing solutions for tackling the COVID-19 pandemic*, in *The Journal of Navigation*, 2021, 1-34.

Spina, A., Cattuto, c., *The institutionalisation of Digital Pubblic Health: lessons learned from the COVID-19 app,* in European Journal of Risk Regulation, 11, 2020, 228–235.

Tamar, s., *Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers,* in *Ethics and Information Technology,* 2020.

Trotogott, R. L. *A Comparative Analysis of Data Privacy Impacted by COVID-19 Contact Tracing in the European Union, the United States, and Israel: Sacrificing Civil Liberties for a Public Health Emergency*, in *ILSA J. Int'l & Comp. L.*, *27*, 2020, 55.

Walrave, M., Waeterloos, C., & Ponnet, K., *Adoption of a contact tracing app for containing COVID-19: a health belief model approach*, in *JMIR public health and surveillance*, 2020, 6(3), e20572.

Wendehorst, C., *Covid-19 Apps and Data Protection,* in E. Hondius et al., *Coronavirus and the Law in Europe,* Intersentia, 2020, accessible at: https://www.comparativecovidlaw.it/2020/09/02/covid-19-apps-and-data-protection/.

Whitelaw, S.,et al., *Applications of digital technology in Covid-19 pandemic planning and response,* in 2 *Lancet Digital Health* 435 (2020).

Zastrow, M., *Coronavirus contact-tracing apps: can they slow the spread of COVID-19?,* in *Nature,* 19 May 2020.

European Union

Aa. Vv., *Coronavirus Pandemic In The Eu – Fundamental Rights Implications: With A Focus On Contact-Tracing Apps,* European Union Agency for Fundamental Rights, 2020.

Bradford, L., Aboy, M., & Liddell, K. *COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes*, in *Journal of Law and the Biosciences*, 2020, 7(1), lsaa034.

Cattuto, C., & Spina, A., *The institutionalisation of digital public health: lessons learned from the COVID-19 app*, in *European Journal of Risk Regulation*, *11*(2), 2020, 228-235.

Ciucci, M., Gouardères, F., *National COVID-19 contact tracing apps*, in IP/A/ITRE/2020-0, European Parliament, Directorate-General for Internal Policies, May 2020. http://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL.

Greer, S., & de Ruijter, A. *EU health law and policy in and after the COVID-19 crisis,* in *The European Journal of Public Health*, *30*(4), 2021, 623.

Greely, H. T., *COVID-19 immunity certificates: science, ethics, policy, and law*, in *Journal of Law and the Biosciences*, *7*(1), 2020, lsaa035.

Gerli, P., Arakpogun, E.O., Elsahn, Z., Olan, F., & Prime, K.S. *Beyond contact-tracing: The public value of eHealth application in a pandemic,* in *Government Information Quarterly*, 2021, 101581.

Pizzetti, F., *Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti,* in *Rivista di diritto dei media,* 2, 2020, 11-33.

Porcedda, M. G., *Businesses need to be careful with personal data during pandemic. Methods using to collect customer data by small businesses are of dubious legality,* in *The Irish Times,* 20 july 2020.

Porcedda, M. G., *Under the radar: lessons from ordinary data processing in easing pandemic lockdown,* in *COVID-19 Law and Human Rights Observatory Blog*, 3 July 2020.

Riemer, K., Ciriello, R., Peter, S., & Schlagwein, D. *Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level,* in *European Journal of Information Systems*, *29*(6), 2020, 731-745.

Renda, A., Castro, R., *Towards Stronger EU Governance of Health Th reats after the Covid-19 Pandemic*, 11 *Eur. J. Risk Regulation* 273 (2020).

Resta, G., *Tracciamento digitale dei contatti,* in Aa. Vv., *Tutela della salute individuale e collettiva: temi etico-giuridici e opportunità per la sanità pubblica dopo COVID-19,* Istituto Superiore di Sanità, 2020, 79 – 88.

Rossello, S., Dewitte, P., *Anonymization by decentralization? The case of COVID-19 contact tracing apps,* in *European Law Blog,* 25 May 2020.

Rowe, F., Ngwenyama, O., & Richet, J. L., *Contact-tracing apps and alienation in the age of COVID-19,* in *European Journal of Information Systems*, *29*(5), 2020, 545-562.

Stefan, O., *COVID-19 Soft Law: Voluminous, Effective, Legitimate? A Research Agenda*, in *European Papers-A Journal on Law and Integration*, *2020*(1), 663-670.

Van Erp, S., *Who "Owns" the Data in a Coronavirus Tracing (and/or Tracking) App?,* in Aa. Vv., in *Coronavirus and the Law in Europe,* Intersentia, 2020.

van Kolfschooten, H., & de Ruijter, A. *COVID-19 and privacy in the European Union: A legal perspective on contact tracing, in Contemporary Security Policy*, *41*(3), 2020, 478 – 491.

Zeno-Zencovich, V., *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale,* in *Medialaws,* 26 May 2020.

Australia

Abbas, R., & Michael, K., *COVID-19 contact trace app deployments: Learnings from Australia and*

Singapore, in *IEEE Consumer Electronics Magazine*, 2020, 9(5), 65-70.
Greenleaf, G., Kemp, K., *Australia's 'COVIDSafe'law for contact tracing: an experiment in surveillance and trust*, in *International Data Privacy Law*, 2021.
Greenleaf, G., Kemp, K., *Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing*, in *UNSW Law Research*, May 15, 2020.
Howell, Bronwyn E. and Potgieter, Petrus H., *A Tale of Two Contact-Tracing Apps – Comparing Australia's COVIDSafe and New Zealand's NZ COVID Tracer,* May 28, 2020, Available at SSRN: https://ssrn.com/abstract=3612596 or http://dx.doi.org/10.2139/ssrn.3612596.
Nabben, K., *Trustless Approaches to Digital Infrastructure in the Crisis of COVID-19: Australia's Newest COVID App, Home-Grown Surveillance Technologies and What to Do About It*, April 14, 2020, Available at SSRN: https://ssrn.com/abstract=3579220 or http://dx.doi.org/10.2139/ssrn.3579220.
Watts, D., COVIDSafe, *Australia's Digital Contact Tracing App: The Legal Issues* (May 2, 2020), 2020, Available at SSRN: https://ssrn.com/abstract=3591622 or http://dx.doi.org/10.2139/ssrn.3591622.

Brazil

Capobianco Palhares, G., et al., *A privacidade em tempos de pandemia e a escada de monitoramento e rastreio,* in *Estud. av.,* 34, 99, 2020.

Canada

Austin, L. M., Chiao, V., Coleman, B., Lie, D., Shaffer, M., Slane, A., Tanguay-Renaud, F., *Test, Trace, and Isolate: COVID-19 and the Canadian Constitution*, in *Osgoode Legal Studies Research Paper*, May 22, 2020.

China

Boeing, P., & Wang, Y., *Decoding China's COVID-19 'virus exceptionalism': Community-based digital contact tracing in Wuhan*, in *R&D Management,* 2021.
Bonsall, D., Parker, M., et al., *Sustainable containment of COVID-19 using smartphones in China: Scientifi c and ethical underpinnings for implementation of similar approaches in other settings,* in: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Policy%20forum%20-%20COVID-19%20containment%20by%20herd%20protection.pdf (2020).
Du, L., Wang, M., *Chinese CoViD-19 epidemic prevention and control measures: a brief review*, in *Biolaw Journal,* Special Issue 1/2020, 741.
Hipgrave, D., *Communicable disease control in China: from Mao to now,* 1 J. Global Health 224 (2011).
Liu, C., & Graham, R. *Making sense of algorithms: Relational perception of contact tracing and risk assessment during COVID-19*, in *Big Data & Society*, *8*(1), 2021, 2053951721995218.
Liu, W., et al., *Response to the COVID-19 Epidemic: Th e Chinese Experience and Implications for Other Countries,* 17 Int. J. Environ. Res. Public Health 2304 (2020).
Tian, H., et al., *An Investigation of Transmission Control measures during the first 50 days of the Covid-19 epidemic in China*, in *Science* 10.1126/science. abb6105 (2020).
Xiao, K., *The Value of Big Data in a Pandemic*, May 13, 2020, Available at SSRN: https://ssrn.com/abstract=3583919 or http://dx.doi.org/10.2139/ssrn.3583919.

Xu, T., et al., *China's practice to prevent and control COVID-19 in the context of large population movement,* 9 *Infectious Diseases of Poverty*, 1 (2020), https://doi.org/10.1186/s40249-020-00716-0.

Wang, Z., *Systematic Government Access to Private-Sector Data in China*, in F. Cate – J. Dempsey, ed., *Bulk Collection,* Oxford, 2017, 244.

Zhang, L., *Measures to control infectious diseases under Chinese law,* January 29, 2020, https://blogs.loc.gov/law/2020/01/falqs-measures-to-control-infectious-diseases-under-chinese-law/.

Zhao, Q., et al., *On the Accuracy of Measured Proximity of Bluetooth-Based Contact Tracing Apps,* in N. Park et al., *Security and Privacy in Communication Networks,* Cham, 2020, 49.

Zhuang, M., Fang, E., Wang, R., Han, Y., *The Effects of COVID-19 on Mobile App Usage*, December 1, 2020, Available at SSRN: https://ssrn.com/abstract=3740433 or http://dx.doi.org/10.2139/ssrn.3740433.

Far East

Findlay, M., Remolina, N., *Regulating Personal Data Usage in Covid-19 Control Conditions,* SMU Centre for AI & Data Governance Research Paper No. 2020/04.

Geddie, J., Aravindan, A., *Singapore plans wearable virus-tracing device for all*, *Reuters*, June 5, 2020, https://www.reuters.com/article/us-health-coronavirus-singapore-tech/singapore-plans-wearable-virus-tracing-device-forall-idUSKBN23C0FO.

Gyooho, L., *Legislative and Administrative Responses to COVID-19 Virus in the Republic of Corea*, April 28, 2020, https://dx.doi.org/10.2139/ssrn.3587595.

Holmes, A., *Singapore is using a high-tech surveillance app to track the coronavirus, keeping schools and businesses open. Here's how it works,* in Business Insider, March 24, 2020.

France

Bensamoun, A., Martial-Braz, N., *StopCovid : sortir des postures ! Point de vue sur l'avis de la CNIL*, in *Revue Dalloz IP/IT*, 2020, n°5 p. 280.

Denis, F., Fontanet, A., Le Douarin, Y.M., Le Goff, F., Jeanneau, S., & Lescure, F.X., *A self-assessment web-based app to assess trends of the COVID-19 pandemic in France: observational study,* n *Journal of Medical Internet Research*, *23*(3), 2021.

Martial-Braz, N., *Nos données de santé en danger... quand l'arbre de la crise sanitaire cache la forêt de la perte de souveraineté, Club des juristes,* 26 June 2020.

Metallinos, N., *Quel encadrement pour les outils numériques du dépistage Covid-19 ?,* in *Communication, Commerce électronique*, n° 7-8 2020, n°59.

Pailler, L., *StopCovid: la santé publique aux prix de nos libertés ? Point de vue*, in *Recueil Dalloz* 2020, p. 935.

Germany

Blaeser, M. , dos Santos Firnhaber, C., *Tracking & Tracing: Fluch oder Segen der Digitalisierung des Gesundheitsmanagements? Corona-Warn-App*, in *RDG*, 2020, 182.

Fast, V., Schnurr, D., *Incentivizing Data Donations and the Adoption of COVID-19 Contact-Tracing Apps: A Randomized Controlled Online Experiment on the German Corona-Warn-App*, May 5, 2021, Available at SSRN: https://ssrn.com/abstract=3786245 or http://dx.doi.org/10.2139/ssrn.3786245.

Kühling, J., Schildbach, R., *Corona-Apps. Daten- und Grundrechtsschutz in Krisenzeiten,* in *NJW,* 2020, 1545.

Paal, B.P., Pauly, D.A., *Datenschutz-Grundverordnung*, Beck, Munich, 3rd ed. 2021, *Einleitung,* par. 45.

Samardzic, D., Becker, T., *Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW*, 2020, 646.

Sander, C., Hilberg, S., Bings, S., *Arbeitsschutzrechtliche Fürsorge- und Schutzpflichten sowie Haftungsrisiken für Arbeitgeber im Zusammenhang mit COVID-19,* in *COVur,* 2020, 347.

Voland, T., Kümmel, M., *Mit Technologie gegen das Virus Rechtliche Fragen im Zusammenhang mit der Corona-Warn-App,* in *PharmR,* 2021, 189.

India

Basu, S. *Effective contact tracing for COVID-19 using mobile phones: an ethical analysis of the mandatory use of the aarogya setu application in India*, in *Cambridge Quarterly of Healthcare Ethics*, *30*(2), 2021, 262-271.

Chaturvedi, A., Kalyani, S., Jain, G., *Reliability and Effectiveness of Indian COVID-19 Mobile Apps*, in *Journal Of Critical Reviews*, 7 (14), 2020, 1296 – 1305.

Dhindsa, Anmol and Kaushik, Sashwat, *The Constitutional Case against Aarogya Setu*, May 19, 2020, Available at SSRN: https://ssrn.com/abstract=3610569.

Italy

Bolognini, L., *Il bilanciamento tra diritti, libertà e interessi pubblici nel contact tracing è questione di alta politica*, in *Medialaws,* 21 May 2020.

Bonomi, M.S., *L'app Immuni: tra tutela della salute e protezione dei dati personali,* in *Federalismi.it Osservatorio di diritto sanitario,* 24 giugno 2020.

Cadelano, S., *Emergenza "Coronavirus" e Privacy: Trattamento dei dati personali da parte dei datori di lavoro,* in *AmbienteDiritto.it,* 2, 2020.

Camardi, C., Tabarrini, C., *Contact tracing ed emergenza sanitaria. "Ordinario" e "Straordinario" nella disciplina del diritto al controllo dei dati personali*, in *La nuova giur. civ. comm.*, 2020, 38.

Ciocia, M.A., *Geolocalizzazione e norme a tutela della* privacy *per il contenimento del rischio da Covid-19,* in *Oltre la Pandemia. Società, salute, economia e regole nell'era* post *Covid 19,* G. Palmieri (a cura di), Editoriale Scientifica, 2020, vol. II, 1069-1086.

Colapietro, C., Iannuzzi, A., *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali,* in *Dirittifondamentali. it,* n. 2/2020, 772.

D'Ambrosio, M., T*racciamento tecnologico del contagio,* in *Actualidad Jurídica Iberoamericana*, *12bis,* 2020, 868-885.

Della Morte, G., *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano,* in *Diritto umani e diritto internazionale*, 14, 2020, 303-335.

Falletti, E., *Privacy Protection, Big Data Gathering and Public Health Issues: COVID-19 Tracking App Use in Italy*, January 2, 2021, Available at SSRN: https://ssrn.com/abstract=3758800 or http://dx.doi.org/10.2139/ssrn.3758800.

Finocchiaro, G., *Il punto sull'app Immuni: bilanciamento tra diritti*, in *Media Laws*, 9-6-2020 (http://www.medialaws.eu/il-punto-sullapp-immuni-bilanciamento-tra-diritti/).

Istituto Superiore di Sanità, Rapporto ISS-Covid 19 n. 59/2020, *Supporto digitale al tracciamento dei contatti (contact tracing) in pandemia: considerazioni di etica e di governance,* available at: https://www.iss.it/rapporti-covid-19/-/asset_publisher/btw1J82wtYzH/content/rapportoiss-covid-19-v.-59-2020-supporto-digitale-al-tracciamento-dei-contatticontact-tracing-in-pandemia-considerazioni-di-etica-e-di-governance. -versione-del-17-settembre-2020.

Perlingieri, C., C*oronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi,* in *Actualidad Jurídica Iberoamericana*, *12bis,* 2020, 836-847

Pertot, T., *Immuni e tracciamento digitale: la protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, in *Le nuove leggi civ. comm.*, 2010, 1149

Pititto, G., *La sfida delle app contro il covid-19,* in *GEOmedia*, *24*(1), 2020, 12 – 19.

Plutino, M., *Immuni,* un'exposure notification app *alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici,* in *Rivista di diritto dei media,* 2, 2020, 172-193.

Poletti, D., *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza,* in *Persona e mercato,* 2020, 31.

Poletti, D., *Contact tracing e app immuni: atto secondo,* in *Persona e mercato,* 2021, 92

Resta, G., *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, in *Giustizia Civile. com*, *Editoriale,* May 5, 2020.

Resta, G., *La app 'Immuni': pregi e limiti del tracciamento digitale dei contatti,* in *Medialaws,* 15-6-2020 (http://www.medialaws.eu/la-app-immuni-pregi-e-limiti-del-tracciamento-digitale-dei-contatti/).

Resta, G., *Tracciamento digitale dei contatti*, in C. Petrini, ed., *Tutela della salute individuale e collettiva: temi etico-giuridici e opportunità per la sanità pubblica dopo COVID-19* , Rapporti ISTISAN 20/30, Istituto superiore di sanità, Rome, 2020, 79-88.

Zeno-Zencovich, V. *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *MediaLaws* 26-5-2020 (http://www.medialaws.eu/i-limiti-delle-discussioni-sulle-app-di-tracciamento-anti-covid-e-il-futuro-della-medicina-digitale/).

South Africa

De Villebois Castelyn, C., Botes, M., Viljoen, I. M., Pope, A., & Pepper, M. S., *Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa*, in *South African Journal of Bioethics and Law*, *13*(1), 2020, 20-25.

South Korea

Lee, G., *Legitimacy and Constitutionality of Contact Tracing in Pandemic in the Republic of Korea,* in *Il Nuovo Diritto delle Società,* 3, 2020, 407-444.

Orlando, A., *Il modello sudcoreano contro il Covid-19: imparare con cautela,* in *DPCE Online,* 2, 2020, 2069-2093.

Spain

Andreu Martinez, B., *Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la covid-19,* in *Actualidad Jurídica Iberoamericana,* 12*bis,* 2020, 848-859.

United Kingdom

Aa. Vv., *The epidemiological impact of the NHS COVID-19 App*, in *Nature*, 2021,1 – 8.

Bachtiger, P., Adamson, A., Quint, J. K., & Peters, N. S., *Belief of having had unconfirmed Covid-19 infection reduces willingness to participate in app-based contact tracing,* in *NPJ digital medicine*, *3*(1), 2020, 1-7.

Braithwaite, I., et al., *Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19* https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30184-9/fulltext.

Briers, M., Holmes, C., Fraser, C., *Demonstrating the impact of the NHS COVID-19 app,* https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app.

Chidambaram, et al., *Observational study of UK mobile health apps for COVID-19,* https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30144-8/fulltext.

Guinchard, A, *Our digital footprint under Covid-19: should we fear the UK digital contact tracing app?*, in *International Review of Law, Computers & Technology*, 2020, 35(1), 84-97.

Hegde, A., & Masthi, R. *Digital Contact tracing in the COVID-19 Pandemic: A tool far from reality*, in *Digital health*, 2020, 6, 2055207620946193.

Horvath, L., Banducci, S., James, O., *Citizens' Attitudes to Contact Tracing Apps*, https://www.cambridge.org/core/journals/journal-of-experimentalpolitical-science/article/citizens-attitudes-to-contact-tracing-apps/F9B8B8CFE051E6D89C3C9ADD6DF76019.

Jacob, S., Lawarée, J., *The adoption of contact tracing applications of COVID-19 by European governments*, https://www.tandfonline.com/doi/full/10.1080/25741292.2020.1850404.

Oswald, M., Grace, J., *The Covid-19 Contact Tracing App In England and 'Experimental Proportionality*, in *Public Law*, 2021, 27-37.

Pagliari, C., *The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response,* in *Journal of Global Health*, *10*(2), 2020.

Privacy International, *UK government Covid tracking app: what we Found,* https://privacyinternational.org/long-read/3752/coronavirus-tracking-ukwhat-we-know-so-far.

Samuel, G., et al., *COVID-19 contact tracing apps: UK public perceptions*, in *Critical Public Health*, 2021, 1-13.

Williams. S.N., et al., *Public attitudes towards COVID-19 contact tracing apps: A UK based focus group study*, https://onlinelibrary.wiley.com/doi/10.1111/hex.13179.

United States of America

Bodie, M. T., & McMahon, M. *Employee testing, tracing, and disclosure as a response to the coronavirus pandemic*, in *Washington University Journal of Law and Policy*, 64, 2020.

French, M., et al., *Corporate contact tracing as a pandemic response*, in *Critical Public Health*, 2020, 1-8.

Ganno, A. *Reforming Privacy Law in America: A Comparative Analysis on Digital Contact Tracing Data and Its Implications in the Age of COVID-19,* 2021, Available at SSRN 3808918.

Ghose, A., Li, B., Macha, M., Sun, C., Foutz, N. Z., *Trading Privacy for the Greater Social Good: How Did America React During COVID-19?* , *NYU Stern School of Business,* June 10, 2020, Available at SSRN: https://ssrn.com/abstract=3624069 or http://dx.doi.org/10.2139/ssrn.3624069.

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C., *Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective*, in *Journal of the American Medical Informatics Association*, *28*(3), 2021, 463 – 471.

Kiosse, A., *Digital Contract Tracing in the Workplace,* in *Washington Journal of Law, Technology & Arts*, *16*(2), 2021, 1.

Lu, X., L. Reynolds, T., Jo, E., Hong, H., Page, X., Chen, Y., & A. Epstein, D. *Comparing Perspectives Around Human and Technology Support for Contact Tracing*, in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems,* 2021, 1 – 15.

Ram, N., & Gray, D. *Mass surveillance in the age of COVID-19*, in *Journal of Law and the Biosciences*, *7*(1), 2020, lsaa023.

"Nudges" et "big data" dans le monde d'après : Une menace sur le Contrat Social ?

Sacha Bourgeois-Gironde, Professeur à l'Université Panthéon Assas et Institut Jean Nicod de l'ENS.

Bruno Deffains, Professeur à l'Université Panthéon Assas, Centre de Recherches en Economie et Droit.

La crise du Covid-19 a révélé de manière aiguë deux tendances déjà latentes dans l'évolution des modes de gouvernance : la collection et le traitement des "big data" relatifs à des comportements individuels et la formation de prédictions sur la manière dont ces comportements peuvent être guidés par le design d'architectures de choix adaptées aux circonstances. C'est le sens et la portée, ou plutôt l'absence actuelle de conceptualisation et d'anticipation des effets de la conjonction entre ces deux tendances que nous aimerions pointer. En soi, il ne s'agit que de techniques et nous ne réprouvons en rien l'usage de techniques, ni même nécessairement de ces techniques, tant que le sens et la portée en sont clarifiés, en vue d'améliorer les modes de gouvernance, que ce soit en temps de crise ou en temps normal. Mais une technique de gouvernance ne s'accorde pas *a priori* et sans plus de précaution théorique avec la légitimité d'un pouvoir institué et constitué sur des bases normatives - lesquelles doivent encadrer, limiter, et conférer une signification publiquement acceptable à sa nature et à son usage.

Comme nous venons de le dire, c'est la conjonction de ces deux techniques, le traitement de données massives associé au design d'architectures de choix, et leur renforcement mutuel, que nous visons plus particulièrement et dont nous pensons qu'elle atteint aux fondements normatifs de notre contrat social. Mais il vaut la peine de rappeler de quelle manière chacune, indépendamment, est devenue saillante au point de paraître former un recours évident dans la gestion de la crise sanitaire actuelle.

La première tendance concerne l'usage et la technique de la collecte des données massives, à l'image des enjeux apparus dans la gestion de la crise du Covid-19. La propagation du virus a provoqué des perturbations considérables dans tous les domaines de la vie, d'une explosion du travail à distance aux mesures de confinement généralisées, qui comprennent souvent des mesures de quarantaine ou de confinement. Un nombre significatif de pays ont même adopté des mesures plus « offensives » pour lutter contre le Covid-19, notamment en utilisant des données individuelles pour suivre les citoyens infectés. Il est rapidement devenu évident que l'une des plus grandes ressources du moment était les données personnelles et, en particulier, les données de localisation. Par exemple, Taïwan a institué une politique

* Reproduced with gracious permission of the Authors. The original text was published by the Club des Juristes, 28.5.2020 and is available, in open access, at the following page: https://blog.leclubdesjuristes.com/big-data-nudging-et-contrat-social-dans-le-monde-dapres/

de suivi individuel particulièrement contraignante. Semblable à un bracelet de cheville, le téléphone transmet les données de localisation de l'utilisateur aux autorités locales et à la police. Si le téléphone sort de la zone autorisée ou cesse de transmettre, la police va vérifier sur place pour s'assurer que les règles de quarantaine sont respectées. Dans l'UE, le règlement général sur la protection des données (« RGPD ») limite ce que les entreprises peuvent et ne peuvent pas faire avec les données de leurs utilisateurs. Il considère certaines caractéristiques comme des « données personnelles » telles que l'emplacement, les données démographiques, le nom, l'adresse… traduisant ainsi une préoccupation croissante en matière de confidentialité des métadonnées. Aux États-Unis, les préoccupations découlent de la façon dont les données personnelles sont traitées, mais il n'y a pas de législation unique et unifiée sur la protection des données. La jurisprudence et les lois des différents États constituent une mosaïque de règles qu'une application de suivi devrait respecter pour être applicable à l'échelle du pays. Partout dans le monde, la question consiste à savoir dans quelle mesure les gens sont prêts à renoncer à une partie de la vie privée dont ils disposent sur leurs données personnelles afin de lutter efficacement contre le Covid-19 et, si oui, que se passe-t-il après que tout soit terminé?

La seconde tendance - popularisée sous le nom de "nudging" depuis le best-seller de Thaler et Sunstein (2009) - a progressivement pénétré certaines sphères gouvernementales[1] ainsi que la culture et les investissements scientifiques de certains experts en sciences comportementales et cognitives. Ces experts trouvent un débouché opportun et efficace dans la société de leur capacité à repérer expérimentalement des corrélations entre ce qu'ils savent du fonctionnement de l'esprit humain et des comportements observés dans des conditions expérimentales. Le point principal que nous pouvons critiquer n'est pas celui de la validité externe de ces expériences et de ces corrélations. Certes, les environnements sociaux sont plus riches et complexes que les environnements de laboratoire, mais il n'est nullement interdit de penser qu'il y a des faits psychologiques et comportementaux robustes qui résistent à leur immersion dans la "vie réelle". C'est d'ailleurs du fait de cette robustesse apparente que l'économie comportementale, à travers l'identification d'une liste de biais cognitifs et comportementaux, a acquis sa popularité. Un temps, la mise à jour de ces biais, a servi le but critique de déstabiliser le mythe de l'homo oeconomicus (probablement un homme de paille) censément guidé par une rationalité et des capacités cognitives parfaites. Ce réalisme psychologique a trouvé un prolongement instrumental, mais quasi-paradoxal, dans l'idée de nudge. Car à présent il s'agit de "rationaliser" ces biais, d'en canaliser les effets au sein d'architecture de choix de sorte à les rendre bénéfiques pour celui qui les subit et finalement optimal pour la société. Pétri de défauts cognitifs,

[1] Voir en ce sens, Cécile Désaunay, « les nudges au service des pouvoirs publics ? », Futuribles, 2017 ; Benoît Floc'h, « L'administration se convertit aux sciences comportementales », Le Monde, 9 août 2019 ; Jean-Gabriel Plumelle, « Pour une société de confiance. Quel rôle pour le service public ? », IGPDE Editions Publications, disponible à l'adresse : https://www.economie.gouv.fr/igpde-editions-publications/lanalyse-comparative_n4

de mauvaises anticipations de ce qui peut maximiser son utilité, l'individu peut tout de même prétendre au bien-être car une entité bienveillante sait a priori comment détourner pour le mieux ses défaillances. Ce n'est pas tant le paternalisme inhérent à cette position, qui a été maintes fois souligné, que nous souhaitons discuter ici. Ce paternalisme "libéral", dit-on, n'aurait rien d'intrusif ou de compromettant pour la liberté individuelle, vu que c'est la disposition des options (leur architecture, le "design" de l'environnement de décision) et non la disponibilité des options elles-mêmes qui est expérimentalement manipulée. C'est l'exemple canonique, chez Thaler et Sunstein, de la cafeteria où les salades sont disposées sur les présentoirs de manière plus saillante que les macaronis au fromage. Le problème que nous percevons dans ces manipulations plus ou moins innocentes tient à leur généralisation, à leur association avec des techniques affinées de prédictions comportementales, et, surtout, à l'absence de véritable réflexion normative sur leur usage qui doit se hisser bien au-delà du jeu conceptuel de surface autour de l'oxymore « paternalisme libéral »[2].

Chez nos experts actuels des sciences comportementales, ce sont par exemple des techniques de communication pour inciter les gens à bien se laver les mains ou d'appréhension intuitive de la bonne distance physique à maintenir entre les individus. Quoi de plus innocent et utile, en effet, que de guider les individus vers ces comportements salutaires par des messages efficaces. Il y a même, n'en doutons pas, de profondes connexions entre l'ancrage évolutionnaire et neurobiologique de notre sens de la pureté, voire du sacré, et la propension ou la réticence, selon les individus, à préserver une hygiène, une prophylaxie et une distanciation sociale biologiquement conservatrices. Là encore on ne peut en principe que louer l'apport des sciences cognitives et comportementales à la compréhension des mécanismes psychologiques qui faciliteront ou feront obstacle à l'application de pratiques de santé publique en période de crise. La dimension qui est cependant oubliée, et qui n'a pas donné lieu à une réflexion spécifique depuis l'apparition et la popularisation des nudges, est celle de la place de ces pratiques dans l'espace public qui semble pourtant leur terrain de jeu privilégié. Que signifient, pour les tenants de ces pratiques, l'espace « public », une politique « publique », la différence entre la sphère privée et la « sphère publique » et les principes fondamentaux qui régissent cette différence ? Dans le débat d'opinion, de fait, on s'inquiète largement de l'emprise des données massives sur la vie privée, mais qu'en est-il de celle des nudges sur la vie publique ? Et qu'en est-il quand nudge et big data travaillent de concert ?

Les problèmes qui nous paraissent importants se posent à trois autres niveaux.

[2] Pour un premier jet de critiques sur la superficialité avec laquelle les auteurs principaux du nudge ont voulu rendre compatibles leurs propositions pratiques avec des normes libérales, critiques différentes de celle que nous allons formuler, nous pouvons renvoyer le lecteur à : Grüne-Yanoff, T. (2012). Old wine in new casks: libertarian paternalism still violates liberal principles. *Social Choice and Welfare*, *38*(4), 635-645.

Le premier problème est ce que nous nommerons le règne du descriptif. Les données brutes ainsi que l'observation de corrélations entre environnement et comportement sont d'autant mieux accueillies qu'elles semblent dépourvues d'ancrage normatif et idéologique. Elles sont considérées comme des descriptions neutres et il n'y a donc pas lieu de s'en défier. Si l'on observe une amélioration comportementale et plus généralement sociale grâce à l'agrégation de comportements corrigés, parce que ces données ou ces corrélations ont été mises en usage, de quoi se plaindre ? Et bien justement du contrepoint que ce privilège du fait, de la donnée et de la corrélation statistique suscite : la méfiance, en retour, envers ce qui ne se présenterait pas a priori comme "neutre". On observe une tendance, en économie comportementale, mais aussi en économie du développement, par exemple dans des travaux récompensés l'année dernière par le prix Nobel de la discipline, à évacuer la dimension politique et normative du travail de l'économiste. Des recettes expérimentales, sophistiquées et administrées de manière impressionnante et plutôt convaincante, basées sur le transfert, à l'échelle d'une région ou d'une nation, d'observations comportementales, peuvent contribuer à améliorer le bien-être d'une population. Le bien-être est pourtant une notion éminemment normative, mais ce qui compte dans ce contexte est que la base sur laquelle il est maximisé est indépendante d'une conception politique particulière. Autrement dit, l'amélioration du bien-être d'une population par ces recettes est compatible avec n'importe quelle conception politique en vigueur qui déciderait que leur usage ne lui est pas incompatible. Ce qui compte est d'éliminer la pauvreté, l'illettrisme et d'écarter la maladie, pas d'envisager leur lien éventuel avec des modalités et des normes de gouvernance qui ont pu, par ailleurs, faciliter leur émergence. Une telle approche creuse un écart problématique entre les usages et les techniques mis au service de ce qu'il convient donc, dans les milieux gouvernementaux ou scientifiques faisant appel aux "nudges", d'appeler des "politiques publiques", et la politique elle-même - c'est-à-dire l'orientation absolument dénuée de neutralité des cadres sociaux, légaux et économiques de nos existences et de nos comportements.

Cet écart se poursuit à un niveau plus profond. En déléguant ponctuellement la rationalité individuelle, jugée déficiente, à un designer bienveillant des architectures de choix, ce n'est pas seulement le risque paternaliste inhérent à cette délégation et la déresponsabilisation individuelle partielle qui posent problème, que la dégradation de la relation consentie et dialogique entre l'individu et ce designer. Le deuxième problème est donc l'accentuation d'une asymétrie informationnelle entre la mise en œuvre de "politiques publiques", quand elles s'appuient sur des nudges, et l'absence de perception qu'a l'individu des modifications qui sont apportées à la nature et à la structure de ses opportunités, quand bien même ces modifications induiraient une amélioration de son bien-être, de sa santé, ou de ses perspectives personnelles. Les nudges sont censés préserver les choix et l'état d'esprit de l'individu. C'est là leur vertu non-intrusive. Un nudge est ainsi généralement mis en place sans le signal qui accompagne l'annonce de sa mise en place. Le guidage des comportements doit se faire implicitement, si ce n'est insidieusement. Cette modification n'est donc pas l'objet

d'un dialogue ni d'un consentement. Sa nécessité paraît inutile, puisque les choix initialement disponibles le sont toujours. Aucune violation de droits constitutionnels, telle qu'une entrave à la liberté individuelle, ne saurait ainsi être impliquée par ces pratiques minimalistes. Mais l'extension de ces pratiques est aussi l'extension d'enclaves dans le domaine public dont la nature n'a pas été consentie, et a fortiori consentie sur une base éclairée et rationnelle, puisque l'absence de celle-ci est précisément le présupposé sur lequel ces pratiques se justifient. Ce n'est donc plus seulement la séparation, sous le prétexte de la neutralité, du descriptif et du normatif, de l'intervention efficace et du politique, dont il devient ici question, mais de la neutralisation de la capacité et de l'exigence démocratique des individus à contribuer à la discussion normative sur ce qui constitue le domaine de l'intervention publique. Cette neutralisation du domaine public par la conception sous-tendant certaines "politiques publiques" suggère le risque d'un amoindrissement du dialogue entre citoyens et puissance publique, qui se tient pourtant à la base du contrat social sous le régime duquel nous avons librement consentis de vivre.

Cette menace sur le contrat social est le troisième problème, le plus aigu. Son actualité tient à la conjonction nouvelle, dans la crise actuelle, des nudges et des big data, en absence d'une réflexion normative sur les risques pour la démocratie qui en accompagneraient la mise en œuvre. Les algorithmes d'aide à la décision fondés sur des données massives mettent en évidence des corrélations qui ne seraient pas observables par des techniques expérimentales classiques. Le design d'architectures de choix qui en découlent diffèrent des nudges "statiques" popularisés par Thaler et Sunstein (tels que la disposition des salades). Les nudges basés sur l'analyse de données massives sont « designés » sur la base d'informations acquises en ligne, en réseau, et continuellement mises à jour. Ce sont des nudges dynamiques et pervasifs, qui, s'ils ne sont peut-être pas intrusifs au sens où il est toujours possible de choisir autre chose que ce qui est, de moins en moins implicitement, prescrit, dessinent des lignes comportementales à suivre, plutôt que des choix uniques et indépendants les uns des autres. Dans le cas de l'application StopCovid, la moralisation de son usage liée au fait de ne pas vouloir être jugé responsable de la contamination de son prochain, la demande de civisme, de sens des responsabilités, voire tout bonnement d'humanité, guident le comportement dans un style devenu véritablement prescriptif et paternaliste.

Le recours au nudge, avec StopCovid, s'opère en fait à deux niveaux. En amont, il s'agit d'inciter les citoyens, pour qui la vertu ne serait pas spontanée, à télécharger et utiliser cette application[3] ; par exemple en associant son téléchargement à l'accès gratuit à des sites d'entertainment, etc. En aval, il s'agit d'analyser les données récoltées pour affiner les recommandations comportementales par le moyen de

[3] Cf. une contribution récente dans La Tribune : https://www.latribune.fr/opinions/blogs/homo-numericus/le-nudge-outil-de-lutte-contre-le-covid-845762.html

nouveaux nudges à élaborer. L'usage de ces nudges massifs et itératifs, quand bien même ils doivent, du fait de l'acquisition d'informations privées, donner lieu à des avertissements individuels et être accompagnés de notices de consentement[4], a des implications troublantes non seulement pour la liberté, comme cela a naturellement été souligné, mais aussi pour l'égalité et la solidarité. Il nous paraît urgent de rétablir à leur endroit la prévalence d'un cadre normatif définissant et limitant leur usage. Et il faut le faire en osant contrecarrer l'argument culpabilisant qui consisterait à laisser croire que l'exigence d'un tel cadre, au mieux ralentirait, au pire s'opposerait à l'usage de techniques efficaces dans la lutte contre les fléaux qui affectent l'humanité.

Pour comprendre les défis auxquels nous allons devoir faire face, il faut revenir au passé et plus particulièrement à la question qui hantait le XIXe siècle : comment concevoir des systèmes de protection sociale qui ne remettaient pas en cause les principes libéraux hérités de la Révolution française ? La société issue de la Révolution, caractérisée notamment par le Code civil, est un monde de citoyens théoriquement libres et égaux, qui nouent entre eux des contrats où les parties engagent leur responsabilité individuelle. Dans cet univers, à chacun de se prémunir contre le risque (vieillesse, maladie, accident) par sa propre prévoyance ou par la mise en cause du fautif : l'ouvrier victime d'un accident du travail devra réussir à prouver la faute de l'employeur. C'est précisément à l'occasion de la loi sur les accidents du travail, adoptée en 1898, que le concept d'assurance collective est utilisé pour la première fois à l'échelle de la nation. En plaçant l'accident sous le registre du hasard et des aléas du destin, on se donne les moyens de dépasser la notion de responsabilité individuelle. C'est sur cette nouvelle base que s'est organisé progressivement tout le système de protection sociale qui a marqué l'émergence de l'Etat providence au XXème siècle[5].

Dans la tradition contractualiste, John Rawls ajoutera dans sa *Théorie de la Justice Sociale* que les partenaires de la coopération *ignorent tout de leur situation personnelle*, actuelle ou future, dans la société : « Parmi les traits essentiels de cette situation, il y a le fait que personne ne connaît sa place dans la société, sa position de classe ou son statut social, pas plus que personne ne connaît le sort qui lui est réservé dans la répartition des capacités et des dons naturels, par exemple, l'intelligence, la force, etc. ». Les partenaires sont ainsi placés, selon la célèbre formule, derrière un *voile d'ignorance*, situation privilégiée pour déterminer les principes de justice en toute équité. Ce voile d'ignorance est fragile mais il l'est encore plus du fait de l'exploitation massive de données individuelles.

[4] Voir en ce sens le communiqué du Comité National Pilote d'Éthique du Numérique (CNPEN) du 29 avril 2020 sur les « **Enjeux d'éthique du numérique du suivi épidémiologique en sortie de confinement** » ainsi que l'avis de la Commission Nationale Consultative des Droits de l'Homme (CNCDH) du 24 avril 2020 sur le « **Suivi numérique des personnes : Un risque d'atteinte disproportionnée aux droits et libertés pour une efficacité incertaine** ».

[5] Pour une perspective historique, voir François Ewald, *L'Etat Providen*ce, Grasset, 1986.

Même si on ne le conçoit pas immédiatement, la digitalisation de la société crée en réalité une crise « philosophique » du contrat social. Jusqu'ici, notre modèle était de type assuranciel. Contrairement à l'assistance, le mécanisme assurantiel créé une solidarité pour faire face à certains risques : les ruptures liées à la maladie, au chômage, à la retraite, aux accidents de la vie… La réponse du système assuranciel est fondée sur la « mutualisation des risques ». Pourquoi acceptons-nous le poids de cette solidarité ? Parce que nous avons conscience que chacun de nous courre des risques, et que nous ne savons pas à l'avance qui seront les victimes des accidents ou des ruptures. C'est cette incertitude sur notre avenir, ce voile d'ignorance, qui fonde la redistribution. Or, aujourd'hui, ce voile se déchire.

La société devient plus transparente et moins homogène du fait de la collecte de données individuelles et d'analyses comportementales et « prédictives » toujours plus sophistiqués dans tous les domaines. L'actualité dans le domaine de la santé doit nous faire prendre conscience de la nécessité de repenser les liens qui nous unissent dans le cadre du contrat social. Au fur et à mesure que le voile se déchire, resterons-nous solidaires de la même façon si nous savons que certains courent des risques énormes, et d'autres pas ? De même, le fait que, pour beaucoup, le chômage et la précarité ne constituent plus des risques accidentels, mais plutôt un état permanent, ne change-t-il pas fondamentalement la nature de leur prise en charge ?

L'« accompagnement » numérique de nos existences tend inéluctablement à restreindre le champ des possibles en termes de capacités d'action individuelle en encadrant nos choix lorsque les nudges rencontrent l'analyse prédictive fondée sur la collecte de données massives. Face à ces nouveaux défis, la solidarité est une valeur à l'épreuve. Elle est confrontée à la promesse de solutions de plus en plus individualisées pour répondre aux risques sociaux et ce à travers le développement d'outils qui accompagnent la promesse faite à chacun de se prémunir au plus juste prix. Dans un tel environnement, on comprend que les logiques de solidarités collectives sont en danger alors même qu'elles n'ont peut-être jamais été aussi essentielles pour préserver le contrat social. La solution ne réside pas dans le cadre d'un paternalisme bienveillant et libertaire mais plutôt du côté d'une interférence non-arbitraire avec nos libertés individuelles. Les « politiques publiques » basées sur l'usage des données massives et des nudges omettent, dans les circonstances actuelles, de réfléchir suffisamment profondément à ce qui constitue « une intervention non-arbitraire ». Cela est encore plus vrai des nudges que des données massives, dans la mesure où ils paraissent spontanément neutres et non-intrusifs. En réalité ils tendent à modifier et à occulter les normes qui sous-tendent notre conception de la sphère publique, et d'autant plus fortement qu'ils sont associés à la collecte d'informations privées. Il nous paraît donc urgent de refonder le contrat social pour éviter que, à la faveur de la crise actuelle, le prédictif ne devienne définitivement prescriptif.

The Institutionalisation of Digital Public Health: Lessons Learned from the COVID-19 App

Ciro CATTUTO* and Alessandro SPINA**

I. Introduction

Amid the outbreak of the SARS-CoV-2 pandemic, there has been a call to use innovative digital tools for the purpose of protecting public health. There are a number of proposals to embed digital solutions into the regulatory strategies adopted by public authorities to control the spread of the coronavirus more effectively. They range from algorithms to detect population movements by using telecommunications data to the use of artificial intelligence and high-performance computing power to detect patterns in the spread of the virus.[1] However, the use of a mobile phone application for contact tracing[2] is certainly the most popular.

These proposals, which have a very powerful persuasive force and have apparently contributed to the success of public health responses in a few Asian countries, also raise questions and criticisms, particularly with regards to the risks that these novel digital surveillance systems pose for privacy and in the long term for our democracies.

With this short paper, we would like to describe the pattern that has led to the institutionalisation of digital tools for public health purposes. By tracing their origins to "digital epidemiology", an approach that originated in the early 2010s, we will expose that, whilst there exists limited experimental knowledge on the use of digital tools for tracking disease, this is the first time in which they are being introduced by policy-makers into the set of non-clinical emergency strategies to a major public health crisis. As reflected in the public debate about the design and implementation of the contact tracing app for COVID-19, the novelty of using digital tools in public health brings in a set of questions concerning not only their alleged effectiveness, but also their compatibility with privacy right and fairness. The institutionalisation of

* Associate Professor in the Computer Science Department Computer of the University of Turin (Italy) and Principal Scientist and Research Area Coordinator at the ISI Foundation of Turin.

** Member of the Legal Service, European Commission (Brussels) and Visiting Lecturer at the Faculty of Law of the University of Fribourg (Switzerland); email: alessandro.spina@protonmail.com. The views expressed in this article are those solely of the authors and do not reflect the official position of the European Commission.

[1] Cf <https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic>.

[2] "Contact tracing" is a public health intervention based on monitoring contacts after exposure to an infected person and aimed essentially to prevent further transmission of a virus: for more details, see <https://www.who.int/news-room/q-a-detail/contact-tracing>.

European Journal of Risk Regulation, 11 (2020), pp. 228–235 doi:10.1017/err.2020.47

digital tools for COVID-19 is therefore taking place within a system of public governance that is unprepared to tackle the ethical, social and legal challenges of these technologies.

The aim of this paper is to demonstrate, with reference to the controversies of the COVID-19 contact tracing app, that the institutionalisation of digital tools for public health requires novel institutional mechanisms to manage their complexity and risks. Our conclusion is that, like in the regulatory models of other risk technologies such as medicines or genetically modified organisms (GMOs), we need to have transparency and public oversight of digital public health.

II. The origins of digital epidemiology

From a scientific point of view, the current efforts to leverage the public health measures on digital strategies should be seen in the broader context of digital epidemiology.[3] What is digital epidemiology? The goal of epidemiology is to understand the patterns of disease and health dynamics in populations, as well as the causes of these patterns, and to use this understanding to mitigate and prevent disease and to promote health. The goal of digital epidemiology is exactly the same, with the main difference being that whilst epidemiology uses traditional data collected by health protection agencies and healthcare providers (eg patient medical records, death certificates, disease registries), digital epidemiology uses digital data, and often data that were not originally collected for health applications[4] (eg search engine queries mentioning medical symptoms for population-scale disease surveillance).

Perhaps one of the first and most well-known examples of digital epidemiology is Google Flu Trends (GFT), which used symptomatic search queries for the purpose of syndromic tracking of influenza-like illnesses.[5] Although the technical merit of the specific tool was subsequently criticized,[6] it did have a lasting impact in creating awareness about new opportunities for the secondary use of digital data, and it paved the way to a rich field of research. Another example of digital epidemiology approaches is the use of telecommunications data to examine the movements of people and their influence on infectious disease dynamics. For example, mobile phone call records were analysed as indicators of travel patterns in an African country, and this provided understanding of malaria spread caused by human mobility.[7] In another study, the position data of subscriber identity module (SIM) cards from the largest mobile phone company in Haiti were used to estimate the magnitude and trends of population movements following the 2010 Haiti earthquake

[3] M Salathé et al, "Digital Epidemiology" (2012) 8(7) PLoS Computational Biology e1002616.

[4] A representative model of the structured effort to gather and analyse web-based signals for the purpose of disease surveillance is a system called HealthMap: JS Brownstein, CC Freifeld, BY Reis and KD Mandl, "Surveillance Sans Frontières: Internet-Based Emerging Infectious Disease Intelligence and the HealthMap Project" (2008) 5(7) PLoS Medicine e151.

[5] J Ginsberg, MH Mohebbi, RS Patel, L Brammer, MS Smolinski and L Brilliant, "Detecting Influenza Epidemics Using Search Engine Query Data" (2009) 457(7232) Nature 1012.

[6] D Lazer et al, "The Parable of Google Flu: Traps in Big Data Analysis" (2014) 343(6176) Science 1203.

[7] A Wesolowski et al, "Quantifying the Impact of Human Mobility on Malaria" (2012) 338(6104) Science 267.

and cholera outbreak.[8] All of the above examples show that the findings of digital epidemiology are based on data generated outside of the public health system (ie data that were not generated with the primary purpose of doing epidemiology).[9] Such a secondary use of data, often privately held at the origin, underpins both opportunities and specific challenges related to digital epidemiology. The other defining character of digital epidemiology is its use of computational and analytical methodologies originating in computer science, such as machine learning, computer vision, natural language processing and more.[10]

Other success stories of digital epidemiology have been based on a more participatory/empowerment model of disease surveillance. In the case of Influenzanet,[11] FluNearYou and Flutracking, for example, citizens acted as self-reporting volunteers and shared self-reported information on symptoms to allow for better comprehension of the determinants of influenza-like illness.[12]

With regards to the measures adopted or being contemplated against COVID-19, we are seeing proposals that rely on data generated outside of public health systems, such as the use of telecommunications for tracking population movements for the classical epidemiological goals of understanding the causes and spread of a virus. However, and this is perhaps the breakthrough novelty of the current circumstances, there is also an institutionalisation of the use of software applications (eg a mobile phone app) that are designed to generate data that not only would be relevant from an epidemiological point of view, but also would be used by public authorities effectively as a form of public health risk management.

Whilst the examples of digital epidemiology carried out in the past decade such as GFT, Influenzanet or HealthMap demonstrated the potential of using digital data as an increasingly valuable proxy for human behaviour for the purpose of scientific research, the proposed integration of these techniques within public health systems of interventions that are "born digital" raises a completely different set of governance and regulatory challenges.

In fact, although digital epidemiology as a scientific domain is a decade old, its integration in public health systems has been, before the outbreak of the SARS-CoV-2 pandemic, almost non-existent. It is true that, for example, looking at the European level, there had been instances in which public health authorities explored these new methods of digital intelligence, particularly with regards to the monitoring of digital

[8] L Bengtsson et al, "Improved Response to Disasters and Outbreaks by Tracking Population Movements with Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti" (2011) 8(8) PLoS Medicine e1001083.

[9] M Salathé, "Digital Epidemiology: What Is It and Where Is It Going?" (2018) 14(1) Life Sciences, Society and Policy 1.

[10] Various studies have used computer vision algorithms to speed up the process of disease detection: S Robertson et al, "Digital Image Analysis in Breast Pathology – From Image Processing Techniques to Artificial Intelligence" (2018) 14 Translational Research 19; M Usman, "Retrospective Motion Correction in Multishot MRI Using Generative Adversarial Network" (2020) 10(1) Scientific Reports 1; R Singh, "Deep Learning in Chest Radiography: Detection of Findings and Presence of Change" (2018) 13(10) PLoS One e0204155.

[11] SP Van Noort, CT Codeço, CE Koppeschaar, M Ranst, D Paolotti and MG Gomes, "Ten-Year Performance of Influenzanet: ILI Time Series, Risks, Vaccine Effects, and Care-Seeking Behaviour" (2015) 13 Epidemics 28.

[12] MS Smolinski, AW Crawley, JO Olsen, T Jayaraman and M Libel, "Participatory Disease Surveillance: Engaging Communities Directly in Reporting, Monitoring, Responding to Health Threats (2017) 3(4) JMIR Public Health Surveillance e62.

sources in order to detect potential disease outbreaks in a timely manner[13] or with regards to the use of mobile apps or social media for pharmacovigilance purposes.[14] But in the context of the COVID-19 pandemic crisis, the focus has markedly shifted towards a fast uptake of digital tools, and in particular the mobile phone app for contact tracing, in public health strategies.

III. The institutionalisation of the COVID-19 contact tracing app

Similarly to the many research projects exploring the application of digital technologies to disease detection, a number of projects used mobile phone signals to measure, understand and predict how individuals change their social behaviour in response to infectious disease.[15]

Software applications such as apps can be used to make mobile phones perform certain recording tasks that are potentially useful for aiding contact tracing, particularly given the fact that, in the case of COVID-19, the disease incubation period is relatively long and individuals that are pre-symptomatic or asymptomatic can spread the virus. Additionally, an app offers a scalable and easily deployable complement to the traditional system of retrieval of information and notification of potentially infected individuals. Therefore, a mobile phone app can be used as a tool for performing critical epidemiological functions,[16] and it has been part of the public health measures adopted during the pandemic outbreak by a number of Asian countries for tracing individuals at risk of developing the disease.

Therefore, by looking at the comparative efforts at the adoption of a contact tracing app and the problems caused by the lack of a pre-existing common regulatory framework, it is possible to gain insights into the challenges of digital public health.

Firstly, it should be observed that while the idea of a digital solution for contact tracing has officially become part of the envisioned European response to COVID-19,[17] there has been no attempt to create a European Union (EU)-wide digital tool, and each Member State is taking its own approach. Recognising the importance of this instrument but also the possibility for multiple national implementations, the European Commission

[13] SL Roberts, "Signals, Signs and Syndromes: Tracing [Digital] Transformations in European Health Security" (2019) 10(4) European Journal of Risk Regulation 722.

[14] A research project aimed at exploring the potential of new technologies such as mobile apps or social media listening for the purpose of pharmacovigilance by regulatory authorities is the WEB-RADR project; for more information, see <https://web-radr.eu>. For an overview, in general terms, of the ongoing efforts to integrate digital systems into public health strategies, see A Odone et al, "Public Health Digitalization in Europe: EUPHA Vision, Action and Role in Digital Public Health" (2019) 29 European Journal of Public Health 28.

[15] For example, the FluPhone project at the University of Cambridge: <https://www.cam.ac.uk/research/news/fluphone-disease-tr.cking-by-app>.

[16] L Ferretti et al, "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing", (2020) Science 10.1126/science.abb6936.

[17] Cf the Joint European Roadmap towards lifting COVID-19 containment measures: <https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf>; in particular, by referring to the Recommendation 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, particularly concerning mobile applications and the use of anonymised mobility data (C(2020) 2296 final).

has published a set of guidance and recommendations on the technical and legal aspects for the development of a contact tracing app[18] that the Member States should respect.

Secondly, the processes used by each Member State for the choice of the app model also reveal striking differences in terms of their transparency and the role played by technical expertise and that of the public or by the national parliaments. In France, for example, President Emmanuel Macron referred to the use of a digital application in the strategy of lifting the lockdown measures as one of the measures regarding which he invited the French Parliament to debate and approve.[19] Yet, it is not clear what type of contribution will finally be given by the parliamentary assembly.[20] In Italy and in The Netherlands, their governments have used a procurement-type procedure by launching a public call for app developers[21] to submit technical proposals for a model of a contact tracing app, and these governments have taken their decisions on the basis of an assessment of the models performed by experts appointed for this task. In the UK, the contact tracing app is being developed by the digital transformation service of the National Health Service (NHSX).[22]

Thirdly, it is envisaged that, before being rolled out to the public, the contact tracing app is to be tested or used under controlled conditions.[23] Testing of the app is considered useful for assessing the effectiveness of the proposed intervention, but also for fine-tuning critical parameters for alerting potential exposed individuals and for avoiding high rates of false positives that could overwhelm the logistical capabilities of the public health service downstream. However, there are no commonly agreed methodologies for assessing the risks or measuring *ex ante* the desired outcomes of digital interventions, and therefore there will be very little evidence available before the app is being promoted as a tool for contact tracing.

Therefore, the SARS-CoV-2 pandemic and the response from public authorities can be seen as a turning point for digital epidemiology and for the future role that digital tools will play in public health. It is too early to say whether this will be, ultimately, a success or failure; however, regardless of the final outcomes of these specific projects, we believe

[18] On 15 April 2020, the European Commission published a document entitled "EU Toolbox for the Use of Mobile Applications for Contact Tracing and Warning", which originates from a network of Member States' authorities, supported by the European Commission (the eHealth Network). This document aims at providing practical guidance to Member States for the development of contact tracing apps: the document is available at <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf>. On the same day, the European Commission also published guidance to ensure that contact tracing apps comply with data protection legislation: <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_669>.

[19] E Macron, *Adresse aux Français*, 13 April 2020 <https://www.elysee.fr/front/pdf/elysee-module-15482-fr.pdf>, in particular: "*Pour accompagner cette phase, plusieurs innovations font l'objet de travaux avec certains de nospartenaires européens, comme une application numérique dédiée qui, sur la base du volontariat et del'anonymat, permettra de savoir si, oui ou non, l'on s'est trouvé en contact avec une personne contaminée. Vous en avez sûrement entendu parler*".

[20] <https://www.politico.eu/article/macrons-coronavirus-tracking-app-sparks-controversy-in-his-own-camp>.

[21] For the Italian "fast call" project led by the Ministry of Digital Innovation, see <https://innovazione.gov.it/innova-per-l-Italia-la-tecnologia-e-l-innovazione-in-campo-contro-l-emergenza-covid-19>; for the Dutch case, see <https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/nieuws/2020/04/11/oproep-om-mee-te-denken-over-apps>. It is also worth mentioning here as an example of experimental governance that the seven app models shortlisted in The Netherlands would then be used for a public "*appathon*": <https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/nieuws/2020/04/15/ministerie-van-vws-organiseert-digitaal-evenement-voor-beoordeling-corona-apps>.

[22] See <https://www.theguardian.com/uk-news/2020/mar/31/nhs-developing-app-to-trace-close-contacts-of-coronavirus-carriers>.

[23] See <https://www.bbc.com/news/technology-52381103>.

that there are some important lessons to learn from this case. In particular, the public debate and the vexed governance process that has accompanied its emergence can provide important lessons for studies of risk regulation and, more generally, for future policy-making in this area.

In the considerations that follow, we will summarise a number of points concerning the risks stemming from the use of the contact tracing app that are generalisable to other digital tools for public health.

IV. The framing of risks of digital technologies for public health

It should first be observed that the introduction of a mobile phone app as a solution to implementing an effective form of contact tracing has been marred by incorrect assumptions and false dichotomies, the first and foremost being the one that accepts that there is a trade-off between the need to respect privacy/data protection and public health. For example, in some extreme instances, a plea has been made for a "temporary" suspension of privacy rights in order to allow the use of digital instruments of surveillance to fight the spread of the virus.[24] On the other hand, an argument has been made that the use of a mobile phone app for public health purposes is in reality a sort of "Trojan horse" that will make everyone accept more and more intrusive and dystopian forms of digital surveillance in our daily lives. It is certainly true that the implementation of such a privacy-invasive intervention could raise the risk of normalising digital surveillance.[25] In reality, the massive scale, granularity and quantity of personal data necessary for implementing a process of contact tracing does not prevent the implementation of serious governance and technical mechanisms to limit, to the maximum extent[26] possible, the interference with the right to privacy and the risk of a "slippery slope" towards generalised digital surveillance. Some of the technical approaches that are being considered are designed around privacy-by-design principles that include data minimisation: for example, decentralised digital contact tracing systems (such as the "DP3T" protocol[27]) store contacts' pseudonyms locally on a user's smartphone, and only transfer this information to a central server after a confirmed diagnosis, allowing risk scores of all of the other users to be updated in a decentralised computation so that no information about negative cases is ever collected and no centralised view of the (social) proximity graph is constructed.

[24] During the pandemic outbreak, the governor of the Italian region of Veneto, Mr Luca Zaia, suggested that privacy law could be temporarily suspended in order to let public health systems trace the contacts of infected people: <https://www.repubblica.it/politica/2020/03/26/news/zaia_sospensione_privacy-252373104>.

[25] See, eg, the considerations of V Dubal, "The Expansion of Mass Surveillance to Stop Coronavirus Should Worry Us All", *The Guardian*, 18 April 2020 <https://www.theguardian.com/commentisfree/2020/apr/18/mass-surveillance-coronavirus-technology-expansion>.

[26] See the recommendations of the European Data Protection Board (EDPB) contained in the "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak" adopted on 21 April 2020: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en>.

[27] See <https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf>.

An incorrect assumption is that digital tools for public health, similarly to apps developed by corporations for commercial purposes, should seek to obtain as much personal data as possible, even though there is no clear justification underpinning the acquisition of such data. In reality, this seems to be a misconceived approach. On the contrary, the collection of data that are not necessary for strict public health purposes increases the risk of "function creep": for example, whether geo-localisation data collected by a contact tracing app could be used for the purpose of enforcement of public order rules, or when it is proposed to mix the contact tracing purpose of the app with other functionalities, such as symptom reporting or telemedicine, which are not strictly necessary from an epidemiological perspective, but may serve other public health purposes, making it difficult to reason about the proportionality and risk/benefit balances of the primary function.

Another false dichotomy rests on the idea that, in order to be effective, the contact tracing app must be made mandatory (ie it has to be pushed into people's lives rather than "opted into"). In reality, this simplistic approach triggers risks of all sorts of adversarial scenarios and new "attack surfaces", leading to the possibility of new cybersecurity threats, organised protests and boycotts, spamming and flooding of the system.[28] On the contrary, a more collaborative, voluntary and interactive approach would enhance the empowerment and autonomy of citizens[29] and is more likely to lead to a bigger response by the population in terms of app downloads. It is perhaps relevant here to mention that even non-coercive, "nudging" techniques to promote the use of the app could negatively impact individual liberty, particularly with regards to vulnerable groups or individuals.[30]

Despite the fact that there is no available evidence of the effectiveness of digital contact tracing, some outspoken proponents of the contact tracing app seem to hold a misconceived belief that a complex and multi-layered issue such as the containment of COVID-19 in our societies can mainly be tackled by computer engineering and digital solutions. This type of technological solutionism raises a series of questions linked not only to the possibility of privacy violations, but also to social fairness. By ruling out or downplaying the current digital divide and the digital illiteracy of large parts of the population, the idea of a digital tool as the exclusive way to trace contacts of potentially infected persons during a pandemic would bring about unfair social discrimination resulting in different forms of health protection for those that have and those that do not have access to digital technologies.

Finally, it should also be acknowledged that a form of power asymmetry exists between public authorities and the big technology companies that own the app platforms. The latter are effectively in control of the digital infrastructure on which the digital tools designed for public health are supposed to operate and therefore can

[28] Security experts R Anderson and B Schneier have already warned about this type of risk; see, respectively, <https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world> and <https://www.schneier.com/blog/archives/2020/04/contact_tracing.html>.

[29] M Nanni et al, "Give More Data, Awareness and Control to Individual Citizens, and They Will Help COVID-19 Containment" (2020) 13(1) Transactions on Data Privacy 61.

[30] Cf the Statement of the IEEE regarding the ethical implementation of artificial intelligence systems (AIS) for addressing the COVID-19 Pandemic: <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/gieais-covid.pdf>.

make far-reaching policy decisions. Additionally, in the case of the contact tracing app, based on the public statement by Apple and Google,[31] it is envisaged that the contact tracing capabilities will be migrated into the operating systems of mobile phones (which remain the proprietary assets of private companies). This might have security and technical advantages for the functionality of the app; however, it also reduces the visibility of the technical implementation details. In summary, the public health function of the app can be designed and shaped by governments; however, these apps can only work via privately held platforms that ultimately maintain an important "gatekeeper" function.[32]

V. Concluding remarks

Since the first experimental applications of digital epidemiology, it could have been easily imagined that the concrete and visible digital transformation of our economies and societies would have led to a call for public authorities to make use of digital tools for public health. The current pandemic outbreak has catalysed the institutionalisation process of digital tools for public health and clearly highlighted current gaps in the public governance system.

On the one hand, the exploitation of digital data for public interest goals such as the fight against COVID-19 is increasingly accepted not only by the scientific community, but also by the public at large.[33] On the other hand, as we have illustrated with the contact tracing app for COVID-19, the system of public oversight of digital tools for public health is not yet prepared to address fully the ethical, social and legal challenges of these technologies. This creates a haphazard situation of potential conflict between technical expertise and public perception of risks, a situation that is widely known and examined in many domains of risk regulation.

Therefore, the institutionalisation of digital tools for public health also requires an institutionalisation of the regulatory framework for the design and deployment of these tools. The regulatory model of other risk technologies such as GMOs or medicines can offer a valid and proven blueprint, particularly regarding the procedures for the involvement of expert bodies, the mechanisms of participation and involvement of the public, the methodologies for assessing their effectiveness and risks[34] and finally the transparency requirements and responsibilities of the oversight bodies.[35]

---

[31] Cf <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology>.

[32] For example, on 14 March 2020, Apple took the decision to vet any app to be placed in the App Store to ensure that "data sources are reputable and that developers presenting these apps are from recognized entities such as government organizations, health-focused NGOs, companies deeply credentialed in health issues, and medical or educational institutions": <https://developer.apple.com/news/?id=03142020a>.

[33] M Ienca and E Vayena, "On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic" (2020) 26 Nature Medicine 463.

[34] See, Editorial, "Show Evidence That Apps for COVID-19 Contact-Tracing Are Secure and Effective" (2020) 580 Nature 563.

[35] The instance of transparency and public reviewability of the source code is included, with other requirements aimed at guaranteeing public oversight of the contact tracing app model, in the Resolution of the European Parliament of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)).

DIGITAL SOLUTIONS TO FIGHT COVID-19

2020 Data Protection Report

October 2020

Council of Europe

[*] The Council of Europe report, prepared on the basis of research by Anne-Christine Lacoste and Sjoera Nas, is available at the following page: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c

Cover and layout:
Documents and Publications Production Department (SPDP), Council of Europe

Photo: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Printed at the Council of Europe

Acknowledgments

This report has been prepared by the Data Protection Unit of the Council of Europe on the basis of the extensive work carried out by Anne-Christine Lacoste and Sjoera Nas, data protection consultants.

Table of Contents

Executive summary

2020 marks a turning point.

Challenges faced worldwide by our societies, governments and health care systems have provided a unique opportunity to reaffirm our founding values of democracy, rule of law and human rights.

Confronted with the Covid-19 health crisis, governments have been seeking to protect their populations and responding effectively to urgent and vital needs. Emergency measures have been adopted that have affected the enjoyment of the rights to privacy and data protection. To avoid undermining the bedrock of our societies, such necessary exceptional measures have to respect the general principles of law, remain proportional to the threat they address and be limited in time.

The pandemic has required swift and effective measures, leading to an increased use by governments of digital technologies to fight the spread of the virus, such as mobile applications installed on smartphones (apps), used for various purposes. This increased interest in new technologies has often been accompanied by a shift towards digital solutions offered by the private sector, public authorities working in cooperation with companies of the digital market.

The use of emerging technologies providing distance communication *in lieu* of human contacts, and algorithms replacing human intervention has simply exploded. Digital technologies used in public places to monitor population, at home, while teleworking or self-diagnosing, or when learning remotely became the new 'normal'.

This quantum-leap in the digitalisation of our lives requires that measures adopted by governments during the health crisis uphold the protection of individuals with regard to the processing of personal data. Privacy and data protection have a pivotal role, essential in building and sustaining trust in digital solutions. Those rights are not an obstacle to the protective responses adopted by governments, they are the guarantee that such responses will be taken in full consideration of human dignity and integrity.

Exceptional measures taken by governments must be provided for by law, respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.

Countries should pay particular attention to the following aspects when using technological tools which process personal data to combat the pandemic:

- the need for a **time limit** (applied to the retention period of all collected personal data) and legal sunset clauses;
- a legally guaranteed **purpose limitation** (the purpose of any processing must be precisely defined, and based on a specific legal basis, with the exclusion of further processing for any other purpose);
- **proportionality** of the measures taken and ongoing assessment of the proportionality considering the effective results of the measures (with the possibility to withdraw the measure where there is no concrete evidence of its benefits);
- cooperation with the **national data protection authority**, at early stages of the design of the processing, as well as at later stages (for example to process the feedback on a data protection impact assessment or an enforcement action);

- **transparency and explainability** of the data processing operations, especially for automated tracing tools (this notably includes the publication of the source code of the software, of impact assessments and security audits);
- **accountability** of data controllers, integration of **privacy by design**, realisation of **data protection impact assessments** of the processing and relevant security measures.

Greater awareness and compliance with those requirements contribute to increase the trust that individuals place in their governments and acceptance of the measures adopted in the general interest.

The role of international fora such as the Council of Europe is essential in recalling the path to take, issuing recommendations and guidance, enabling exchange of information and best practices. Such is the objective of the present report, to provide insights on what a significant number of countries have done to fight the pandemic, and how this complies with the applicable standards.

The manner in which the health crisis has been addressed prompts a reaffirmation of the resilience of the data protection principles as a key component of the effective functioning of our democracies. The future lies in our capacity to react promptly to new challenges without undermining our core values and putting our societies at greater risk on the longer term than do the present threats we have to address.

2020 DATA PROTECTION REPORT
Resilience of data protection frameworks in times of crisis

Introduction

2020 brought immense challenges to our societies. Governments had rapidly and effectively to respond to the exceptional and evolving situation linked to the Covid-19 pandemic.

The impact on human rights and fundamental freedoms of measures taken to curb the spread of the virus represents both a challenge to the resilience of data protection principles and an opportunity to test such resilience.

In respect of data protection, the digitisation of our societies has also been considerably accelerated by the crisis and the isolation imposed, which required many of us to work, to learn and to socialise at a distance.

This report gives an overview of the data protection landscape in that specific context of 2020, in the countries parties to the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (hereafter "Convention 108").

55 states[1] are parties to Convention 108, which has recently been modernised in order to adapt this landmark instrument to the new realities of an increasingly connected world, and to strengthen the effective implementation of the Convention. The Protocol[2] amending Convention 108 was opened for signature on 10 October 2018 in Strasbourg (CETS No. 223) and has since been signed and ratified by numerous countries to bring this modernised instrument, "Convention 108+", rapidly into force.

2020 brought another important change to the enforcement of the right to data protection in the field of transatlantic international data transfers, with the invalidation of the "Privacy shield" agreement concluded between the European Union (EU) and the United States of America (USA). The decision of the Court of Justice of the EU will affect international data flows and negotiations beyond the sole EU-USA scope and once again highlights the importance of Convention 108+ at a global level[3].

This report[4] contains two parts. The first part provides an overall analysis of legislative and key developments and their impact on the fundamental rights to privacy and data protection. The second part provides an in depth and technical review of the use of digital contact tracing applications and monitoring tools. The report contains an assessment of the main findings, with recommendations on how to ensure efficiency and resilience of the data protection framework.

The changes to the legal framework, governmental decisions, reactions of the private sector and the civil society are assessed against the principles of Convention 108. When the new principles of Convention 108+ are taken as a reference, such as the principles of accountability, privacy by design and by default, this is specifically mentioned in the report. Indeed, while Convention 108+ has not yet entered into force, its new principles represent a relevant reference for all current parties to Convention 108 (including parties that are members of the EU and already bound by equivalent provisions in accordance with the data protection legal framework of the EU).

1. List of countries available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
2. Text of Convention 108+ available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
3. Also see the Joint Statement of 7 September by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe on " Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services" at https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb
4. The present report takes into account positions and statements of the main oversight bodies and institutions at regional and international level, including the Council of Europe, the Fundamental Rights Agency of the EU and the European Data Protection Board, the Global Privacy Assembly, the World Health Organisation and the OECD, as well as reliable sources of information including academic work on constitutional matters, civil society publications and recent jurisprudence. It also relies on the replies to a questionnaire sent to parties to Convention 108 on data protection and the use of digital tools in the context of Covid-19.

I. Legal analysis of the legislative developments

Governments have been facing difficult challenges in seeking to protect their populations from the threat of Covid-19. This could alter the regular functioning of democratic societies and lead to measures which could infringe upon on rights and freedoms.

Convention 108+ allows the lawful use by governments of exceptions without necessarily having to adopt emergency measures (which include exceptional derogations). However, such exceptions must be provided for by law, respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.

> "Data protection can in no manner be an obstacle to saving lives and [..] the applicable principles always allow for a balancing of the interests at stake."
>
> "Data protection standards are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health, it is crucial to ensure that the necessary data protection safeguards are implemented when adopting extraordinary measures to protect public health." [5]

If it is necessary to go beyond those rules, a special law or decree in compliance with constitutional principles is required. However, the sole requirement of legal certainty does not guarantee that such derogations to individual rights are necessary and proportionate. Indeed, emergency measures have to comply with other specific requirements. In particular, any measure must be necessary and meet an important objective of public interest, and the essence of individual fundamental rights must be preserved, especially the rights of access, opposition and deletion of data[6].

A. Emergency measures

Due to the pandemic, most countries parties to Convention 108 have adopted emergency measures which restrict fundamental rights, based on the possibilities afforded by their own legal system.

Three main approaches can be identified:

- adoption of general emergency measures giving the government special powers (notably based on laws or decrees, in application of constitutional law);
- adoption of emergency measures in specific sectors, often based on public health or pandemic regulations;
- adoption of emergency measures without a specific legislative basis.

These different approaches have led to a patchwork of provisions in the 55 countries parties to Convention 108. Most provisions give extensive power to the governments, though usually only for a limited period of time.

Nine parties to the European Convention on Human Rights (ECHR) made use of Article 15 of the ECHR on derogation in time of emergency: Albania, Armenia, Estonia, Georgia, Latvia, North Macedonia, Romania, San Marino, and Serbia[7]. Such derogations must have a clear basis in domestic law in order to protect against arbitrariness and must be strictly necessary to the public emergency, in this case, fighting against the pandemic.

5. Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
6. The guidance provided by the EDPB with regard to the GDPR is equally relevant and valid in the context of Convention 108 : EDPB statement on the restrictions to data subjects rights in connection to the state of emergency in Member States, 2 June 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-restrictions-data-subject-rights-connection-state_en.
7. Reservations and Declarations for Treaty No.005 - Convention for the Protection of Human Rights and Fundamental Freedoms, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations

Measures range between national ones based on emergency processes clearly defined (where there is more transparency and legal certainty) and local or regional measures taken by local authorities. Whichever approach applies, the degree of intrusiveness of the measures adopted and their impact on individuals has in any case to be assessed.

The principles governing a state of emergency have been identified by the Venice Commission[8] and clarified in the toolkit published by the Secretary General of the Council of Europe[9], as follows:

- overarching principle of the Rule of Law
- necessity
- proportionality
- temporariness
- effective (parliamentary and judicial) scrutiny
- predictability of emergency legislation
- loyal co-operation among state institutions

Measures such as mandatory quarantines and lockdowns limiting the freedom of movement may be necessary to combat the Covid-19. However, it seems from available reports and in particular the report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe and the Bulletins of the Fundamental Rights Agency of the EU[10] that some of those measures do not always comply with these principles.

Even though such measures can be highly invasive and constitute important limitations to fundamental rights (privacy, data protection but also freedom of movement and assembly, and in some cases freedom of speech), the necessary oversight by supervisory authorities, parliaments and courts has sometimes been missing. Some constitutional courts have already issued rulings on some measures[11]. Other courts were prevented from fulfilling their role[12].

How emergency measures have impacted more specifically the rights to data protection and privacy, and especially the principles of Convention 108 and Convention 108+, depends on the nature of the measures adopted (secondary laws, decrees, decisions), their implementation and on the effectivity of oversight, including the judiciary and the supervisory authorities.

B. Analysis of the impact on specific provisions of Convention 108 and Convention 108+

1. Legal basis

Article 5 of Convention 108+ provides that the processing of data can be carried out on the basis of the "free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law", which, according to the explanatory report to the Convention[13], includes processing « necessary for the protection of the vital interests of the data subject or of another person, (…) for compliance with a legal obligation to which the controller is subject, and data processing carried out on the basis of grounds of public interest or for overriding legitimate interests of the controller or of a third party. »

As clearly recalled by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe in their joint statement of 30 March 2020[14], the catalogue of legal bases is broad

8. Reflexions on Respect for Democracy, Human Rights and the Rule of Law during States of Emergency, Venice Commission, available at https://rm.coe.int/respect-for-democracy-hu-man-rights-and-rule-of-law-during-states-of-e/16809e82c0
9. Council of Europe toolkit on respecting the rule of law in state of emergency, available at https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40
10. The impact of the Covid-19 pandemic on human rights and the rule of law, Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, available at https://pace.coe.int/en/files/28679
11. In the **Czech Republic**, although the Constitutional Court invoked a lack of competence to review the declaration of a state of emergency, it did annul some specific measures of the Ministry for Health. In **Romania**, the Constitutional Court annulled the quarantine rules adopted by the government as according to the Court, this limitation of the freedom of movement should have been based on a law adopted by the Parliament.
12. In **Hungary** for instance, ordinary courts were closed thus preventing the Constitutional Court review of the proportionality of measures introduced under emergency conditions as this procedure could solely be initiated by ordinary courts.
13. Explanatory Report, paragraph 46.
14. Joint Statement of 30 March on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter

enough to cover various data processing activities developed in the context of the Covid-19 crisis. Besides consent and necessity to process data based on the public interest, the vital interest of the data subject and of others can in particular cases be invoked to justify data processing for the purpose of monitoring of a life-threatening epidemic.

While the processing of data in the context of the fight against the pandemic can find its legitimacy in the Convention, the exceptional circumstances related to the vital threat and the public interest call at national level for additional and more specific regulation to ensure compliance with the principle of legal certainty. Such regulations should define the scope and purpose of the intended data processing.

Legal basis: legal obligation and public interest

Processing of personal data without a specific and appropriate legal basis has been denounced in particular by academia and civil society concerning a number of emergency responses adopted in some countries.

In **Greece** and in **France**, the use of drones triggered such concerns and legal action. In Greece, an NGO highlighted that the deployment of drones was based on a law which did not include any specific data protection guarantees and did not explicitly refer to the data protection legislation[15]. In France, two NGOs brought an action before the Conseil d'État. They flagged the absence of an explicit legal framework for the use of drones over Paris to monitor people's movement during and after the lock-down period. The Conseil d'État ordered the government to immediately cease the surveillance[16].

Though most countries parties to Convention 108 have made the use of Covid-19 mobile phone applications (apps) voluntary, this is not the case for isolation containment apps. In **Russia**[17] and **Turkey**[18], use of isolation containment apps is mandatory. **Slovenia**[19] appears to be the only country party to Convention 108 that has made the use of a proximity and contact tracing app mandatory by law, while subsequently announcing that its use would be on a voluntary basis.

Countries may invoke the legal basis of public interest with reference to health law provisions to contain a pandemic, or general provisions allowing regional authorities to maintain order. This ground has been invoked by countries that have introduced mandatory temperature scans at borders, airports, and public places or mandatory registration of contact data for visits to cafés and restaurants for the purpose of contact tracing. However, in order to successfully invoke this legal basis, there must be a very close link between the law and the public interest purpose, and the country must ensure that the processing is strictly necessary for this purpose.

A specific legal basis is essential to enable a public authority to process personal data for a determined purpose. Additional benefits of separate legislation, aside from due parliamentary process and legal certainty, are the possibility to introduce a sunset clause, as well as a legal requirement to obtain advice from the data protection authority, a legal obligation to conduct a data protection impact assessment and a requirement to implement appropriate data protection safeguards.

Use of telecommunications data requires specific attention. Telecommunications data are not only protected by general data protection law but also by specific regulations guaranteeing confidentiality of communications (constitutional protections of telecommunication secrecy). Even the mandatory processing of aggregated – and thus anonymous – data requires detailed legislation, since the creation of such statistics first requires an intervention from the telecom operators to process individual location data, for a purpose which is not part of their initial competence. In view of the data protection risks for individuals, countries cannot merely rely on the ground of public interest without specific legislation. This explains why a number of parties to Convention 108 adopted or amended existing telecommunication regulations, in order to allow for a wider processing of telecommunication data to create statistics.

15. Coronavirus pandemic in the EU – Fundamental Rights Implications – Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
16. Conseil d'État, Order of 18 May 2020, n° 440442, 440445, available at https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones
17. https://www.mos.ru/news/item/73074073/ See also Human Rights Watch, Russia: Intrusive Tracking App Wrongly Fines Muscovites, available at https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites
18. In Turkey, the app is mandatory for those diagnosed with Covid-19. Virus case tracking app launched in Turkey, Daly News, 19 April 2020, available at https://www.hurriyetdailynews.com/virus-case-tracking-app-launched-in-turkey-154005
19. Slovenian PM calls for mandatory coronavirus app against Commission advice Samuel Stolton, Euractiv, 8 July 2020, available at https://www.euractiv.com/section/digital/news/slovenian-pm-calls-for-mandatory-coronavirus-app-against-commission-advice/

Legal basis: consent

While consent is one of the possible lawful basis to process personal data, the requirements for consent to be valid are hard to meet, especially in view of the sensitivity of health and location data and in the Covid-19 circumstances, the pressure to accept processing due to the exceptional pandemic context. In the employment and educational context, consent is not considered as an optimal legal basis as, due to the imbalance of power, it is difficult to assess if it is freely given. In such circumstances, the legal obligations of the employer or the public interest obligations of educational institutions would be a more suitable ground, as suggested by the European Data Protection Board (EDPB) in its statement[20] on the pandemic. The inadequate use of consent was also pointed out by the data protection authority of **Slovenia** in the context of a legislative proposal concerning the processing of telecommunication data. This led to the withdrawal of the proposal before the law was adopted[21].

2. Purpose limitation, storage and sharing of data

Article 5.4.b) of Convention 108+ provides that personal data should be "collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes". Further use is not forbidden *per se*, and its compatibility with the original purpose depends on the details of the processing and the context. Further use of health data for scientific research, often based on coded or anonymised data, will not trigger the same limitations as their use in order to control individuals' movements or impose sanctions.

Compliance with this principle appears to be one of the major challenges in the context of the Covid-19 crisis. Confronted with an unknown and constantly evolving situation, some governments have adopted broad regulations giving them an extensive margin of manoeuvre.

It follows from reports[22] and replies to the questionnaire developed in part II, that boundaries between health care and police enforcement purposes have been sometimes blurred. In **Slovenia**, **Greece** and **Hungary**, health authorities share patients' lists with the police and other enforcement authorities. In **Austria**, mayors have access to some patients' data as they are in charge of providing food and services to those in quarantine. In the **Netherlands**, the municipal healthcare service has to report infection cases to the mayor of the municipality in which the patient resides as well as to the regional safety authority, with a view to allow the adoption of measures such as mandatory quarantine for those infected[23].

In **Hungary**, the Minister for Innovation and Technology as well as an operational body consisting of representatives of the Ministry of Interior, the police, and health authorities, are entitled by decree[24] to acquire and process any kind of personal data from private or public entities, including traffic and location data from telecommunication providers, with a very broad definition of the purpose for which data can be used. The decree also requires medical and health care universities and high schools to transfer students' data to the police, to fulfil the urgent need for extra public health staff. In **Denmark**, an executive order[25] first foresaw broad access by the police and the Danish Patient Safety Authority to personal data including bank transfers and communication data, before its scope was narrowed.

Some countries have published data on patients or deceased persons. Even if such data were presented as anonymised, published details such as age, gender, combined with location in regions with a low population density, enabled reidentification and further use. In **Montenegro**[26], directly identifiable data were published,

20. Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/ edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf
21. Statement of the Slovenian data protection authority of 20 March 2020, available at https://www.ip-rs.si/novice/epidemija-ne-sme-biti-razlog-za-ukinitev-ustavnih-pravic-1178/
22. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1 , Country reports - Coronavirus COVID-19 outbreak in the EU - Fundamental Rights Implications - April 2020 - Country research, available at https://fra.europa.eu/en/country-data/2020/coronavirus-covid-19-outbreak-eu-fundamental-rights-implications-april-2020
Recommendations on privacy and data protection in the fight against Covid-129, Access Now, March 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf
23. See details at the Dutch National Institute for Public Health and the Environment, available at https://www.rivm.nl/
24. Governmental Decree no. 46/2020 on prevention, avoidance of the mass human disease threatening the safety of human health and property, and on the measures taken in the state of danger in order to protect the health of the Hungarian citizens (III.) (*46/2020. (III. 16.)*, 16 March 2020, Article 13, available at http://njt.hu/cgi_bin/njt_doc.cgi?docid=218547.380736.
25. Bekendtgørelse om oplysningsforpligtelser samt behandling af personoplysninger med henblik pa˚ hindre udbredelse og smitte i forbindelse med haˆndtering af Coronavirussygdom 2019 (COVID-19), 30 May 2020 available at https://www.retsinformation.dk/eli/lta/2020/746 .
26. Montenegro publishes personal data of persons in isolation, 27 March 2020, available at https://privacyinternational.org/examples/3576/montenegro-publishes-personal-data-persons-isolation

with the full name of the infected persons. The same issue was raised in the **Czech Republic**[27], **Slovakia**[28], **Portugal**[29], **Romania**[30], and **Hungary**[31].

The duration of the storage of data is often unclear, especially when data are made public or are shared with several health or police entities. This issue was raised in **Greece**, on data related to quarantined persons. Even if few coercive measures were taken in this country, civil society expressed concern that the retention periods and further processing of personal data were not sufficiently clarified[32]. In the **United Kingdom**, the Coronavirus Act[33] foresees that the Secretary of State may make regulations to extend the time that biometric samples such as DNA and fingerprints may be retained for national security.

Data collected by tracing apps benefit, in the vast majority of parties to Convention 108, of a limited duration of storage: in the countries that use decentralised contact and proximity tracing apps, data are generally deleted after two weeks.

3. Proportionality

The intrusive character of measures adopted during the pandemic is at the core of reactions by many actors including data protection authorities, parliaments, courts and the civil society. The "fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake" foreseen in Article 5 of Convention 108+ has been assessed in different contexts.

Measures that cannot achieve their intended purpose can never be considered proportionate. However, the real effectivity of many measures has yet to be tested and examined, and debates regarding the proportionality of the interference with the right to data protection, in light of the evidenced and actual efficiency of the measure adopted are still underway.

In **Norway**, the data protection authority required suspension of the contact-tracing app because of the low number of downloads. This low number had an essential impact on the effectiveness of the tool, and the authority decided in an order of 12 June 2020 that the balance between privacy and necessity of the measures did not justify the processing of data, which had to be deleted[34]. In the **United Kingdom**, the government initially suspended the further development of its own proximity tracing app, after an extensive test on the Isle of Wight showed that only one person was notified through the app out of the 55 000 people that had installed it. It also revealed that the app could only correctly identify contacts on Android phones 75% of the time, and 4% of the time on iPhones. On 24 September 2020, the government launched a revamped version of the proximity tracing app, based on the Google Apple Exposure Notification System.[35]

Measures can also be disproportionate if their impact on the private life of individuals is too high. In **France**, the scope of the envisaged measures led to a reaction of the Senate: the emergency law project proposed an amendment[36] to permit, for a period of six months, "any measure" to allow the collection and processing of health and location data to deal with the COVID-19 epidemic. The degree of intrusion of the measure in the fundamental right to privacy was the reason for its rejection[37]. The State Data Protection Inspectorate of the Republic of **Lithuania** imposed a temporary limitation on the processing of personal data in the "quarantine" mobile app. for the possible breaches of Articles 5 (2) of the General Data Protection Regulation (GDPR)

27. *Prima*, Jonah experienced hatred on the Internet because he is infected with coronavirus, 25 March 2020, available at https://prima.iprima.cz/koronavirus-sars-cov-2/jonas-zazil-nenavist-na-internetu-protoze-je-nakazeny-koronavirem
28. Coronavirus COVID-19 outbreak in the EU, Fundamental Rights Implications, Country report, Slovakia, 4 May 2020, available at https://fra.europa.eu/sites/default/files/fra_uploads/sk_report_on_coronavirus_pandemic-_may_2020.pdf
29. Coronavirus COVID-19 outbreak in the EU, Fundamental Rights Implications, Country report, Portugal, 23 March 2020, available at https://fra.europa.eu/sites/default/files/fra_uploads/portugal-report-covid-19-april-2020_en.pdf
30. Coronavirus COVID-19 outbreak in the EU, Fundamental Rights Implications, Country report, Romania, 23 March 2020, available at https://fra.europa.eu/sites/default/files/fra_uploads/romania-report-covid-19-april-2020_en.pdf
31. Jogsértő Listát Közölt az Állam A Koronavírus Áldozatairól, 31 March 2020, available at https://tasz.hu/cikkek/jogserto-listat-kozolt-az-allam-a-koronavirus-aldozatairol
32. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
33. Coronavirus Act 2020, available at https://www.legislation.gov.uk/ukpga/2020/7/section/24/enacted
34. Order of the Norwegian data protection body of 12 June 2020, available at https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/midlertidig-stans-av-appen-smittestopp/
35. Digital Health, NHS Covid-19 contact-tracing app to be launched in England and Wales, 11 September 2020, https://www.digitalhealth.net/2020/09/nhs-covid-19-contact-tracing-launch-england-wales/
36. Amendement au Projet de loi, *Faire face à l'épidémie de Covid-19 - PJL*, available at: http://www.senat.fr/amendements/commissions/2019-2020/376/Amdt_COM-57.html
37. http://www.senat.fr/amendements/commissions/2019-2020/376/Amdt_COM-57.html and OECD Policy Responses to Coronavirus (COVID-19) - Ensuring data privacy as we battle COVID-19, available at http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/

of the EU[38]. In **France** again, the Conseil d'État acknowledged the claim of the French Human Rights league and ordered the suppression of thermal cameras in a school, as their use was considered disproportionate in respect of the right to privacy right of children[39].

In many parties to Convention 108, the measures taken in order to allow a wider processing of telecommunication data triggered specific reactions. According to Article 8 of the ECHR, they benefit from a specific protection under the principle of secrecy of correspondence and communications. The role of parliaments, and especially opposition groups, is visible in several instances. Some proposed measures were either stopped before adoption of the law or contested, in a few cases, before the constitutional courts.

In **Slovakia**, some members of the parliament filed a constitutional complaint against the telecommunications law allowing for access to telecommunications data for Covid-19 purposes, arguing that the scheme disproportionately infringed the rights of data subjects, and did not provide a robust control mechanism against possible misuse of the data. This has led the Constitutional Court to suspend[40] part of the measure before adopting its final decision[41]. A similar action was launched by members of parliament before the Constitutional Court of **Bulgaria** against rules allowing health and police authorities to use location data to track individuals, for violation of the right to privacy and the confidentiality of correspondence[42].

In **Croatia**, amendments foreseen in the Electronic Media Act[43] to track cell phones with a view to protect national and public security were blocked in the legislative process by amendments of the opposition[44].

In **Germany**[45] and **Slovenia**[46], a strong reaction from the data protection authorities led to a withdrawal of measures foreseeing wide processing of telecommunications data (and especially location data) to trace persons at risk, while in **Denmark**, human rights and tech associations raised strong concerns about the intrusiveness of the tracking of individuals with location data[47].

4. Security measures

Protecting data against unlawful access is all the more important considering the sensitive character of most of the data collected in response to the health crisis. Both data protection authorities and civil society have played a crucial role in verifying and reinforcing the security of the proposed digital solutions.

The Information Commissioner of **Slovenia** for instance identified, further to numerous complaints, security weaknesses on the website processing self-reported health data, and especially a lack of proper encryption. The website operators had to suspend the online activities of the site until the necessary improvements were brought to the system, including a privacy impact assessment[48].

In **Austria**, the source code of the contact-tracing app was reviewed by independent research organisations.[49] They identified weaknesses and inspired the developer to adapt the application.

38. Decision of the Lithuanian Data Protection Inspectorate of 25 June 2020, available at https://vdai.lrv.lt/lt/naujienos/nurodyta-laikinai-sustabdyti-programele-karantinas-del-galimai-netinkamo-asmens-duomenu-tvarkymo
39. Caméras thermiques à Lisses : le juge des référés ordonne de mettre fin à leur usage dans les écoles, available at https://www.conseil-etat.fr/actualites/actualites/cameras-thermiques-a-lisses-le-juge-des-referes-ordonne-de-mettre-fin-a-leur-usage-dans-les-ecoles
40. Decision of the Constitutional Court of Slovakia of 13 May 2020, PL. ÚS 13/2020-103, available at https://www.ustavnysud.sk/documents/10182/1270838/PL_+US+13_2020+-+Rozhodnutie+-+Uznesenie+z+predbezneho+prerokovania.pdf/464a47b6-66b4-4545-9a9f-eb0f10b4bd80
41. Slovakia: Change of Government under COVID-19 Emergency, Slavomíra Henčeková, Šimon Drugda, 22 May 2020, available at https://verfassungsblog.de/slovakia-change-of-government-under-covid-19-emergency/
42. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
43. Amendments to the Electronic Media Act, available at https://vlada.gov.hr/UserDocsImages/2016/Sjednice/2020/O%C5%BEujak/216 sjednica VRH/216 - 3.docx
44. Croatia's Response to COVID-19: On Legal Form and Constitutional Safeguards in Times of Pandemic, Nika Bačić Selanec, 9 May 2020, available at https://verfassungsblog.de/croatias-response-to-covid-19-on-legal-form-and-constitutional-safeguards-in-times-of-pandemic/
45. Statement of the Federal German data protection authority of 23 March 2020, available at https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_Novelle-InfektionsschutzG-Bundestag.html?nn=5217016
46. Statement of the Slovenian data protection authority of 30 March 2020, available at https://www.ip-rs.si/novice/epidemija-ne-sme-biti-razlog-za-ukinitev-ustavnih-pravic-1178/
47. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
48. Decision of the Slovene data protection authority of 3 April 2020, available at https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1503
49. Report on the findings of the organisations available at https://noyb.eu/en/report-red-cross-corona-app-reviewed-noyb

5. Transparency

Data controllers have the obligation under Article 8 of Convention 108+ to inform data subjects about several aspects of the processing, including their identity, the legal basis and purpose of the processing, the categories of data processed, recipients and the means for data subjects to exercise their rights.

In several parties to the Convention, data protection authorities insisted on the need to clearly inform individuals about the collection and processing of their data. This was the case in **France**, where the CNIL called for clear information about the functioning of the Covid tracing app and the conditions of deletion of data[50]. The lack of adequate information of data subjects was also flagged in **Hungary**, on how and for what purposes traffic and location data are processed, and in **Romania**, about the geo-tracking of people in quarantine[51].

As shown in more detail in the second part of this report, 20 countries actively published the source code of their apps. This transparency represents a significant and highly welcome change compared to the existing practice of software development.

6. Rights of the data subjects

Data protection authorities and regional bodies such as the EDPB and the Chair of the Committee of Convention 108[52] have urged to respect the rights of individuals in a context where many intrusive measures were being considered or adopted. In practice however, the exercise of rights such as the right of access or opposition as foreseen under Article 9 of Convention 108+ can be difficult for the data subjects. In some instances, these rights have even been formally restrained.

In **Ireland**[53] and in the **United Kingdom**[54], the data protection authorities formally expressed understanding for the position of data controllers who face time constraints due to the crisis and may be unable to reply to access requests within legal deadlines. While recalling that those deadlines are set by law, the authorities announced that, when examining claims of individuals, they would take into account extenuating circumstances or compelling public interests to the benefit of data controllers. The **British** Information Commissioner added however, that it would take a strong regulatory approach against organisations taking advantage of the health crisis to breach data protection laws.

Hungary on the other hand has formally limited individuals' fundamental rights by the decree 179/2020 of 4 May 2020. The government has adopted derogations to the GDPR, allowing data controllers involved in Covid-19 related data processing to suspend the fulfilment of data subjects' requests under Articles 15-22 of the GDPR, such as the right of access or erasure, until the state of emergency is revoked[55]. This has triggered several concerned reactions, including by the EDPB[56].

7. Automated decision making and use of AI

Article 9 of Convention 108+ protects individuals against automated decision making. It provides for the right "not to be subject to a decision significantly affecting (them) based solely on an automated processing of data without having (their) views taken into consideration". Data subjects also have the right to obtain knowledge of the reasoning underlying data processing applied to them.

In the context of the pandemic, this provision protects individuals against automated decisions affecting them directly, which would be based on personal data gathered by apps and other e-devices. The principle would apply, for instance, to immunity passports projected or developed in some countries such as **Argentina**,

50. Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », available at https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid
51. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
52. Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
53. Covid 19 and Subject Access Requests, 25th March 2020, available at https://www.dataprotection.ie/en/covid-19-and-subject-access-requests
54. The ICO's regulatory approach during the coronavirus public health emergency, 13 July 2020, available at https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf
55. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
56. EDPB response to NGOs on Hungarian decrees and statement on Article 23 GDPR, 3 June 2020, available at https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en

Germany and **Italy**[57], as long as they use health data of users to automatically decide on their freedom of movement. The purpose of such "immunity passports" or "risk-free certificates" would be to enable individuals to travel or to return to work assuming that they are protected against re-infection, based on the detection of antibodies. The World Health Organisation (WHO) has however warned that "there is currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection"[58] which raises doubts regarding the reasoning underlying the decision-making process and the validity of automated decisions taken by an app or a passport on such basis.

The same issues arise when AI is used in digital contact tracing apps, notably to help to calibrate the assessment of the risk of contamination, which may be questionable as without clear understanding of the contamination patterns, the construction of relevant mathematical models cannot be guaranteed.

In response to the questionnaire, **Croatia**, **Portugal**, **Morocco**, **Tunisia** and the **Slovak Republic** have indicated the use of AI in such apps.

8. Accountability, privacy impact assessment, privacy by design and by default

Convention 108+ includes new accountability obligations for data controllers in its Article 10. Among those is the obligation to make a specific assessment of the impact of a data processing activity on the fundamental rights of the data subjects. Including privacy by design and privacy by default in digital solutions developed to fight the pandemic is another essential element of the data protection framework.

The development of specific applications will be examined in more detail in the second part of this report, but some positive examples are worth mentioning here. Some governments have involved independent actors with an oversight role at an early stage of their actions and have shared the required impact assessments.

In **Finland** for instance, a parliamentary working group on information policy[59] was involved in the identification of data protection and privacy requirements before the contact tracing app was developed. Further to heavy criticism by the **Slovenian** data protection authority, a web-based project relying on self-reporting that enabled individuals to report symptoms, recovery and other Covid-19 related information, was suspended and put offline as long as the data protection impact assessment was not completed further to the authority's instructions[60].

In **France**, **Belgium**, **the Netherlands**[61] and **Italy** notably, data protection authorities were consulted prior to the development of a contact-tracing app[62], which sometimes led to substantial changes to the design of the application.

Privacy by design is also a key asset used by governments in their reflexions on whether to set up centralised or decentralised tracing apps. In their second joint statement[63] on digital contact tracing, the Chair of the Committee of Convention 108 and the Council of Europe Data Protection Commissioner considered that "digital contact tracing systems should be based on an architecture which relies as much as possible on the processing and storing of data on devices of the individual users". While no system can protect completely against security vulnerabilities and risks of re-identification, centralised storage presents more risks of further misuse of data than a decentralised system. Of the 55 countries parties to Convention 108, 14 have chosen such a centralised approach for proximity and contact tracing apps, while 26 countries have chosen a decentralised approach. In addition, 5 countries do not plan to use apps at all. Part II of the report describes in more detail the choices made by parties to Convention 108.

57. Covid-tech, the sinister consequences of immunity passports, Ella Jakubowska, EDRI, 10 June 2020, available at covid-tech-the-sinister-consequences-of-immunity-passports
58. Immunity passports in the context of Covid-19, scientific brief, WHO, 24 April 2020, available at immunity-passports-in-the-context-of-covid-19
59. The webpage of the parliamentary working group is available at https://tietopolitiikka.fi/en/members/
60. Decision of the Slovene data protection authority of 3 April 2020, available at https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1503
61. Dutch DPA, Privacy corona-apps not demonstrated (in Dutch only), available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-apps-niet-aangetoond
62. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 47, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
63. Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 28 April 2020, available at https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

9. Transborder data flows

The importance of reliable data analytics and benefits of sharing of data in the common efforts of both governments and private sector actors worldwide to combat the pandemic is striking. In that context, the application of transborder data flows regimes implies that personal data transferred from the jurisdiction of a party to Convention 108 continues to be appropriately protected wherever it flows.

Derogations exist, which require a case-by-case approach for each specific transfer that would be made outside the jurisdiction of parties to the Convention.

International transfers could for instance rely on the explicit, specific and free consent of the data subject who has been informed of risks arising in the absence of appropriate safeguards or on the basis of prevailing legitimate interests, in particular important public interests such as public health imperatives, where this is provided for by law and constitutes a necessary and proportionate measure.

Convention 108+ in its Article 14 and with the other principles it lays down protects the individuals while providing a framework for international data flow, which is even more acute and relevant in the context of Covid-19.

10. Enforcement and sanctions

Convention 108+ foresees in its Article 15 supervisory powers for data protection authorities, including the right to impose administrative sanctions and to engage in legal proceedings "or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention".

While supervisory authorities have been very active in issuing statements and recommendations, and also in accompanying governmental decisions in several instances, few coercive decisions have been taken[64]. This may be explained by the exceptional context and the option taken by most authorities to avoid antagonising the right to data protection and public health interests which may have led, in a crisis and emergency context, to disproportionate responses.

Civil society and NGOs[65] have been very active in triggering enforcement actions before courts.

C. Specific legislation and processing of personal data

Governments have adopted secondary legislation or amended existing laws in order to facilitate the management of the health crisis, touching upon the health sector but also the telecommunications sector.

The following practices have been permitted by legislative measures:

- use of mobile phone applications, for different purposes;
- use of traffic and location data from mobile phones and apps;
- use of other technical tools (eBracelets, smart cameras allowing for facial recognition, thermal scans, remote control by drones and robots, mandatory testing).

Few of these measures were adopted after completion of the appropriate legislative procedure, including parliamentary scrutiny. In many other cases no specific legal basis was considered necessary.

1. Mobile applications

The use of mobile apps has been one of the main technologies used by governments and companies to contain the pandemic and serving many different purposes. Although most countries developed apps to aid proximity and contact tracing, some other countries invested efforts in apps aimed at fulfilling other purposes.

64. See as one of the few examples, the order of the Norwegian supervisory authority to suspend the Covid tracing app: Order of the Norwegian data protection body of 12 June 2020, available at https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/midlertidig-stans-av-appen-smittestopp/
65. Such as the French action brought by « La Quadrature du Net » against drones, with the Conseil d'État, Order of 18 May 2020, n° 440442, 440445, available at https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones , and the Human Rights League's action against thermal scans in schools, with the decision available at https://www.conseil-etat.fr/actualites/actualites/cameras-thermiques-a-lisses-le-juge-des-referes-ordonne-de-mettre-fin-a-leur-usage-dans-les-ecoles

Examples of such other purposes are:

- information to population (news, general alerts, general instructions to avoid infections, maps to avoid hotspots);
- medical support (self-diagnosis, reporting, information to access to health services);
- crowd control (mandatory and non-mandatory applications - quarantine enforcement, forms for movement during lockdown, map travel patterns, record physical passage, contact and proximity tracing, report of violation of rules).

Some countries have used non-specific Covid-19 applications to map hotspots (**Czech Republic**) or send alert to populations (AlertSwiss in **Switzerland**).

The development and use of those digital solutions triggered opinions and statements from national and regional data protection bodies[66]. These opinions insist on the need for specific legislation to determine the purposes of data processing by the Covid-19 apps and to prohibit the processing of data collected for further purposes.

However, only a few countries prepared specific legislation - this was the case in **Norway**, **Italy, Belgium, France and Finland**[67] - and took the required preliminary steps to limit the impact of the tool on fundamental rights. In its answer to the questionnaire, Norway explained: "The legal foundation for the app is a dedicated regulation. The Parliament recently supported the use of a twofold purpose, with separate consents for each: 1) Contact tracing and 2) (aggregate) analysis of infection patterns and infection control impact. The app provides links to services for self-reporting of symptoms, but is not part of the (legal) purpose of the app." More detailed observations about the different types of apps and their purposes are provided in the second part of this report.

2. Use of traffic and location data from mobile phones and apps

The Joint European Roadmap prepared by the EU to support lifting the containment measures[68] encourages governments to process aggregate and anonymised data from social media and mobile network operators, to reveal patterns and trends in social mobility and help predict the spread of the virus. Such use of aggregated data[69] has actually been put in place in most parties to Convention 108, with the notable exception of the United Kingdom, Poland and the Netherlands[70].

The Joint Research Centre currently receives data from 14 mobile network operators in 19 EU member states (**Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden**) and **Norway**.

In **Germany** and **Denmark**, concerns were expressed regarding the irreversibility of anonymisation and potential third-party access to the data[71]. Similarly, in the **Netherlands**, the data protection authority issued an initial negative advice about a legislative proposal aimed at obliging telecom operators to systematically provide anonymised data to the national statistics agency (CBS).

Some countries process directly identifiable location data to help contain the spread of the virus. The **Polish** Covid Act[72] for instance, imposes an obligation on the telecommunication operators to provide location

66. EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf and Joint Statement on the right to data protection in the context of the COVID-19 pandemic, Alessandra Pierucci, Chair of the Committee of Convention 108, and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 14/05/2020, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
67. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 52, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
68. Joint European Roadmap towards lifting COVID-19 containment measures, 15 April 2020, p. 7, available at https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/european-roadmap-lifting-coronavirus-containment-measures_en
69. Information gathered from multiple sources and expressed in a summary form for purposes such as statistical analysis, to notably examine trends, make comparisons, or reveal information and insights that would not be observable when data elements are viewed in isolation.
70. The Joint Research Center has published a first set of three technical reports based on the data. See: https://ec.europa.eu/digital-single-market/en/news/coronavirus-mobility-data-provides-insights-virus-spread-and-containment-help-inform-future and https://ec.europa.eu/jrc/en/news/coronavirus-mobility-data-provides-insights-virus-spread-and-containment-help-inform-future.
71. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
72. Special Covid-19 Act of 2 March 2020 and subsequent Act of 31 March 2020, Act on special support instruments in relation to the spread of virus SARS-CoV-2 of 16 April 2020, available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000567

data of phones belonging to persons subjected to quarantine upon request of the Ministry of Digitalisation. The government also launched the mobile app "Home Quarantine" which allows police to monitor individuals' compliance with quarantine, including facial recognition technology and providing for fines in case of non-compliance[73].

In **Slovakia**, a new provision of the Electronic Communications Act[74] enables the public health authority to access phone-location data normally subject to telecommunication secrecy. Some data are processed in anonymised form, for statistical purposes of identifying, preventing and modelling threats to life and public health, but also to identify individuals who should be notified of special measures taken to protect their life and health.

Similar measures were adopted in **Bulgaria**. An amendment to the Law on Electronic Communication, implemented through the Law on Emergency, allows the police to request from telecommunication companies 'immediate access' to traffic data of users to control quarantine compliance, with *a posteriori* judicial oversight[75].

For the same purpose of quarantine control, telephone companies in **Mexico** are obliged to provide access to cell phone antennas to the Digital Agency for Public Innovation[76]. The province of **Santa Fe** in Mexico is allegedly requiring those who have violated quarantine to download an app that specifically tracks their movements[77]. In **Argentina**, the Ministry for Health developed an app that every visitor entering the country is legally required to install and use for 14 days. The app gives the ministry access to real-time location data.[78]. Similarly, in **Turkey**, it is mandatory for people infected with Covid-19 to download an app called "Life fits inside the house" (HES) as part of the "Pandemic Isolation Tracking Project." The app follows the movement of people instructed to self-isolate, and if they leave their homes, they receive a warning via SMS and are contacted instantly through automatic call technology and told to return to isolation. Use of the app is also mandatory for people wishing to travel by train or plane between cities in Turkey. Only if the app confirms that they have not been infected with the virus, will they be allowed to travel.[79]

In **Austria**, the law allows for the processing of identification and movement data by telecommunication providers in order for them to be able to send SMS warnings to end users[80]. Similarly, in **Lithuania**, following the adoption of a resolution declaring a state-level emergency, mobile operators are required to send text messages to customers requiring them to self-isolate when they return from foreign countries affected by the virus[81]. It is not clear if the mobile operators provide personal data to the relevant ministries.

3. Other digital solutions

Examples of other digital solutions and tools that have been put in place, often without a specific law, to help monitoring the spread of the virus, are:

- websites with health questionnaires;
- use of eBracelets;
- use of smart cameras allowing for facial recognition;
- thermal scans;

73. Details on the website of the Polish Government, at https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa-ruszyl-proces-jej-udostepniania
74. Slovakia: Change of Government under COVID-19 Emergency, available at https://verfassungsblog.de/slovakia-change-of-government-under-covid-19-emergency/
75. European Union Fundamental Rights Agency, Coronavirus pandemic in the EU – Fundamental Rights Implications, national report for Bulgaria, available at https://fra.europa.eu/sites/default/files/fra_uploads/bg_report_on_coronavirus_pandemic_-_may_2020.pdf
76. Statements on the web portal of the city of Mexico, available at https://cdmx.gob.mx/portal/articulo/cierre-de-centros-comerciales-por-emergencia-sanitaria
77. Controlarán a quienes incumplieron elaislamiento con una App en sus celulares, 23 March 2020, available at https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html
78. Disposición 1771/2020 on the Covid-19 application, adopted 25 March, available at https://www.boletinoficial.gob.ar/detalleAviso/primera/227170/20200326
79. Human Rights Watch, https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa See also: duvaR.english, Health Ministry's mobile app for travel may breach privacy law, experts warn https://www.duvarenglish.com/health-2/coronavirus/2020/05/25/health-ministrys-mobile-app-for-travel-may-breach-privacy-law-experts-warn/_ ore information about the Pandemic Isolation Tracking Project is available on the official site of the Directorate of Communications : https://www.iletisim.gov.tr/english/haberler/detay/director-of-communications-altun-shares-a-post-on-pandemic-isolation-tracking-project
80. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 55, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
81. This use of the telecommunications data was approved by the Lithuanian State Data Protection Inspectorate, Text Messages on the Coronavirus Pandemic to Persons Returning from Abroad are Sent Legally in Lithuania, available at https://vdai.lrv.lt/en/news/text-messages-on-the-coronavirus-pandemic-to-persons-returning-from-abroad-are-sent-legally-in-lithuania

- remote control by drones and robots;
- mandatory virus testing.

The processing of health data through websites and apps that encourage self-reporting of health-related data to health authorities while at the same time providing advice to individuals, is generally based on the (explicit) consent of individuals, while other digital solutions require a specific legal basis.

In nine countries (**Denmark, Finland, Ireland, Italy, Mauritius, Norway, Spain, Ukraine, and Uruguay**) websites are available with health questionnaires where people can report symptoms. A **Dutch** website from the RIVM (National Institute for Public Health and the Environment) was taken offline twice, due to structural information security problems.[82] It is important to note that the input to these health questionnaires can be used to publish maps indicating virus hotspots.

eBracelets are currently used in **Liechtenstein** and **Cyprus** and tested in **France**. **Liechtenstein** is testing an existing electronic bracelet that measures skin temperature, pulse, respiration and blood flow.[83] The Liechtenstein government funds the test on 2 200 of the 38 000 inhabitants of the principality, in the hope it can also detect Covid-19 infection in early stage.[84]

According to the answers to the questionnaire, wearable technology is also used in **Cyprus**, but no public information could be found. Bluetooth-enabled wristbands can also be used to enforce physical distancing, and collect information about compliance with this rule. The port of Antwerp[85] in **Belgium**, for instance started to use Bluetooth-enabled wristbands to enforce social distancing rules on the workplace. The wearables give off warning signals when workers come too close to each other.

Although the location data are only exchanged locally, proximity details are stored on a central server.[86] On its website, the Belgian data protection authority confirms that completely anonymous proximity tracing bracelets may be used on the workplace[87] and explicitly warns that such bracelets may not be used if (location) data of identifiable persons are used and stored. Such processing is only permitted based on the (explicit) consent of the employee, which is of concern in view of the imbalance of power between employees and employers.[88]

While none of the parties to Convention 108 currently have plans to make the use of wearables mandatory, it is interesting to mention developments in **Singapore**, as many countries were previously inspired by Singapore to develop contact tracing apps to contain the virus. Singapore is currently planning to equip all 5,7 million inhabitants with a wearable contact tracing device.[89] The Ministry for Health has not ruled out that use will be made mandatory. An online petition against use of the dongle has been initiated[90] and privacy advocates have warned on the risks of placing Bluetooth sensors in public places, *de facto* turning the dongles into potential population location trackers.[91]

Drones and robot surveillance are used to monitor compliance with physical distancing measures in public spaces, notably in **Greece**, **Belgium** and **Hungary**[92]. Robots with thermal imaging cameras have been

82. *MBS News*, RIVM website infection radar temporarily offline after data breach, 7 June 2020, available at https://www.mbs.news/en/2020/06/rivm-website-infection-radar-temporarily-offline-after-data-breach-inland.html.
83. ICO Liechtenstein, What a COVID-19 Bracelet Says about Liechtenstein, 7 August 2020, available at https://www.ico.li/what-a-covid-19-bracelet-says-about-liechtenstein/
84. *Basler Zeitung*, Liechtenstein als Corona-Labor, Fruchtbarkeits-Armbänder gegen das Virus, 18 April 2020, available at https://www.bazonline.ch/das-liechtenstein-experiment-867253873911 See also the manufacturer information, available at https://www.avawomen.com/ava-bracelet-for-covid-19/.
85. The company that produces the bracelets writes: "*When an employee is infected, the company physician can consult the wearable register to retrieve the identities of the colleagues that have been too close to the employee during the previous two weeks.*"
86. Bracelets, Beacons, Barcodes: Wearables in the Global Response to COVID-19, available at https://www.globaldiasporanews.com/bracelets-beacons-barcodes-wearables-in-the-global-response-to-covid-19/ See also : https://rombit.be/covid-solutions/
87. Belgian data protection authority, Covid-19 on the work floor (in Dutch only), https://gegevensbeschermingsautoriteit.be/burger/thema-s/covid-19/covid-19-op-de-werkvloer
88. Ibidem.
89 Reuters, Singapore plans wearable virus-tracing device for all, 5 June 2020, available at https://www.reuters.com/article/us-health-coronavirus-singapore-tech-idUSKBN23C0FO.
90. *Change.org*, Singapore says 'No' to wearable devices for Covid-19 contact tracing, available at https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing
91. *BBC*, Coronavirus: Why Singapore turned to wearable contact-tracing tech, 5 July 2020, available at https://www.bbc.com/news/technology-53146360
92. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, op. cit., p. 56.

used for the same purpose in **Tunisia**[93]. Drones have also been used to record people's temperature in **Croatia**[94] and equipped with cameras for crowd control in **Cyprus**[95].

Smart cameras can be used in various ways, from facial recognition used to control quarantine compliance, as is the case in **Moldova**[96] and **Russia**[97], to automated recognition of masks in public transports, as developed in a **French** project[98].

Thermal scans are also being widely used to monitor access to public and private premises, increasingly in airports. In **Argentina**, **Cyprus**, **Estonia**, **Mauritius**, **Spain**, and **Ukraine**, thermal cameras are used for fever detection, including mounted on drones.[99] The use of infrared thermometers triggered reactions from several data protection authorities. The **Dutch**[100], **Lithuanian**[101] and **Portuguese**[102] authorities stated that the use of thermal scans by employers is illegal, while others like the **Belgian** authority questioned the legal basis for their use in airports[103]. The **Spanish**[104], **French**[105] and **Cypriot** data protection authorities[106] issued general reminders about the strict application of the data protection framework to thermal scans.

The most recent development concerns plan of mandatory testing of visitors, as well as inhabitants. In **France**[107] and **Germany**[108], visitors from certain countries could be subjected to mandatory testing of the presence of the virus.

Both in **Monaco** and **Andorra**, announcements refer to the testing of the entire population to examine the presence of the virus[109].

Regardless of the type of test used (viral or antibody) mandatory testing is a highly invasive measure as it involves the use of biometric samples to detect the health status of individuals. Its deployment will have to be weighed in light of the effectivity of the system in limiting the spread of the virus, knowing that the virus may go undetected, while it may take 1 to 3 weeks for antibodies to be present after an infection and that there is still a lack of scientific evidence on immunity and contagion aspects.

4. Increase of teleworking and distance learning

Many countries have adopted lockdown measures, which led to a rapid uptake of teleworking and distance learning, and heavy reliance on new digital solutions. Such digital solutions have the potential to lead to additional intrusions in the private life of individuals as they imply significant processing of personal data of a sensitivity as it belongs to the most intimate sphere of the individuals.

93. Coronavirus: Tunisia deploys police robot on lockdown patrol, Rana Jawad, 3 April 2020, available at https://www.bbc.com/news/world-africa-52148639
94. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
95. Answer to the questionnaire but no public information sources provided.
96. Moldova: Transnistria uses facial recognition to identify quarantine violators, 23 March 2020, available at https://privacyinternational.org/examples/3629/moldova-transnistria-uses-facial-recognition-identify-quarantine-violators
97. 100 000 cameras: Moscow uses facial recognition to enforce quarantine, 24 April 2020, Sam Ball, available at https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine
98. La détection automatique des masques dans le métro parisien remise en cause, Armelle Exposito, 13 May 2020, available at https://ateliers.cfjlab.fr/2020/05/13/la-detection-automatique-des-masques-dans-le-metro-parisien-remise-en-cause/
99. Answers to questionnaire CoE, no public information sources provided.
100. Statement of the Dutch supervisory authoirity on thermal scans, 24 April 2020, available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-temperatuur-meten-mag-niet-zomaar
101. Statement of the Lithuanian DPA on Personal Data Protection and Coronavirus COVID-19, 16 March 2020, available at: https://vdai.lrv.lt/en/news/personal-data-protection-and-coronavirus-covid-19
102. Statement of the Portuguese supervisory authority on the unlawfulness of the use of thermal scans by employers, 23 April 2020, available at https://www.cnpd.pt/home/orientacoes/Orientacoes_recolha_dados_saude_trabalhadores.pdf
103. Statement of the Belgian supervisory authority on the legal basis for thermal scans in Brussels airport, 17 June 2020, available at https://www.autoriteprotectiondonnees.be/citoyen/controles-de-temperature-lapd-prend-contact-avec-brussels-airport
104. Statement of the Spanish DPA regarding the taking of temperature by shops, work centers, and other establishments, 30 April 2020, available at https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos
105. Statement of CNIL on the use of thermal scans and smart cameras in relation to the pandemic, 17 June 2020, available at https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras?
106. Statement of the Cypriot DPA on the use of thermal scans, 24 April 2020, available at http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/798C8B6809EBDC87C2258554004137CB?OpenDocument.
107. *Forbes*, 16 High-Risk Countries Face Mandatory Covid Tests In France, 24 July 2020, available at https://www.forbes.com/sites/tamarathiessen/2020/07/24/us-16-countries-mandatory-covid-tests-france/
108. Reuters, Germany fights virus uptick with mandatory testing for travellers, 6 August 2020, available at https://www.reuters.com/article/us-health-coronavirus-germany-cases-idUSKCN252074T.
109. https://all-andorra.com/13-latest-covid-19-updates-and-events-across-the-country-as-of-wednesday-25th-march-2020-20h/. See also : *ARD*, Tageschau, Andorra testet alle, 2 April 2020, available at https://www.tagesschau.de/ausland/andorra-coronavirus-101.html

In the majority of cases, the use of these digital solutions was not decreed or organised via legislation. Instead, employers, doctors, schools and universities simply began to use freely available tools, sometimes without the necessary anticipation and consideration of the potential data protection impact.

Data protection authorities have expressed concerns about the following issues notably:

- legal basis for the processing of employees and students' data;
- risks of constant on-line monitoring;
- disproportionate access to the terminal and private home of the individual (screenshots);
- risk of function creep;
- data security.

In **Italy** for instance, the supervisory authority recalled that data processed for teaching purposes may not be used for other purposes. It also raised cybersecurity concerns, as did the authorities of the **Netherlands** and **Sweden**. The data protection authorities also addressed the difficulty of obtaining a valid consent as the legal basis for the data processing. In view of the imbalance of power between employers and employees at work, or between students and their teachers, it is very difficult to meet the threshold of *freely given* consent.

In a **Dutch** court case, students from the university of Amsterdam tried to obtain prohibition of the mandatory use of online proctoring software to take tests during the pandemic. In summary proceedings, the judge explained that the measure was necessary to execute the public task of the university, and proportionate, as long as there were no alternative means of taking exams in a physical classroom[110].

Guidance on distance learning was published in **Greece**, the **Netherlands**, **Portugal**, **Sweden**, **Italy** and **Lithuania**[111]. The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe also provided recommendations in that respect[112]. They stress the need for data protection oriented standard configurations, with a view to limit the data collection to what is strictly necessary, recall the need of full transparency about the processing of data, the choice of a proper legal basis and the approval of parents in this respect.

With regard to teleworking, and the processing of health data of employees, many data protection authorities have emphasised the need to apply the same requirements of privacy by design and by default. While details of the guidance may differ due to specific national health and labour law, the supervisory authorities have generally insisted on the need for a proper legal basis and minimisation of the collection of data. The data protection authorities share a preference for a collection of data limited to general risks exposure, rather than explicit health data including medical diagnosis. In **Luxembourg**, **France** and **Belgium**, for instance, employers' questionnaires including such health data have been forbidden due to the sensitivity and specific protection of that data. Proportionality of the measures, balanced with the existence of a specific risk, is a widely shared requirement[113].

110. District Court Amsterdam, 11 June 2020, ECLI:NL:RBAMS:2020:2917, available at http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2020:2917 Student Proctoring Software Gets First Test Under EU Privacy Law, 29 July 2020, available at https://news.bloomberglaw.com/tech-and-telecom-law/student-proctoring-software-gets-first-test-under-eu-privacy-law.
111. Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2, European Union Fundamental Rights Agency, 28 May 2020, p. 56, available at https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1
112. Joint Statement on the right to data protection in the context of the COVID-19 pandemic, Alessandra Pierucci, Chair of the Committee of Convention 108, and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 14 May 2020, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.
113. EU Member State Data Protection Authorities Deal with COVID-19: An Overview, p. 4 and s., Christina Etteldorf, EDPL, 2/2020, available at https://www.lexxion.eu/wp-content/uploads/2020/03/COVID-19-Special-Data-Protection-Authorities-Deal-with-COVID-19.pdf

II. A case-study: the use of digital solutions

When the impact of the Covid-19 pandemic became clearer, many parties to Convention 108 started to develop digital solutions and technical tools to control the dissemination of the virus. Most countries focussed on the use of apps. Though most countries developed apps to aid contact tracing, some countries also invested efforts in apps to help people with self-diagnosis of symptoms, or to enforce containment measures.

The Council of Europe sent a questionnaire on 27 May 2020 to the 55 parties to Convention 108.

The questionnaire consisted of 5 questions with multiple choice answers and limited free space for additional information:

1. Do public authorities in your country plan to use or already use Covid-19 apps? If so, for what of the mentioned purposes?
2. What guarantees will, or do, the Covid-19 apps offer to ensure the right to respect for private life and the protection of the personal data of those concerned?
3. To your knowledge, do these apps use artificial intelligence (machine learning) and if so, for what purpose?
4. Do public authorities in your country plan to use, or already use, other information technologies to monitor and/or control the spread of Covid-19?
5. Is the data protection authority (in the countries where it exists) involved in the development, deployment, control of any app or other technology listed above?

47 recipients answered the questionnaire, out of which 6 are African and Latin American parties to Convention 108[114] and the analysis that follows is based on the replies made. In order to get a more complete overview of digital solutions implemented in the countries parties to Convention 108, external news and aggregation sources were also used, as referenced in footnotes[115]. The situation rapidly evolving, changes may have occurred in some countries after the publication of this report and readers are invited to consult the latest national references for a fully up-to-date information.

Governments and stakeholders involved in the fight against the pandemic have been relying on data analytics and digital solutions to fight the spread of the virus, by notably using mobile location data to evaluate movements of population or to enforce confinement measures, using devices as digital proof of immunity, symptoms' detection, self-testing, or digitally tracing the contacts of an infected person. This first digital solution, which was the most broadly considered worldwide is the first to be examined.

114. No answers were received from Azerbaijan, Greece, Malta, Montenegro, Poland, the Republic of Moldova, the Russian Federation and Turkey. In view of the low spread of the virus in the Principality and the uncertainty as regard its population's acceptance, the authorities of Monaco decided that such a system was not necessary. Of the non-respondent countries, only Greece and Montenegro do not seem to have any digital contact tracing app.
115. Relevant sources that were checked for information about (new) contact tracing apps, are: XDA developers list of countries with apps, available at https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/, MIT Technology Review Covid Tracing Tracker, available at https://public.flourish.studio/visualisation/2241702/ , European Commission, Open Source Solutions helping to tackle COVID-19, available at https://joinup.ec.europa.eu/collection/digital-response-covid-19/open-source-solutions#Tracking , European Mhealth solutions for managing the covid-19 outbreak, available at https://mhealth-hub.org/mhealth-solutions-against-covid-19, Github European contact tracing apps for Android, available at https://github.com/ct-report/summary and List of Covid-19 Apps at https://docs.google.com/spreadsheets/d/1qfbhFZbWCXd4GspSD6LL8CNmgzKEYtL-gQQk1gEKqrk/edit#gid=0

A. Digital contact tracing apps

Looking manually at contact tracing (and alerting) has always been used in epidemic monitoring to reduce the spread of infections and consists in identifying the persons who may have come into contact with an infected person to alert them, where necessary, and allow them to get the necessary care and self-isolate to avoid further spread of the disease.

With this health crisis, mobile apps have been seen by many as a complementary response to the need to rapidly perform such contact monitoring, with sometimes limited consideration of the absence of evidence of their efficacy, and thus of the proportionality of the measures adopted.

Mobile apps are a computer program (or software application) designed to run on a mobile device (a smartphone or tablet computer) rather than on desktop or laptop computers.

In order for the mobile devices to communicate possibly with other devices, a protocol establishes the set of rules determining how the data will be transmitted.

Regarding digital contact and proximity tracing, various protocols have been developed since the beginning of the health crisis, providing different functionalities.

The table below provides an overview of the existing protocols used in digital contact and proximity tracing.

Table 1 – Existing protocols

Name	Origin	Centralisation	Link
Exposure Notification	Apple and Google	Decentralised	https://www.apple.com/covid19/contacttracing
Blue Trace/ Open Trace	Singapore Government Digital Services	Semi-centralised	https://github.com/opentrace-community
DP-3T (Decentralized Privacy-Preserving Proximity Tracing)	EPFL, ETHZ, KU Leuven, TU Delft, University College London – UCL, CISPA, Oxford, University, Torino University, ISI Foundation	Decentralised	https://github.com/DP-3T
OpenCovidTrace	1Checkin, Evocativideas, MLM Holdings, Nebula Ventures, open source community, Quantstellation	Decentralised	https://opencovidtrace.org https://github.com/OpenCovidTrace
PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing)	Fraunhofer Institute for Telecommunications, R. Koch Institute, Technical University of Berlin, TU Dresden, Erfurt University, Vodafone Germany	Semi-centralised	https://github.com/pepp-pt/pepp-pt-documentation
PACT: Private Automated Contact Tracing	MIT Computer Science and Artificial Intelligence Laboratory, Massachusetts General Hospital, MIT Lincoln Laboratory, MIT Media Lab, Boston University, Weizmann Institute of Science, Brown University		https://pact.mit.edu
Privacy-Sensitive Protocols And Mechanismsfor Mobile Contact Tracing (PACT)/ CovidSafe	Microsoft volunteers, University of Washington		https://arxiv.org/abs/2004.03544 https://github.com/covidsafe
RecoVer	Softmining, Nexus TLC, Minervas (Trucky), Pushapp		https://www.smcovid19.org/recover/

Name	Origin	Centralisation	Link
ROBERT (ROBust and privacy-presERving proximity Tracing protocol)	Inria	Semi-centralised	https://github.com/ROBERT-proximity-tracing
TCN Protocol (Temporary Contact Number)	CovidWatch, CoEpi, ITO, Commons Project, Zcash Foundation, Openmined	Decentralised	https://github.com/TCNCoalition/TCN
Tensho	CryptIQ		https://github.com/cryptiqdev/tensho
Whisper Tracing Protocol	Nodle, Coalition Network		https://github.com/NodleCode/coalition-android https://www.coalitionnetwork.org/

A key difference in approach, embedded in the protocol, is the choice between centralised data collection by the national (possibly health) authorities versus decentralised data processing.

The main difference with the centralised contact tracing apps is that all proximity data, including the Bluetooth strength, are exclusively calculated on, and processed in, the app.

If users are diagnosed with the virus, they can choose to upload the data they have collected from other nearby Bluetooth devices to an application server from a designated health authority. Every app periodically downloads the temporary exposure keys shared voluntarily by other infected users, and compares these keys with the random codes registered in the previous days as a result of contacts with other users with the app. If a match is found, the application runs an algorithm on the device which, depending on the estimated duration and distance of the contact, and in accordance with the criteria established by the health authorities, decides whether to display a notification on the user's device exposed to the risk of contagion. The notification warns the user of the match, its date, invites him to self-confirm, and contact the health authorities. This technical design of the app prevents users from involuntarily sharing personal data with other users, or with the health authorities.

To prevent false positives, the protocol foresees the use of unique codes generated by the health authorities. Users first have to upload such a unique code in the app after they have tested positive, before their app sends its logfiles to the server.

Table 2 below shows whether countries have chosen a central approach for their proximity and contact tracing apps, or a decentralised approach. For countries without an app, the URL of official information is shown, usually from the Ministry for Health in that country.

Of the 55 countries parties to Convention 108, 14 have chosen a centralised approach for proximity and contact tracing apps (some solutions are actually semi-centralised, such as the app used in **France** or apps using the PEPP-PT protocol). In **Norway**, the use of the centralised tracking app is suspended due to data protection concerns.

In total, 25 jurisdictions have chosen a decentralised approach (**Austria, Azerbaijan, Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, the British Overseas Territory of Gibraltar (hereafter Gibraltar), Ireland, Italy, Latvia, Malta, Morocco, Netherlands, Poland, Portugal, Slovak Republic, Slovenia, Spain, Switzerland, Tunisia, United Kingdom** and **Uruguay**). Apps using the DP-3T protocol or the Google Apple Exposure Notification System (GAEN) follow a decentralised approach.

In addition, 6 countries do not plan to use a contact tracing app at all (**Bosnia and Herzegovina, Greece, Liechtenstein, Luxembourg, Mauritius** and **Sweden**). In **Lithuania** , a private sector initiative for a contact tracing app was abandoned.

In 10 countries, the technical approach retained is unclear, with the probable use of an app from a neighbouring country (**Andorra**, **San Marino**), or because the app is still in development, or there are no plans to use an app for contact and proximity tracing (**Albania, Cabo Verde, Georgia, Montenegro, Moldova, Senegal, Serbia** and **Ukraine)**.

Table 2 – Digital contact tracing apps: central or decentral approach

Jurisdiction	Name of application	Government information about the app or official information on the app	Central	Decentral
Albania	Unknown.	https://www.kryeministria.al/en/?s=corona&post_type=newsroom		
Andorra	(for self diagnosis)	https://visitandorra.com/en/covid-19-in-andorra/		
Argentina	CuidAR	https://www.argentina.gob.ar/jefatura/innovacion-publica/acciones-coronavirus/aplicacion-y-tableros-de-gestion	√	
Armenia	COVID-19 Armenia	https://play.google.com/store/apps/details?id=am.gov.covid19	√	
Austria	Stopp Corona	https://at.roteskreuz.stopcorona		√
Azerbaijan	Watch COVID (COVİD izlə)	https://apps.apple.com/az/app/covid-izle/id1511326016		√
Belgium	In development[116]	https://www.info-coronavirus.be/en/		√
Bosnia and Herzegovina	No plans to introduce app.	https://covid-19.ba/		
Bulgaria	Virusafe – not BLE but GPS	https://virusafe.info/	√	
Cabo Verde	unknown	https://covid19.cv/		
Croatia	Stop COVID-19	https://www.total-croatia-news.com/news/45331-croatia-presents-its-stop-covid-19-app		√
	Digital Assistant Andrija	https://andrija.ai/		
Cyprus	COVTRACER	https://covid-19.rise.org.cy/en/ https://www.pio.gov.cy/coronavirus/en/index.html	√	
Czech Republic	eRouška ("eFace-Mask")	https://koronavirus.mzcr.cz/en/		√[117]
	Mapy.cz	https://en.mapy.cz/		
Denmark	Smittestop	https://com.netcompany.smittestop_exposure_notification		√[118]
Estonia	Covid app – in development	https://e-estonia.com/trace-covid-19-while-respecting-privacy/		√[119]
	Immuunsuspass – In development[120]			
Finland	Ketju - In development[121]	https://thl.fi/en/web/thlfi-en/-/corona-application-trial-starts-on-tuesday		√[122]
	Selfdiagnosis	https://www.omaolo.fi/		
France	STOPCOVID	https://www.economie.gouv.fr/appli-stop-covid-disponible	√	
Georgia	Stop Covid	https://stopcov.ge/		
Germany	Corona-Warn-App	https://www.coronawarn.app/de/		√
Greece	No app			
Gibraltar	Beat Covid Gibraltar	https://www.gibraltar.gov.gi/beatcovidapp/privacy		√

116. https://www.computable.be/artikel/columns/overheid/6963986/5658341/blyaert-betwist-geen-corona-app-voor-eind-september.html
117. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting June 2020, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf page 4.
118. Ibid and https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/
119. Ibid.
120. https://medicalxpress.com/news/2020-06-estonia-virus-immunity-passport-app.html
121. https://github.com/ct-report/summary
122. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020, page 4.

Hungary	VirusRadar	https://virusradar.hu/	√	
	HKR	https://hazikaranten.hu/	√	
Iceland	Rakning C-19 App	https://www.covid.is/app/is	√	
Ireland	Covid Tracker	https://www.hse.ie/eng/services/news/newsfeatures/covid19-updates/covid-tracker-app/		√
Italy	Immuni	https://www.immuni.italia.it		√
Latvia	APTURI COVID	https://www.apturicovid.lv/#en		√
Liechtenstein	No app	https://www.liechtenstein.li/land-und-leute/gesellschaft/gesundheitswesen/corona-virus/		
Lithuania	App suspended by DPA	https://koronastop.lrv.lt/en/news/useful-and-meaningful-self-isolation-with-a-mobile-app-quarantine		
Luxembourg	No app	https://coronavirus.gouvernement/en.lu.html		
Malta	In development	https://deputyprimeminister.gov.mt/en/health-promotion/covid-19/Pages/landing-page.aspx		√[123]
	Covid-19 Check	https://covid19check.gov.mt/		
Mauritius	No app	http://www.covid19.mu		
Mexico	COVID-19 MX (self-diagnosis & info)[124]	https://play.google.com/store/apps/details?id=mx.gob.cdmx.adip.covid19cdmx&hl=en_US		
Monaco	Uses French app	https://en.gouv.mc/Portail-du-Gouvernement/Policy-Practice/Coronavirus-Covid-2019	√	
Montenegro	No app	http://www.gov.me/en/homepage/measures_and_recommendations/		
Morocco	Wiqaytna	www.wiqaytna.ma/		√
Netherlands	Coronamelder in development	https://coronamelder.nl/corona		√
	OLVG corona app – self diagnosis	https://www.olvg.nl/de-corona-check		
North Macedonia	Stop Korona!	https://stop.koronavirus.gov.mk/en	√[125]	
Norway	Smittestopp – suspended by DPA 6/16[126]	https://www.fhi.no/en/id/infectious-diseases /coronavirus/use-of-smittestopp-privacy-policy/ & https://helsenorge.no/coronavirus/smittestopp	√	
Poland	ProteGO Safe	https://www.gov.pl/web/koronawirus/protegosafe		√[127]
	Kwarantanna domowa	https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa--ruszyl-proces-jej-udostepniania		
Portugal	STAYAWAY COVID In development	https://covid19estamoson.gov.pt/app-estamoson-covid19/		√
Republic of Moldava	Unknown	https://ansp.md/index.php/category/actualizarea-situatiei-privind-coronavirus/		
Romania	Unknown			
Russian federation	Social Monitoring	https://www.mos.ru/news/item/73074073/	√	
San Marino	Unknown, can probably use Italian app	http://www.iss.sm/on-line/home/artCataggiornamenti-coronavirus.49004093.1.20.1.html		

123. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020, page 4.
124. The Ministry for Health (Federal Public Administration Agency) of the Mexican government developed and launched the application COVID-19 MX to help self-diagnosis, find nearby hospitals and provide statistics.
125. https://stop.koronavirus.gov.mk/en
126. https://github.com/ct-report/summary
127. European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting June 2020, page 4.

Senegal	Unknown. Appears to be Daancovid19	https://daancovid19.sn		
Serbia	Unknown	https://covid19.rs/eng-instituteforpublichealth-updates/		
Slovak Republic	COVID19 Zostan Zdravy	https://www.dhis2.org/covid-19	√	
Slovenia	Ostani Zdrav In development	https://www.gov.si/en/news/2020-07-30-application-for-protecting-public-health-and-lives-is-anticipated-to-be-available-in-mid-august/		√
Spain	Radar COVID. In development[128]	https://www.mineco.gob.es/portal/site/mineco/menuitem.2efe1f7b4e40d4856c8a0f35026041a0/?vgnextoid=de1969e8c9b11710VgnVCM1000001d04140aRCRD + regional apps, such as https://play.google.com/store/apps/details?id=org.madrid.CoronaMadrid		√[129]
Sweden	No plans to introduce app	https://www.government.se/government-policy/the-governments-work-in-response-to-the-virus-responsible-for-covid-19/		
Switzerland	SwissCovid	https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-728718249		√[130]
Tunisia	E7mi (contact tracing)	https://e7mi.tn/faq_ar.html		√[131]
	Stop Corona (self-diagnosis)	https://www.stopcorona.gov.tn/		
Turkey	HES (Life fits inside the house)	https://play.google.com/store/apps/details?id=tr.gov.saglik.hayatevesigar&hl=en_US	√	
Ukraine	Name unknown	https://covid19.gov.ua/ & https://www.kmu.gov.ua/news/projdi-observaciyu-vdoma & https://moz.gov.ua/koronavirus-2019-ncov		
United Kingdom	New NHS Covid-19 launched 24 Sept. 2020	https://covid19.nhs.uk/		√
Uruguay	CoronavirusUY (self- diagnosis)	https://www.gub.uy/ministerio-salud-publica/coronavirus		√[132]

1. Centralised tracing apps

Inspired by the Singapore Trace Together app and the South Korean Corona 100 app, for example the **United Kingdom**, **Germany**, **Hungary**, **Slovenia**, **Malta** and **France** started to develop centralised contact tracing apps. In total, 14 countries have apps with a centralised data collection. Some countries were inspired by the Pan-European Privacy-Preserving Proximity Tracing protocol (PEPP-PT). This first generation of apps raised many privacy alerts, as these apps sent contact logs with pseudonymised personal data to a central (government) back-end server after a user reported to be infected with the virus. This centralised approach allowed the recipient authority to calculate the proximity, and individually notify other users of the app of potential contact with an infected person. On 19 April 2020, the approach chosen by PEPP-PT was strongly criticised by over 300 security and privacy academics from 26 countries. Though many countries have since moved to a decentralised model of contact tracing, and the centralised apps deployed in the **United Kingdom**

128. https://english.elpais.com/society/2020-06-29/spain-launches-first-phase-of-coronavirus-tracking-app.html
129. *El Pais*, Spain launches first phase of coronavirus-tracking app, 29 June 2020, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf
130. https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-728718249
131. https://e7mi.tn/faq_fr.html and https://e7mi.tn/presentation.pdf, only available in Arabic.
132. https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

and **Norway** were suspended for lack of effectivity, **France** continued with a semi-centralised approach, launching StopCovid.[133]

In **Bulgaria**, the government developed a contact tracing app based on GPS location data, instead of Bluetooth data. The app *Virusafe* aims at assisting the competent authorities in organising and controlling the anti-epidemic measures imposed in the country. The controller of the personal data processed through the app is the Ministry for Health. Use of the app is voluntary and all data processing, including data about health and geolocation data, is based exclusively on consent.

In **Cyprus**, in addition to the use of ebracelets, a proximity tracing app is deviced. The purpose is to check the users' location trails and identify the places a carrier has visited and in turn, locate other contacts who have been in close proximity with the diagnosed carrier.

In **Hungary** and **North Macedonia**, a contact tracing app (named *Virusradar* in Hungary and *StopKorona!* in North Macedonia) requires users to provide a mobile phone number. The user receives a code via SMS that is necessary to register with the app, which entails the possibility to establish a connection between the phone number and the app's unique ID. Like other contact tracing apps, *Virusradar* uses Bluetooth to communicate with other users and exchanges encrypted, anonymous data about the distance of surrounding devices if they have been at a dangerous distance for the past 14 days. Users can choose to share their data with epidemiologists, but they can also be asked by professionals to share their data, thereby notifying people who have been in close contact with an infected person. Hungary and North Macedonia have chosen slightly longer time and distance limits than most other countries: 20 minutes within 2 metres distance, instead of 15 minutes within 1.5 metres distance.[134]

2. Decentralised tracing apps

25 respondents have indicated that the decentralised approach has been retained in the development of their apps.

Numerous parties to Convention 108 already use, or plan to shortly use , the DP-3T protocol or the Google Apple Exposure Notification System (GAEN). These are: **Austria, Belgium, Croatia, Denmark, Estonia, Finland, Germany, Ireland, Italy, Latvia, Malta, Poland, Portugal, Slovenia, Spain, Switzerland, the Netherlands** and the **United Kingdom**.

The privacy policy of the **Spanish** RadarCovid app provides an interesting level of detail[135].

In **Austria**, the Red Cross Stop Corona app was reverse engineered by security firm SBA Research. In a joint analysis with NOYB-founder Max Schrems, they concluded the app complied with data protection laws, even though the app transmits a mobile number to the Red Cross servers.

Belgium initially did not plan to launch a proximity tracking app. In **Luxembourg**, members of parliament urged the government in May 2020 not to introduce a digital tracing app. They insisted on four necessary conditions should the government decide to develop an app: "the app should protect privacy, disclose the source code, communicate with other European apps and not allow data identifying individuals to be collected centrally."[74] In Belgium, the government finally decided to launch after the summer its Coronalert app.

The **Danish** *Smittestop* app was based on the Norwegian example with the same name, with the difference that the Danish app is based on the GAEN system and does not collect additional location data on top of the bluetooth exchanges. The reason the Norwegian app developers initially choose to collect other location data was due to the fact that more than half of Norwegians use iPhones and prior to the launch of the GAEN system, iPhones were not recording the data when users were not actively using the app.[136]

Italy explains that it uses data from the app to monitor the evolution of the epidemic and to enhance the accuracy of the model through which the app establishes whether the contact is sufficiently at risk as to trigger a notification. It is not clear how Italy obtains data from the app, which allegedly operates in a decentralised way.

133. *RFI*, France's Covid-19 tracking app has only identified 14 people at risk, 24 June 2020, https://www.rfi.fr/en/science-and-technology/20200624-france-s-covid-19-tracking-app-has-only-identified-14-people-at-risk
134. *Hungary today*, Coronavirus: New App to Track Nearby Positive Cases Available to Download, 14 May 2020, available at https://hungarytoday.hu/coronavirus-hungary-app-virusradar/ North Macedonia, StopKorona!?, available at https://stop.koronavirus.gov.mk/en
135. RadarCovid privacy policy (in Spanish), available at https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html
136. *DR*, Danish corona app 'according to Norwegian model': This is what you can expect, (in Danish only), 8 April 2020, available at https://www.dr.dk/nyheder/penge/dansk-corona-app-efter-norsk-model-det-kan-du-forvente

Latvia underlined the decentralised nature of the app, based on a voluntary use, with all data remaining on the device. It is only when a user chooses to provide contact information that a notification is sent from the device to the health authority with the contact phone number, date and duration of the contact with the infected person. The logs on the app are automatically deleted after 14 days. With regard to the purpose of contact tracing, the use of the app is presented as making it possible to achieve the goal of detecting new cases of the disease more efficiently and in a more precise way.[137]

B. Other purposes

Although most countries deviced apps for the purposes of proximity and contact tracing, some countries invested efforts in apps aimed at achieving other purposes. Some of these purposes operate at a general level to bring assistance and guidance to users, while others imply more intrusive and coercive features with a view to control the spread of the pandemic.

Examples of such other purposes are:

- provide general news and information about the pandemic;
- help people with self-diagnosis of symptoms;
- provide instructions to avoid infection;
- provide information about access to health services;
- create maps to help people avoid virus hotspots;
- enforce containment measures;
- fill in a form about reasons for movement during lockdown;
- map travel patterns from inhabitants;
- create daily statistics of recorded cases;
- record physical passage of visitors at entry and control points;
- allow users to submit online reports about the violation of rules by other people;
- provide crowd control.

Table 3 below shows the different purposes for which countries use such apps, based on the answers to the questionnaire, as completed with publicly available information sources.

Table 3 – Different purposes of the apps

Jurisdiction	Name of application	Purpose(s)						
		Contact tracing/ Proximity Alert	Self-diagnostic	Containment check	Crowd control	Map travel patterns	Immunity passport	Other
Andorra	In development		√					
Argentina	CuidAR		√	√	√	√	√	
Armenia	COVID-19 Armenia	√	√					√
Austria	Stopp Corona	√		√	√			
Azerbaijan	Watch COVID (COVİD izlə)	√						√
Belgium	Coronalert	√						
Bulgaria	Virusafe – not BLE but GPS	√	√					
Croatia	Andrija		√					
Cyprus	COVTRACER	√						
Czech Republic	eRouška	√				√		
Denmark	Smittestop	√						
Estonia	In development	√						

137. Latvian Data Protection Inspectorate, in Latvian only, Stop Covid does not track people, available at https://www.dvi.gov.lv/lv/zinas/mobila-lietotne-apturi-covid-neizseko-personas/

Finland	Ketju In development[138]	√	√					√
France	STOPCOVID	√						
Georgia	Stop Covid	√				√		
Germany	Corona-Warn-App	√						
Gibraltar	Beat Covid Gibraltar	√						
Hungary	VirusRadar	√		√				
Iceland	Rakning C-19 App	√						
Ireland	Covid Tracker	√	√					√
Italy	Immuni	√						√
Latvia	APTURI COVID	√	√					
Liechtenstein	No app but wearable	√						
Lithuania	Coronavirus – No longer available	√	√					
	Quarantine app suspended			√				
Luxembourg	No app							
Malta	Covid- 19 Check		√ [139]					
Mexico	Self diagnostic		√					
Monaco	French app	√						
Morocco	Wiqaytna	√	√					
Netherlands	Coronamelder In development	√						
	OLVG Corona app		√					
North Macedonia	Stop Korona!	√						
Norway	Smittestopp – suspended 6/16[140]	√				√		
Poland	ProteGO Safe	√						
	Kwarantanna Domowa		√	√				
Portugal	STAYAWAY COVID In development	√						
Russian federation	Social Monitoring			√				
San Marino	Unknown			√				
Senegal	Daancovid19	√	√	√		√		
Serbia	Unknown							
Slovak Republic	COVID19 ZostanZdravy	√		√				
Slovenia	Ostani Zdrav In development	√						
Spain	Radar COVID		√					
Switzerland	SwissCovid	√				√		
Tunisia	Stop Corona	√						
	E7mi		√					
Turkey	HES	√	√	√		√	√	
Ukraine	Name unknown		√	√		√		
United Kingdom	NHS Covid-19 contact-tracing app	√						
Uruguay	CoronavirusUY	√	√					

In **Finland, Lithuania, Malta, Mexico,** the **Netherlands, Poland** and **Slovenia** apps and websites are developed for self-diagnosis. In Finland, a web-based symptom checker has been implemented. The symptom checker enables anyone to analyse his/her symptoms, get reliable guidance/information and contact health care for further guidance and testing. A similar website with a health questionnaire from the Dutch National

138. Source: https://github.com/ct-report/summary
139. *Malta Independent*, Coronavirus: Take the test – web app launched, 30 April 2020, available at https://www.independent.com.mt/articles/2020-04-30/local-news/Coronavirus-Take-the-test-web-app-launched-6736222624\
140. Source: https://github.com/ct-report/summary

Institute for Public Health and the Environment was taken offline twice due to structural information security problems. The website should have shown an anonymised map of the Netherlands showing zones with high grades of infection.[141] As described in the first part of this report, the Slovenian website was suspended pending completion of a Data Protection Impact Assessment.

The **Lithuanian** app enables daily coronavirus symptom tracking, and the receiving of health advice and information. The **Mexican** app gives direct access to the epidemiological health care telephone number and provides a map that identifies the closest health units to the user's location. The app also provides information about the virus, tips to prevent infection and official government news about the pandemic. In **Uruguay**, the CoronavirusUY app is aimed at people that suspect they are infected with the virus. In a second phase, all people that have been diagnosed with the virus will be invited to download the app. The Uruguayan Ministry for Health has assured that the app does not collect geolocation data of the app users, and that the data are not used for any other purpose.[142]

In **Armenia**, the Covid-19 app is presented as producing daily statistics of recorded cases, (legal) decisions, a list of medical institutions, instructions to avoid infection, as well as tools for public control, including an opportunity to submit an online report on violations of the rules by other people or to fill in a mandatory electronic movement form.

In **Azerbaijan**[143] and **Ireland**, the app provides news and information sources about the pandemic. The app in Azerbaijan enables direct contact to the Anti-Coronavirus Hotline in one touch.

Only two countries that answered the questionnaire (**Argentina** and **Austria**) plan to use the app for crowd control, while seven countries plan to use data from the app to map (aggregated) travel patterns (**Argentina, Czech Republic, Georgia, Norway, Senegal, Switzerland and Ukraine**). In addition, **Turkey** uses its HES app to map intercity travels by train and by plane.

According to the answers to the questionnaire, eight countries plan to use the app to enforce quarantine measures. These countries are **Argentina, Austria, Hungary, Lithuania, Senegal, Slovak Republic** and **Ukraine**. It seems from public sources that **Poland**, **San Marino**, **Turkey** and **Russia** also use(d) an app for this purpose.

Initially, **Poland** only developed an app to enforce quarantine measures. Use of this Home Quarantine app would be mandatory for everybody that notified officials they had contracted the virus, or because they returned to Poland from abroad. The app collected detailed location data and required people to upload selfies when prompted so that officials could pinpoint their exact location.[144] The use of this app is not mandatory. Later, Poland also decided to develop a proximity tracing app based on the decentralised proximity tracking technology of GAEN.[145]

Hungary has also developed an app to enforce quarantine measures, The *Házi Karantén Rendszer* app (The Home Quarantine System, HKR). People who have been officially quarantined for Covid-19 infection have to be registered, and their location data are monitored. At randomly generated times, the HKR system sends remote control requests via SMS, and a health assessment questionnaire once a day. Users have to start the app within 15 minutes of receiving the request. The app automatically takes several pictures of the user, to provide proof of their identity and location. These data are then compared with the address of the home quarantine provided during registration.[146] The data are sent to the GP from the patient, and are used in an aggregated, anonymised form to predict health needs.

Since April, based on a decree of the mayor of **Moscow**, infected patients must install the Social Monitoring app if they wish to do the quarantine at home. Prior to installation of the app, "the nurse takes a picture of the patient and records the data in an identity document. This information is transferred to a single data center

141. MBS News, RIVM website Infection radar temporarily offline after data breach, 7 June 2020, available at https://www.mbs.news/en/2020/06/rivm-website-infection-radar-temporarily-offline-after-data-breach-inland.html.
142. Uruguay Ministry for Health, Coronavirus UY: this is the app designed for those who suspect they have Covid-19, in Spanish only, available at https://www.elpais.com.uy/informacion/salud/coronavirus-uy-asi-app-covid-presento-gobierno-hoy.html.
143. Explanation in the app stores about the purposes of the Watch COVID" (*COVİD izlə*) app for iOS and Android devices, for Apple available at https://apps.apple.com/az/app/covid-izle/id1511326016
144. *Politico*, Poland's coronavirus app offers playbook for other governments, 2 April 2020, available at https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/
145. Reuters, Poland rolls out privacy-secure coronavirus tracking app, 9 June 2020, URL: https://www.reuters.com/article/us-health-coronavirus-poland-tech-idUSKBN23G208
146. Translated in English, the app description is: "Anyone who has been placed in official home quarantine can decide whether they want to take advantage of the HKR system by continuously fulfilling remote monitoring requests through the application or by undertaking personal police control during the quarantine period without using the application." Hungary, HRK app information (in Hungarian only), available at https://hazikaranten.hu/

and the "Social Monitoring" service."[147] On installation the app collects to confirm the phone number, and the user must make a selfie. After that, the app continuously collects location data from the smartphone. The Moscow authorities combine these data with city video surveillance to enforce quarantine orders. If a patient refuses to use the service, he or she faces a fine of 4 000 rubles. In addition, the patient will be placed in an observatory or medical facility and will not be able to return to home treatment. The tracking data are stored on the city hall's server for one year.[148]

Similarly, the **Turkish** Ministry for Health created the '*Hayat Eve Sığar*' (HES) app (*Life fits inside the house*) as part of the Pandemic Isolation Tracking app.[149] If citizens in quarantine leave their house, they immediately receive a warning via SMS. Persons that wish to travel by train or plane between cities in Turkey have to show a code from the app. Only if the app confirms that they have not been infected with the virus will they be allowed to travel.

Liechtenstein does not use a mobile app, but is testing[150] an existing electronic bracelet that measures skin temperature, pulse, respiration and blood flow.[151] The Liechtenstein government funds the test on 2 200 of the 38 000 inhabitants of the principality, in the hope it can also detect Covid-19 infection in early stage.

According to the answer received, wearable technology is also used in **Cyprus**.

Even if the use of such wearable technology is strictly voluntary, data protection risks exist for the users, as people may feel pressured to demonstrably wear the bracelet, while the reliability of measurements has not been proven and the potential consequences of a wrong conclusion about the health of the wearer can be serious (mandatory quarantine, exclusion from the workplace, social exclusion, stigmatisation, discrimination, etc).

C. Public engagement and private sector involvement

Although **Sweden** did not launch any official government app, researchers at Lund University in Sweden have launched a free app to help map the spread of infection in Sweden and increase knowledge of the coronavirus.[152]

In **Germany** and in the **Netherlands**, there was a fierce public debate about the privacy risks of a contact tracing app. In Germany, the development of the CoronaWarn app was critically followed by the federal data protection authority (BfDI) that did not see any objection against its use.[153] Germany conducted and published a very detailed data protection impact assessment.[154]

17 countries conducted a DPIA to mitigate high risks, but the DPIA was only published in 9 countries: next to **Germany**, in **Austria, Ireland, Mauritius, the Netherlands, Norway, Liechtenstein, San Marino,** and **Ukraine**. The United Kingdom announced it will also publish the DPIA at the public launch.

A number of privacy academics and experts in the **Netherlands** created a manifesto 'Safe against Corona', with 10 conditions for the app to comply with. In addition to the above mentioned criteria from the Parliament of Luxembourg (protect privacy, disclose the source code, communicate with other European apps and not allow data identifying individuals to be collected centrally), the Dutch signatories demanded that the app could only be used for one purpose (controlling the virus), that it should be demonstrably effective, that the

147. https://www.mos.ru/news/item/73074073/ See also Human Rights Watch, Russia: Intrusive Tracking App Wrongly Fines Muscovites, available at https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites
148. Idem.
149. Human Rights Watch, Mobile Location Data and Covid-19: Q&A, section Mobile Apps to Enforce Quarantine and Social Distancing Orders, available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa See also: duvaR.english, Health Ministry's mobile app for travel may breach privacy law, experts warn, available at https://www.duvarenglish.com/health-2/coronavirus/2020/05/25/health-ministrys-mobile-app-for-travel-may-breach-privacy-law-experts-warn/ More information about the Pandemic Isolation Tracking Project is available on the official site of the Directorate of Communications, available at https://www.iletisim.gov.tr/english/haberler/detay/director-of-communications-altun-shares-a-post-on-pandemic-isolation-tracking-project
150. *Basler Zeitung*, Liechtenstein als Corona-Labor, Fruchtbarkeits-Armbänder gegen das Virus, 18 April 2020, https://www.bazonline.ch/das-liechtenstein-experiment-867253873911 See also the manufacturer information, https://www.avawomen.com/ava-bracelet-for-covid-19/
151. ICO Liechtenstein, What a COVID-19 Bracelet Says about Liechtenstein, 7 August 2020, https://www.ico.li/what-a-covid-19-bracelet-says-about-liechtenstein/
152. https://www.lunduniversity.lu.se/article/covid-symptom-tracker-app-launched-sweden
153. German magazine *Datenschutz Praxis*, Data protection with the Corona-Warn-App: The most important facts, 18 June 2020, (in German only) available at https://www.datenschutz-praxis.de/fachnews/datenschutz-bei-der-corona-warn-app-die-wichtigsten-fakten/
154. Corona Warnapp DPIA (in German only), 15 June 2020, available at https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf

results should be reliable and verifiable through publicly, user friendly, available source code that use of the app should be temporary and never imposed through coercion by governments or third parties.

The development of a contact tracing app by the Dutch Ministry for Health was preceded by an *appathon*, with public presentations by seven selected app developers (chosen out of 700 proposals). [155] Immediately after the weekend, the Dutch data protection authority reported that it could not assess the privacy impact because of the unclear legal requirements and purposes and the seven proposals were also criticised in a security audit.[156] In the end, none of the seven proposed apps met the data protection requirements and the Netherlands is currently working on a new contact tracing app, developed under full public scrutiny, with a chat module open for all interested people and a github repository where the source code is published.

A similar open development approach, with intensive collaboration between public authorities, volunteers and the private sector, was chosen in **Estonia** and **Senegal**. In March 2020, **Estonia** organised a *hackathon* (*Hack the Crisis*) to inventorise good ideas to contain the Corona virus.[157] One of the winning ideas was a health monitoring app which can be used to track the extent of an outbreak. As well as helping users identify their symptoms, the app also warns of nearby virus hotspots.[158] Since April 2020, nine Estonian companies and several government institutions are developing a decentralised, privacy-preserving contact tracing application.[159]

In **Senegal**, a platform of more than 450 volunteer digital experts was set up. This initiative, called *Daancovid19*, involves people from the private sector, civil society, and the research and innovation sector. The platform was initiated by the Organisation of Information and Communication Technology Professionals (OPTIC), and was adopted by the Ministry for Health and Social Action (MSAS) and the Ministry of the Digital Economy and Telecommunications (MENT).[160] The call for digital solutions resulted in 29 different solutions, ranging from different types of tracking apps to a remote controlled robot to assist with the care for infected patients. According to the students from the technical university that presented the idea, *Docteur Car* should be able to measure temperature and deliver medicine and food. The robot should be able to speak multiple languages such as Wolof, Pulaar, French and English.[161]

D. Transparency and Open source

As shown in table 4 below, many countries have made the source code of their apps open source in order to increase transparency and provide a higher level of trust amongst the general public. The Free Software Foundation Europe keeps track of the apps, and has for example called on Denmark to release the code of the app under a Free Software (Open Source) license.[162]

Table 4 – Countries that publish the source code of the apps

Country	Name of application	Open Source URL
Austria	Stopp Corona	https://github.com/austrianredcross
Belgium	In development[163]	To be published on github
Cyprus	COVTRACER	https://github.com/ct-report/CY
Czech Republic	eRouška ("eFaceMask")	https://github.com/covid19cz?q=erouska

155. Dutch Ministry for Health, Welfare and Sport, Health ministry to hold digital event to test coronavirus apps, 15 April 2020, https://www.government.nl/ministries/ministry-of-health-welfare-and-sport/news/2020/04/15/health-ministry-to-hold-digital-event-to-test-coronavirus-apps
156. Dutch DPA, Privacy corona-apps not demonstrated (in Dutch only), available at https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-apps-niet-aangetoond
157. https://www.weforum.org/agenda/2020/07/estonia-hackathon-pandemic-covid19-technology/
158. https://www.velmio.com/corona-tracker
159. E-estonia, How do you trace Covid-19 while respecting privacy?, April 2020, https://e-estonia.com/trace-covid-19-while-respecting-privacy/
160. https://daancovid19.sn/
161. https://daancovid19.sn/communique-de-presse-daancovid19-29-solution-numeriques-referencees-dans-le-cadre-de-la-lutte-contre-le-coronavirus/
162. FSFE, Denmark keeps source code of Coronavirus tracing app secret, 29 June 2020, available at https://fsfe.org/news/2020/news-20200629-01.en.html
163. https://www.computable.be/artikel/columns/overheid/6963986/5658341/blyaert-betwist-geen-corona-app-voor-eind-september.html

Finland	Ketju In development[164]	https://github.com/ct-report/FI
France	STOPCOVID	https://github.com/ct-report/FR
Germany	Corona-Warn-App	https://github.com/ct-report/DE
Hungary	VirusRadar	https://github.com/ct-report/HU
Iceland	Rakning C-19 App	https://github.com/aranja/rakning-c19-app
Ireland	Covid Tracker	https://github.com/HSEIreland/
Italy	Immuni	https://github.com/immuni-app
Latvia	APTURI COVID	https://github.com/ApturiCOVID
Monaco	Uses French app	https://github.com/ct-report/FR
Morocco	Wiqaytna	https://github.com/Wiqaytna-app
Netherlands	Coronamelder In development	https://github.com/minvws
Norway	Smittestopp – suspended by DPA 6/16[165]	https://github.com/ct-report/NO
Poland	ProteGO Safe[166]	https://github.com/ProteGO-Safe
Slovak Republic	COVID19 ZostanZdravy	https://github.com/ct-report/SK
Switzerland	SwissCovid	https://github.com/ct-report/CH
United Kingdom	NHS Covid-19 contact tracing app	https://github.com/NHSX

The publication of the source code may help to build confidence in the system, as an important aspect of transparency, and provides means of control of the respect for the rights to privacy and data protection. According to a study about the acceptance of mock tracing apps by a researcher from the German university of Göttingen, arguments on societal benefits related to the use of apps were found among the most appealing elements even for the most sceptical and undecided persons.[167]

E. Users' expectations

Trust in such digital solutions is instrumental to the level of adoption, and thus the effectivity of the system. Users must be assured that their right to personal data will be respected and a lack of clarity in the purpose specification, mixed messages about the legal grounds, a failure to apply rigorous data minimisation and no fixed, or very long, retention periods seem to be amongst the common concerns of users.

In reply to the questionnaire, only 15 respondents indicate that the app data are exclusively provided to a national health authority bound by medical secrecy, with the explicit consent of users. The majority of countries that have answered share the data with other authorities too, on the basis of other legal grounds. These may be metadata[168] about the use of the app, or aggregated data. Similarly, data minimisations is only applied rigorously during collection and transmission in half of the responding jurisdictions, and only half of the respondents indicate that all data will be deleted after a fixed period of time.

An explicit legal sunset clause limiting the period of time of the use of the app is foreseen in **17 countries**. These are: **Bulgaria, Czech Republic, Denmark, Finland, Georgia, Italy, Latvia, Liechtenstein, Morocco, Norway, San Marino, Senegal, Slovak Republic, Netherlands, Tunisia, Ukraine and Uruguay**.

164. https://github.com/ct-report/summary
165. Idem.
166. https://koronazglowy.com/
167. Trang, Simon; Trenz, Manuel; Weiger, Welf H.; Tarafdar, Monideepa; Cheung, Christy. 2020. One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps, in: *European Journal of Information Systems*, available at https://www.tandfonline.com/doi/full/10.1080/0960085X.2020.1784046
168. Data that describes other data or an underlying definition or description of data (data about data). Metadata makes finding and working with data easier – allowing the user to sort or locate specific documents. Some examples of basic metadata are author, date created, date modified, and file size. Metadata is also used for unstructured data such as images, video, web pages, spreadsheets, etc.

- To conclude, it is important to stress that this global health crisis was also a unique opportunity to join forces in combating the Covid-19 and exchanging information and experience. Regretfully, in spite of numerous calls for coordination and interoperability of digital solutions, countries have individually implemented widely diverging systems, thereby indirectly limiting the efficiency of the measures taken, and depriving themselves of a possible influence that together, they could have exercised on actors of the digital market.

- Given the extremely tight time pressure imposed on all countries, scarce expertise and resources could have been more efficiently invested on research and development of common effective digital solutions. Measures that have been adopted and implemented in a haste have also affected the quality and effectiveness of the contribution and intervention of supervisory authorities and other competent advisory and oversight bodies. Supervisory authorities and other competent bodies should be given the means to carry out independent assessments of the elements provided to them by governments.

- To mitigate the risks of ad hoc measures or fragmented approaches and to contribute to the effectivity of applications by a large uptake, it is essential for governments and other relevant stakeholders to build trust together, closely involving the civil society and the general public in the development of those digital solutions and investing in transparency measures (publication of the source code, dissemination of the findings of data protection impact assessments, organisation of *hackathons/appathons*, etc).

Nathalie Martial-Braz

Nos données de santé en danger… quand l'arbre de la crise sanitaire cache la forêt de la perte de souveraineté !

Par Nathalie Martial-Braz, Professeure de droit privé, Université de Paris, Membre de l'Institut Universitaire de France

Le Health Data Hub (HDH), ou Plateforme des données de santé, est née aux termes d'un arrêté du 29 novembre 2019 de cette volonté, annoncée à grand bruit[1], de promouvoir des entrepôts de données prompts à nourrir des algorithmes d'intelligence artificielle nationaux ou à tout le moins européens, ce afin de « *conforter, en France et en Europe, l'écosystème de l'IA* ». La promesse était belle : la French Tech n'allait plus avoir à s'exporter et les GAFAM n'auraient qu'à bien se tenir ! La France allait devenir un champion de l'intelligence artificielle, notamment dans le domaine de la santé, grâce au trésor de guerre constitué de longue date par les nombreuses institutions publiques en charge du traitement des données sensibles des 67 millions de citoyens[2]. « Souveraineté » devait donc constituer le maître mot de cette entreprise stratégique de développement de l'intelligence artificielle nationale. « Souveraineté » dont on a pu éprouver la nécessité à l'occasion d'une crise sanitaire mondiale suscitant un repli national massif de l'ensemble des États soulignant d'autant plus la dépendance desdits États ayant abandonné leur autonomie sur l'autel du gain de productivité. « Souveraineté », encore, que l'on a brandie et cherché à promouvoir lorsque la question de mettre le numérique au service du suivi de l'épidémie a été posée pour refuser la solution toute faite proposée par les géants que sont Apple et Google, solution pourtant forcément interopérable dans l'ensemble des États y souscrivant, mais il fallait la jouer Française et centralisée !

L'hébergement hors UE… le nœud gordien de la perte de souveraineté !

Comment comprendre dès lors que dans un tel contexte le choix des autorités publiques se soit porté sur un de ces GAFAM, Microsoft, plutôt que sur un acteur français tel qu'OVH ou une solution européenne, à l'instar de l'initiative franco-allemande lancée le 4 juin, GAIA-X, permettant de conserver une souveraineté, pour assurer l'hébergement du plus important entrepôt de données sensibles dont la France dispose. Si nombreux s'en sont émus depuis la signature du contrat de sous-traitance avec Microsoft à la fin de l'année 2019, la CNIL, singulièrement, a insisté dans sa **délibération n° 2020-044 du 20 avril 2020** relative au projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire, sur la nécessité d'entourer le HDH des « *garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel* ». Préconisant par conséquent que des mesures techniques et juridiques soient adoptées pour assurer un haut niveau de protection des données. Ce faisant, la CNIL relève que son examen ne peut être complet relativement aux transferts hors UE de ces données de santé et de leur divulgation non autorisée par le droit de l'Union dès lors que les contrats fournis ne précisent « *ni la localisation des données ni l'ensemble des garanties relatives aux*

* Reproduced with gracious permission of the Author. The original text was published by the Club des Juristes, 23.6.2020 and is available, in open access, at the following page: https://blog.leclubdesjuristes.com/nos-donnees-de-sante-en-danger-quand-larbre-de-la-crise-sanitaire-cache-la-foret-de-la-perte-de-souverainete/

modalités d'accès aux données par les administrateurs de l'hébergeur ». Après avoir rappelé le contexte justifiant les inquiétudes du Comité européen à la protection des données relativement à l'accès par les juridictions américaines aux données transférées vers les États-Unis pour des impératifs de sécurité nationale[3] et les contentieux relatifs à ces préoccupations devant la Cour de Justice[4] , la CNIL recommande expressément que « *la Plateforme des données de santé assure un hébergement et un traitement des données sur le territoire de l'Union européenne* ». De même, à plus long terme, la CNIL émet le souhait que « *eu égard à la sensibilité des données en cause, que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne* ». En dépit de ces mises en garde, l'arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire confie le traitement et la collecte des données de santé à la plateforme du HDH hébergée sur le cloud de Microsoft Azure. Cet hébergement, largement contesté également du fait du non respect des procédures classiques d'appel d'offre et de mise en concurrence, avait fait l'objet d'un courrier adressé au ministre des Solidarités et de la Santé par un collectif, Santénathon, regroupant des organisations du mouvement du logiciel libre et de l'Opensource. Face au mutisme ministériel, ce collectif rejoint par le collectif InterHop, composé de professionnels du secteur de la santé et de l'informatique médicale, mobilisé de longue date sur cette question de l'hébergement du HDH, et un certain nombre de personnalités et d'organisations soucieuses de la protection des données de santé ont déposé un référé liberté devant le Conseil d'État qui a rendu son ordonnance le 19 juin.

Une victoire à la Pyrrhus ?

Alors que l'ensemble des parties se sont rapidement félicitées de la décision rendue par le Conseil d'État qui impose au HDH de se mettre en conformité avec la loi auprès de la CNIL sous 5 jours, tant au regard des impératifs de pseudonymisation que d'information des personnes concernées, cette victoire n'est toutefois pas totale. En effet, relativement à l'hébergement des données sur le Cloud Microsoft Azure, les juges du Conseil d'État se montrent beaucoup plus nuancés. S'ils imposent une meilleure information des personnes concernées en obligeant la plateforme à publier sur le site que les données de santé hébergées sont transférées hors UE aux États-Unis, l'existence même de cet hébergement ne semble pas poser, en soi, de difficulté. Il y a en effet une distinction à opérer, Microsoft hébergeant les données de santé « au repos » dans des data centers situés sur le territoire de l'UE (Pays-Bas et à terme France) néanmoins, les données peuvent transiter par les États-Unis pour le fonctionnement de la solution technique et notamment pour des opérations d'administration. Or le Conseil d'État relève, tout d'abord, que l'existence de la décision d'adéquation de la Commission et de la reconnaissance du *Privacy Shield*[5] , actuellement contestée, empêche de considérer que l'hébergement de ces données par Microsoft, société adhérant au *Privacy Shield*, soit en lui-même problématique. Le collectif ne parvient pas ensuite à convaincre le Conseil d'État du risque d'accès aux données ainsi hébergées sur le fondement du *Cloud Act*. En conséquence, le conseil décide que « *la circonstance que cette société relève du droit américain et puisse être amenée, pour les opérations d'administration de la solution technique qu'elle propose, à transférer des données aux États-Unis, ne peut être regardée (…) comme portant une atteinte grave et manifestement illégale aux libertés fondamentales* ». La décision reste toutefois éminemment contextuelle et pourrait donc être très différente si au plan européen, la décision d'adéquation venait à être remise en cause. Au-delà de la réponse juridique apportée par le Conseil d'État, souhaitons que la réponse politique qui pourrait être donnée soit à la hauteur des enjeux en cause.

[1] Rapport Villani, **Donner un sens à l'intelligence artificielle**, Remis lors du colloque *IA for Humanity* le 29 mars 2019 au Collège de France en présence du Président de la République.
[2] Sur ces données et les instituts en charge de leur collecte et de la gestion des accès, v. *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, dir. N. Martial-Braz et J. Rochfeld, n°506.
[3] Plus précisément sont en cause l'article 702 de la loi américaine FISA, le décret (« Executive Order ») n°12 333 et Clarifying Lawful Overseas Use of Data Act » du 23 mars 2018.
[4] CJUE C-311/18 décision à venir.
[5] **Décision d'exécution (UE) 2016/1250 du 12 juillet 2016** conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données États-Unis.

Tamar Sharon

Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers

Abstract: Since the outbreak of COVID-19, governments have turned their attention to digital contact tracing. In many countries, public debate has focused on the risks this technology poses to privacy, with advocates and experts sounding alarm bells about surveillance and mission creep reminiscent of the post 9/11 era. Yet, when Apple and Google launched their contact tracing API in April 2020, some of the world's leading privacy experts applauded this initiative for its privacy-preserving technical specifications. In an interesting twist, the tech giants came to be portrayed as greater champions of privacy than some democratic governments. This article proposes to view the Apple/Google API in terms of a broader phenomenon whereby tech corporations are encroaching into ever new spheres of social life. From this perspective, the (legitimate) advantage these actors have accrued in the sphere of the production of digital goods provides them with (illegitimate) access to the spheres of health and medicine, and more worrisome, to the sphere of politics. These sphere transgressions raise numerous risks that are not captured by the focus on privacy harms. Namely, a crowding out of essential spherical expertise, new dependencies on corporate actors for the delivery of essential, public goods, the shaping of (global) public policy by non-representative, private actors and ultimately, the accumulation of decision-making power across multiple spheres. While privacy is certainly an important value, its centrality in the debate on digital contact tracing may blind us to these broader societal harms and unwittingly pave the way for ever more sphere transgressions.

Introduction: contact tracing and the automation of a public health practice

Since the outbreak of the COVID-19 pandemic in early 2020, governments and health authorities around the world have attempted to mobilize digital technologies to address this novel threat, including the use of tracker wristbands, smartphone applications, thermal cameras, facial recognition and drones (The Economist 2020). In the prolonged anticipation of more permanent solutions like a vaccine, contact tracing apps in particular are being explored as tools to help contain the spread of the virus (EC 2020; WHO 2020). Contact tracing is a time-tested method that has been successfully used to fight infectious disease outbreaks including syphilis, measles, HIV and Ebola.

It involves identifying infected individuals and informing the people they have been in contact with that they are at risk, through a meticulous process of retracing where and with whom an infected individual has been in proximity. Automated contact tracing offers

* Reproduced with gracious permission of the Author. The original text was published by 23 Ethics and Information Technology (2020) and is available, in open access, at the following page: https://link.springer.com/article/10.1007/s10676-020-09547-x

several advantages over traditional contact tracing in the case of the COVID-19 pandemic (CDC 2020a; Ferreti et al. 2020). First, it seeks to automate a labor-intensive practice in a situation where there is a scarcity of human contact tracers. Moreover, it may offer more accuracy where human memories are fallible— particularly in the case of COVID-19, where infection can be asymptomatic for up to two weeks.

The speed of contagion of the COVID-19 virus, finally, requires swift contact tracing in order to be effective. Digital contact tracing seeks to address these limitations, by providing speed, scale and accuracy.

As with many attempts at automation, numerous obstacles impede the path to smooth, seamless digital contact tracing. It is not at all clear, in the first instance, that these contact tracing apps will be effective (Ada Lovelace Institute 2020). In countries where digital contact tracing was first deployed, such as China, Singapore and South Korea, the actual role of this technique in controlling the spread of infections is ambiguous (Frieden 2020). Accuracy is another major concern here.

Bluetooth, currently the preferred technology for digital contact tracing, can result in high amounts of false positives, by picking up "contacts" that are not epidemiologically significant (Lee 2020; Vaughn 2020). Effective digital contact tracing also relies on a high level of uptake by the population, which will be difficult to ensure if these systems are to be voluntary (Hinch et al. 2020).

This issue is complicated by the question of who can participate in digital contact tracing. Not everyone has access to a smartphone, even in wealthier nations. And of those who do, an estimated 1.5 billion people globally still use basic phones that do not have the necessary technical requirements, such as Bluetooth "low energy" chips, that are being used in many contact tracing apps (Counterpoint 2020). Importantly, these populations tend to be lower socio-economic groups and older people, exactly those people who are also among the most vulnerable to the virus (O'Neil 2020). While these limitations have dampened some of the initial enthusiasm around digital contact tracing as an easy solution to curbing the spread of the virus, the technology is still seen as an important complement in national post-lockdown strategies. At the time of writing, at least 80 contact tracing systems have been launched or are in development around the world[1], and supra-national bodies like the European Commission and the WHO are publishing guidelines for app development, or developing their own (EC 2020; Dave 2020).

Beyond these more practical questions, one of the major points of contention in the implementation of digital contact tracing has been its potential to cause harm through privacy breaches (Ienca and Vayena 2020; McGee et al. 2020). In Europe and the United States, in particular, where public awareness on the use of digital surveillance for public interests has gained a heightened sensitivity to privacy issues since the Snowden revelations, this triggered a vigorous public debate on the need to develop privacy-friendly digital contact tracing. Yet, when Apple and Google—corporations whose data practices are typically the focus of ethical debate—launched their contact tracing API in April 2020, some of the world's leading privacy experts applauded this initiative for its privacypreserving technical specifications. In an interesting twist, the tech giants came to be portrayed as greater champions of privacy than some European governments. This article explores what else is at stake when two of the world's most powerful corporations move into the field of pandemic response management, even when this is done in a privacy-preserving manner.

[1] For early June 2020, according to The Correspondent's "Track(ed) Together" database. See https://thecorrespondent.com/collection/track-ed-together.

Drawing on Michael Walzer's (1983) theory of justice, and the autonomy of spheres of social life as a precondition for equality and justice, I propose to view the Apple/Google API in terms of a broader phenomenon of powerful tech corporations encroaching into ever new spheres, by virtue of the fact that their digital expertise has become a coveted currency in almost all spheres of life. From this perspective, the (legitimate) advantage that tech companies have accrued in the sphere of the production of digital goods provides them with (illegitimate) access to the spheres of health and medicine, and more worrisome, to the sphere of politics. Each of these transgressions, I explain, poses specific risks that are not captured by the focus on privacy harms. Encroachment into the sphere of health and medicine can lead to a crowding out of significant traditional sectorial expertise and the reorganization of health and medicine in line with the values and interests of corporate actors. Encroachment into the sphere of politics can lead to new dependencies on corporate actors for the delivery of essential public goods, often underpinned by relationships of charity and gratitude rather than justice and duty, and ultimately to the shaping of public policy by non-elected, unaccountable actors. The overall risk is an accrual of advantage and power across spheres—what Walzer calls tyranny. While privacy is an important intrinsic and instrumental value, the centrality that it has received in the debate on digital contact tracing, and arguably in other debates on digitalization, may blind us to these broader societal harms and unwittingly pave the way for ever more sphere transgressions.

Lessons learned: privacy takes central stage Mission creep

Beyond the pressing question of whether digital contact tracing will actually prove to be effective, public debate in many countries has focused on the risks contact tracing apps pose to privacy[2].While it is clear that, in times of crisis, governments may need temporary powers that suspend some civil liberties and that the sharing of sensitive data like one's health status and location can contribute to containing the spread of the virus, the use of digital methods for doing so introduces novel risks. Namely, the ease by which digital data, as opposed to data in the paper age, flow between contexts that are governed by different norms of privacy (Nissenbaum 2010), has given rise to new fears of "mission creep". For example, data on people's health status collected for contact tracing could be used for other purposes and by third parties: for determining who can and cannot get back to work, or for determining who can and cannot access public spaces like subways, malls and markets (Morley et al. 2020; Parker and Jones 2020)[3]. Location data, similarly, can be used to show who a person associates with and to infer what they were doing at a given time, fear of which can have a chilling effect on people's participation in certain activities (Rahman 2020). Privacy here needs to be addressed from both the angle of the person who

[2] Privacy is not the only ethical concern that has been voiced by legal scholars, ethicists and activists. Others include fair data sharing practices, responsible data use, discrimination, freedom of movement and voluntariness. See for example Lucivero et al. (2020) and Morley et al. (2020). Furthermore, this article focusses on the contact tracing debate and the involvement of large tech companies in pandemic response measures in the context of the US and Europe. For an overview of COVID-19 responses in the global setting and in relation to global justice, see the volume edited by Taylor et al. (2020).

[3] China's AliPay Health Code app, one of the first contact tracing apps, is being used in this way. In the Netherlands, a QR based app is being used to allow access to some restaurant terraces (https://checkgesprek.nl).

is infected and the person who is at risk of infection because they have been in contact with the infected person.

Within the public discussions around digital contact tracing, these concerns have tended to be framed in terms of a trade-off between individual privacy rights and public health. The European General Data Protection Regulation supports this framing with specific articles that provide the legal grounds for processing personal data in the context of epidemics. Article 9, for example, allows the processing of personal data "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health", provided that such processing is proportionate to the aim pursued, respects the right to data protection and safeguards the rights and freedoms of the data subject. But many concerns have been raised about just how much privacy should be traded off for public health, and if this dichotomous framing is actually an accurate depiction of the considerations at hand (Goldenfein et al. 2020). Importantly, as privacy advocates and civil liberties campaigners have pointed out (Ross 2020; Schwartz 2020), the "privacy vs. public health" framing is reminiscent of the counterterrorism debate that followed the 2001 attacks on the World Trade Center, which was framed in terms of "privacy vs. security". In that debate, the tangible threat of terrorism justified an expansion of governments' surveillance powers (whose effectiveness was also questionable), and the creation of a global surveillance behemoth that persists to this day. Similarly, scholars question what will happen to the epidemiological surveillance constellation that contact tracing apps support once the pandemic is over, and if the erosion of privacy will become part of a permanent state of vigilance against new viruses (McGee et al. 2020; Roth et al. 2020). Prompted by these concerns, a number of advocacy and advisory groups and governing bodies have indicated the need to develop contact tracing apps in a way that would be privacy preserving, with an emphasis on voluntariness, transparency, collection and sharing of non-traceable identifiers and de-centralized storage (see e.g. EC 2020; EDPS 2020; Ada Lovelace Institute 2020; NCB 2020).

Contact tracing privacy by design

For these critical experts, the trade-off between privacy and public health is a false one.

Furthermore, it is possible to translate the value of privacy, as well as other ethical and legal principles, into technological design (Hildebrandt and Tielemans 2013), thus imposing material restrictions on possible excesses in times of crisis, and all the while promoting public health. Design choices have therefore been foregrounded in the discussion on digital contact tracing.

First and foremost, the use of low-energy Bluetooth has been advanced as an important design solution. A number of the early digital contact tracing systems, for example the ones used in China and South Korea, but also in India, Israel and Iceland, use location data from phones. Automated GPS tracking does not only lack in precision, it is typically non-consensual and scores low on privacy. Bluetooth-based apps, conversely, avoid tracking the location of users and are perceived as less intrusive. Here, phones generate random numerical IDs or "handshakes" that are transmitted to nearby devices, which commit these to a contact history log. If a person experiences symptoms or tests positive, this will send a notification to the devices whose identifiers it had previously received. Because these handshakes are encrypted, and because users' location is not logged, Bluetooth has been portrayed as superior to location tracking for privacy reasons, and has been recommended

by the EC guidance for app development (EC 2020) and favored by many European governments.

Another important criterion for many privacy experts has been that contact tracing apps rely on systems that are decentralized. Centralized apps, used for example by Singapore and Australia, send data collected by a user's phone to a central database controlled by a national health agency or other governmental authority. This authority then works out who to send an alert to among the contacts that an infected person's phone has registered. This concentration of data and power has been a crucial point of contention for privacy advocates, who have widely supported decentralized systems. In this model the data collected by phones are not sent to a central server but are stored locally, on individual phones, and the phones do the contact-matching themselves—no central authority needs to be involved. The "Decentralized Privacy-Preserving Proximity Tracing", or DP- 3T, protocol was an important frontrunner in this regard (Troncoso et al. 2020), developed by a group of European academics in response to the early "Pan-European Privacy-Preserving Proximity Tracing" consortium which backed a centralized system. DP-3T triggered a debate on centralized vs. decentralized systems which became highly political (Criddle and Kelion 2020)[4], and resulted in many countries, such as Germany, Austria, Estonia and Switzerland, opting for decentralized models, and the European Parliament (2020) and the CDC (2020b) calling for apps to be decentralized.

Apple and Google: the unexpected champions of privacy-friendly contact tracing Amidst these heated debates, in early April 2020 Apple and Google revealed that they, too, were busy developing contact tracing technology (Apple 2020). In a first instance the Apple/Google software consists of an API that allows Apple and Android phones to exchange data with each other. Users have to download contact tracing apps that use the API as the underlying system. At a later stage, contact tracing software will be added directly into the operating systems of phones as a default. To many, the Apple/Google initiative came as a surprise. Not just because the plans had remained covert, or because the two companies habitually tend to be competitors more than collaborators, but because their initiative put privacy center stage. The questionable data practices that these technology corporations are known for—Google admittedly much more than Apple— would not normally inspire trust for such a sensitive technology like digital contact tracing.

Likewise, one of the big lessons learned from post-9/11 surveillance creep was the importance of the merging of military and corporate interests driving the political economy of surveillance (Ball & Snider 2013). And yet, the Apple/Google API has been presented as a response to some of the gravest privacy concerns voiced in the digital contact tracing debate. Indeed, the draft technical documentation that the companies quickly released showed that many of the specifications of the proposal incorporated requirements spelled out by privacy experts for secure contact tracing, and had even been inspired by the ultra privacy-sensitive DP-3T protocol (Leprince-Ringuet 2020).

These include: the use of Bluetooth (no need for location data); the generation of random identification numbers by phones that change every 10–20 min (no personally identifiable data is exchanged); an opt-in system (users have to consent to their device broadcasting their identifiers once they've tested positive); and the cherry on top—a

[4] See for example, the joint statement signed by over 300 academics internationally in support of decentralized protocols: https://giuper.github.io/JointStatement.pdf. Much of this discussion played out on Twitter: https://twitter.com/mikarv/status/1252213057213915136?s=20

decentralized model (data is stored and processed on users' devices).

This alignment with privacy specifications led to widespread endorsement and applause for the Apple/Google initiative by some of the leading privacy experts in the contact tracing debate. For example, the European Data Protection Supervisor immediately backed the initiative, stating in a tweet that "it seems to tick the right boxes as regards #user choice, #data protection by design and pan-European #interoperability"[5]. And researchers behind the DP-3T protocol praised the compatibility of the Apple/Google API with their own. As Marcel Salathé, one of the researchers who helped write DP-3T commented, "For us (…) it was a no-brainer. Most of the things we had proposed with DP-3T were in Apple and Google's API" (in Leprince-Ringuet 2020). The Apple/Google API's privacy preserving specifications, along with the promise for greater interoperability across countries—something that the European Commission promoted as crucial since initial discussions on digital contact tracing—were persuasive, and more and more governments announced that they would adopt it. These include [at the time of writing] Austria, Canada, Denmark, Estonia, Germany, Ireland, Italy, Japan, Latvia, Malaysia, Northern Ireland, and Switzerland[6]. In an interesting twist, the tech giants came to be portrayed as greater champions of privacy than some democratic governments, and as what one privacy consultant called "the most efficient privacy regulators in the world" (in Scott et al. 2020).

Not all privacy experts agree about the level of privacy protection the Apple/Google API will deliver. For Jaap-Henk Hoepman (2020) for example, embedding the contact tracing functionality in the operating system layer creates a dormant functionality for mass surveillance, whereby the contact tracing microdata are under the control of Apple/Google. Furthermore, Hoepman explains, the platform can easily be transformed into a centralized form of tracing, and may allow malicious apps to learn which people an infected person has been in contact with. Others are calling for the implementation of additional safeguards, such as careful auditing and mechanisms for ensuring the technology can be uninstalled once the pandemic is over. Others still are more generally suspicious of the Bluetooth technology the API makes use of, which operates in the background without users noticing or knowing what happens exactly to their data[7]. But this focus on privacy, while certainly important, risks blindsiding us to the bigger questions at hand. Even if the Apple/Google contact tracing technology does get the privacy issue just right, what other trade-offs are involved in letting these companies contribute to the development and deployment of what might be the largest scale crisis management measure for the pandemic so far? The Googlization of pandemic response To answer this, it is helpful first to note that the development of digital contact tracing is only one of many ways that the large tech corporations, not just Apple and Google, but also Facebook, Amazon, Microsoft, other subsidiaries of Alphabet, as well as their Asian counterparts including Alibaba, Baidu Tencent and Huwaei, have contributed to addressing the threats posed by COVID- 19. In addition to providing key information and resources on COVID-19 on

[5] https://twitter.com/EU_EDPS/status/1248661369274150912.

[6] See MIT Technology Review's 'Covid Tracking Tracker'. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracingtracker/

[7] Some critics of Bluetooth-based contact tracing are instead advocating for QR-code based contact tracing, which requires much more intentionality on the part of users, who have to scan QR codes to enter certain spaces. See for example Hoffman et al.'s piece on the "Zwaai" QR-code based app in this issue.

their respective platforms, many of these companies began developing COVID specific data collection, data sharing and data analysis tools, or have earmarked significant amounts of funds for COVID related research, early on during the pandemic.

Tech companies and the COVID-19 threat In March 2020 already, Facebook added COVID specific "Disease Prevention Maps" to its "Data for Good" program, for sharing user location data with researchers seeking to identify virus hotspots (Facebook 2020). Also early on, Verily, Alphabet's life sciences subsidiary, launched a screening and testing website where users could fill out a multi-question survey about their symptoms and get directed to a drive-through testing location, run by Alphabet, Verily and Google volunteers. Originally limited to the state of California, the number of testing sites soon expanded across the US, to include 130 sites in 12 states at the time of writing. Apple contributed to a similar triage effort in California by building an app with Stanford Medicine to connect firefighters, police officers and paramedics to testing sites (Leswing 2020). In the UK, Amazon, Microsoft, Google and Palantir are assisting the National Health Service (NHS) in setting up a "COVID-19 data store", to track how hospitals are managing beds, capacity oxygen and ventilators, and to help them allocate resources appropriately (Fitzgerald and Crider 2020). Almost all of the large tech companies, furthermore, are contributing in some way or other to research and clinical efforts on COVID-19. IBM, Amazon, Google and Microsoft have contributed computing power, necessary to process very large datasets in epidemiological, bioinformatics and molecular modelling. Google Cloud, for example, has mobilized $20 million in Google Cloud credits to support academic research (Kurian 2020). Baidu and Google's DeepMind are applying deep-learning techniques for modeling the structure of the coronavirus' proteins, which could be useful in developing a vaccine (DeepMind 2020). And Microsoft and Facebook, via the Chan Zuckerberg Initiative, have helped compile datasets of COVID-19 related research papers for easy query. An interesting case in point is Verily's coronavirus screening website. Initially set up to help triage individuals at high risk in a context of limited risk screening and testing capacity, the initiative soon fused with Verily's Project Baseline. The Project Baseline is an ambitious project set up some years ago that seeks to create a "baseline" of human health by aggregating a wealth of clinical, genomic and lifestyle data donated by healthy volunteers. The dataset will be used for research purposes and the platform as a means of connecting potential participants with clinical research. Shortly after Verily launched its screening tool, it began calling the initiative the "Baseline COVID-19 Pilot Program". What this indicates is that the triage tool will soon be used for much more than just triage and testing, most likely for channeling users towards enrollment in trials, such as the serology study that Verily announced as the first of its Baseline COVID-19 Research Project initiatives (Verily 2020). Verily could thus quickly leverage an already existing infrastructure for data collection for biomedical research to expand its COVID-19 involvement.

Most of these companies have not only been involved in providing the infrastructure for research to take place, but have also been forthcoming in funding research. The Chan Zuckerberg Initiative has donated over $13 million to a collaboration between UC San Francisco, Stanford University and the Chan Zuckerberg Biohub, to study COVID-19. And the Bill and Melinda Gates Foundation, in particular, has been portrayed in the media as one of the "leaders in the coronavirus response" (Piper 2020). The foundation, with one of the largest endowments of any charity in the world and 20 years of experience in public health and infectious disease response, launched numerous pandemic response endeavors as early as February 2020 and announced in April that it would shift most of its

attention to fighting the pandemic (Grothaus 2020). These have included commitments of some $300 million, for home testing kits, a "Therapeutics Accelerator" to study the most effective treatments for the virus, vaccine development (and enhancement of global manufacturing and delivery capacity), and a relentless media tour by Gates himself on the importance of social distancing[8].These philanthropic efforts extend to other types of relief responses as well.Amongst others, Google has donated Chromebooks and WiFi hotspots to households in California, to help students with remote schooling during the pandemic, and committed to donating over $800 million to support small and medium sized businesses, health organizations and governments.

Apple donated $10 million to a COVID-19 fundraiser organized by the WHO. Amazon, in addition to providing $5 million worth of devices to hospitals, schools and families, including Kindles, Fire tablets and Echo for patient monitoring (Amazon 2020), has also donated $100 million to a large charity that operates food banks around the US. And in what some commentators have called "China's Big Tech donation spree" (Cerulus 2020) Alibaba and Huwaei provided European hospitals hit early on with protective suits and medical masks.

Precedents in the Googlization of health If this capacity on the part of tech corporations to contribute not only financial resources, but also the technical, infrastructural and biomedical expertise required to address the current public health crisis seems surprising, it shouldn't. In the past decade consumer technology companies have swiftly and surely moved into the health and biomedical sector, positioning themselves as important facilitators of data-driven digital health and medicine, in what can be called a "Googlization of health" (Sharon 2016, 2018). Launched in 2014, Apple's ResearchKit software, for example, now allows medical researchers to carry out clinical studies using the iPhone, and is currently being used by prominent medical institutions like Yale and Stanford. Verily, in addition to its ambitious Project Baseline, is collaborating in research on Parkinson's disease in Europe and with pharma companies on clinical trial development. Other Alphabet subsidiaries, like DeepMind, are developing AI for medical diagnostics, with some recent successes in cardiovascular disease, eye disease and breast and lung cancer. Amazon has developed a machine learning tool for the processing of unstructured medical texts and its Alexa voice-assistant is now being used by the UK's NHS to provide NHS health advice to users at home. A number of these companies are also involved in electronic health record management, employee healthcare, health insurance, and the provision of healthcare services, with Verily's new opioid addiction clinic open since 2019. Neither is health and medicine the only sector into which these companies have begun making permanent inroads pre-corona.

During the same period, we have also witnessed their growing involvement in, amongst others, the sectors of transportation, urban planning, education, and space exploration (see for example Vaidhyanathan (2011) and van Dijck et al. (2019)).

Sphere transgression: from digital goods to health and medicine
The dangers of sector creep

In his seminal book Spheres of Justice (1983), the political philosopher Michael

[8] Gates is often quoted as having anticipated that a pandemic similar to coronavirus would sweep the globe in a TED talk in 2015.

Walzer elaborates a theory of justice and complex equality based on the autonomy of spheres in which different societal goods—education, welfare, wealth, friendship, political power, etc.—are distributed. While inequality is bound to exist amongst individuals within spheres, Walzer maintains that a just society is one where advantage in one sphere cannot be converted into dominance in another. Thus, while one citizen may be chosen over another for political office, leading to some inequality in the sphere of politics, this advantage should not confer that person any advantages in other spheres, such as superior medical care, access to better schools for her children or greater entrepreneurial opportunities. Such conversions and transgressions between spheres, according to Walzer, are a form of tyranny. They lead to both a loss of meaning and significance of those goods which succumb to the distributive logic of the wrong sphere, as well as to the dominance of some members of society by others.

Walzer did not identify an area of technological production in which digital goods are distributed as a sphere per se. But his notion of complex equality based on the separation of distributional spheres is useful for describing what is happening in a phenomenon like the Googlization of health or of pandemic response[9]. Indeed, what we are witnessing as these companies move into new sectors is that the technical expertise—in terms of data collection, data analytics and infrastructure development—which confers them a clear and legitimate advantage in the sphere of digital goods, is currently being converted into advantages in other spheres, such as the sphere of health and medicine and the sphere of politics. In a context in which ever more sectors of society are undergoing processes of digitalization and datafication, this is to be expected, and it may result in increased technical efficiency and other benefits in some spheres. However, what Walzer would call its "tyrannical" nature requires urgent attention, and presents risks that are hardly limited to privacy harms.

The crowding out of essential, "spherical" expertise The recent push in the health and medical sector to move towards more data-driven personalized medicine (Frohlich et al. 2018) has turned digital expertise into a coveted good in the sphere of health, and has made tech companies attractive partners to collaborate with. In other words, it is not based on the merits of their medical (or epidemiological) expertise that these companies' novel presence in health and medicine is justified[10].This lack of traditional "spherical" expertise is problematic. As scholars in the field of science and technology studies have shown,

[9] For a more detailed explanation of how this framework can be applied in this context, and why this amounts to more than just the encroachment of the market sphere into the sphere of health and medicine, see Sharon (2020). There I show how a multiple sphere ontology and the notion of sphere transgression based on illegitimate conversions of advantages of one into other spheres sheds light on additional risks raised by the Googlization of health. These have to do not only with an importation of a marketplace logic into the sphere of health andmedicine – although this is the most evident risk – but also with the importation of an "industrial" logic of efficiency, a "civic" logic of democratization of knowledge, a "project" logic of innovation for innovation's sake, and possibly others.

[10] Though developing inhouse medical expertise, by hiring leading medical specialists into their ranks, is a strategy that is being pursued by these companies alongside the new partnerships they are establishing with traditional institutions and sectorial actors (Check 2015; Reisinger 2018). For an analysis of how these new partnerships are being justified, see Sharon (2018).

routine human practices and professional tasks, in the medical and other fields, always involve implicit values, norms and skills which are at risk of being omitted or lost when a practice is standardized and automated (Berg 1997; Timmermans and Mauck 2005). In this understanding, automation amounts to the importation of practices that embody values such as efficiency, optimization and speed— values that are and should be decisive in the sphere of technological production—at the expense of traditional sectorial norms and values, which are not always noticeable to outsiders.

Digital contact tracing is a prime instance of the promise of automation, whereby traditional, often repetitive human tasks—be these checking out supermarket products, welfare benefit allocation, driving or medical decision-making—seek to be augmented if not replaced by more efficient, objective and speedy automated systems. But as a practice, digital contact tracing involves implicit values and skills which are integral to its overall aims and cannot be easily translated into automated processes. These include, first and foremost, the capacity to navigate complex human interaction. The public health workers traditionally carrying out contact tracing are trained to undertake epidemiological detective work to establish which contacts matter for disease contagion.

This is based on criteria like the environment that was shared with another person, the kind of activity which was being carried out at the time, and for how long. Replacing this type of inquiry with the exchange of signals via Bluetooth is proving problematic (Ada Lovelace 2020). Some phones can detect signals from up to 30 m, without being able to determine if a signal was transmitted from 1 to 29 m away. Bluetooth technology also cannot account for important obstacles to virus transmission, like walls, through which Bluetooth signals can still be transmitted.

Moreover, it can hardly control for environmental variables, like ventilation, or direction of the wind. In other words, what constitutes a "contact" for a smartphone does not always have epidemiological value.

Second, the success of traditional contact tracing rests on the ability of the public health worker to build a relationship of trust with the interviewee. Not only so that people feel safe revealing personal details, but also because contact tracing is as much about identifying persons at risk of infection as it is about providing them with targeted information. Contact tracers need to deliver public health advice, such as the recommendation to go in to quarantine, in a way that people will listen to and act upon this advice. Human skills, including empathy, patience and understanding, which are demonstrated and enacted in the back-and-forth of conversation between people, are required here, and all but missing in an app notification. Moreover, much of the work of human contact tracers has to do with ensuring that people have the material conditions required to sustain a 14-day quarantine, including food in their homes, the ability to care for children who may need to be removed, how to isolate in small spaces and when to seek medical attention (Bourdeaux, Gray and Grosz 2020; Ross 2020). For all of these reasons, for those familiar with the practice, contact tracing has been called "an art as much as a science" (Otterman 2020), which cannot be easily replaced by an app, no matter how accurate or widely used it would be. Here, the importance of keeping a human "in" (or "on top of") the loop, as critical scholars of algorithms rightly argue for, is not just about avoiding pernicious feedback loops and algorithmic discrimination, but also about carefully acknowledging everything that goes into making a practice "good" (Mol 2008; Pols 2012) before rushing to automate its most self-evident components.

The crowding out of spherical, here epidemiological, expertise has been to an important

extent further facilitated by the over-simplified equation of decentralized approaches with privacypreservation, and centralized approaches with government surveillance; an opposition in part promoted by Apple and Google in the digital contact tracing debate. As a number of public health experts have pointed out, there are good reasons to opt for a centralized approach that have to do with a thorough understanding of contact tracing as a practice involving the norms and skills discussed above, more than with privacy (Kelion 2020, Leprince-Ringuet 2020, Parker et al. 2020)[11].The most important one goes back to the paucity of the epidemiological data collected by Bluetooth-based contact tracing in comparison to the context-rich data collected by human contact tracers. With a high risk of false positives and false negatives, a centralized approach, according to some public health officials, allows for better supervision and control of these data so that warnings are only sent out to people who have been in epidemiologically significant contact with an infected person. Too many false alarms can quickly result in people not paying attention to warnings sent by an app.

Sphere transgression, here the conversion of technical expertise into an advantage in the sphere of health and medicine, thus risks crowding out practices, norms and values that have been central to this sphere. The deeper the inroads the large tech companies undertake into the health and medical and other sectors, with what might be very efficient, quick and low-cost solutions, the more they also make themselves necessary passage points for the adequate functioning of these sectors, increasing our reliance on them for essential goods. In the context of a pandemic, where human proximity is the primary threat, the dependency on infrastructures for mediated and remote human contact—telehealth, communications services, cloud storage—is amplified (Klein 2020). This can lead to a reshaping of these sectors to align with the values and interests of non-specialist private actors, which may or may not be the interests and values of those groups and individuals who should immediately benefit from the distribution of goods in those spheres, be they patients, students, residents of a city, or more generally speaking, citizens.

Sphere transgression: from digital goods to public services A governance surplus This conversion of tech expertise into an advantage in the health and medical sphere and other professional sectors also translates into a governance surplus. It grants these actors not just a say in defining the values of a professional sector, but also in the future directions that a sector will take and thus in political decisions concerning society writ large. This is an additional transgression, here into the sphere of politics. Unlike the sometimes aggressive and disruptive practices of tech companies pushing into sectors like health and medicine, this transgression increasingly tends to be a peaceful one, a response to a solicitation on the part of policy makers themselves. In the context of the pandemic, this type of solicitation took place very early on. Already as early as mid-March 2020, representatives from Facebook, Google, Microsoft and Amazon were asked to join several COVID-19 task force meetings at the White House (Robbins 2020). In the UK in the same week, representatives of these companies and Palantir were invited by government officials to present their offers to help tackle the pandemic in terms of data science, app development and data architecture (Volpicelli 2020). And Verily's first testing sites (and so the creation

[11] While some proponents of centralized tracing also argue that there is no reason per se why privacy and data security cannot be preserved in a centralized approach (Ilves 2020). Just as data collected by health authorities via manual tracing need not reveal the identity of infected persons, explore the nature of that contact or be shared with third parties, neither must this necessarily be the case in digital contact tracing.

for its database for COVID-19 related research), were developed in partnership with California state's governor's office. In May, Governor Andrew Cuomo of New York, the hardest hit state in the US, announced new partnerships with both Eric Schmidt, former Google CEO, and the Bill and Melinda Gates Foundation (BMGF)[12]. Schmidt will chair a blue-ribbon commission on how to leverage, accelerate and use technology to shape New York's post-COVID reality, while the BMGF will help develop a blueprint for a "smarter education system".

Numerous commentators have argued, also in relation to the current pandemic, that at least in the US and the UK, the surge of big tech involvement has much to do with an ongoing privatization, deregulation and reorganization of the public sector (Couldry and Mejias 2018; Klein 2007, 2020; Lawrence et al. 2020; Magalhaes and Couldry 2020; Mazzucato 2015; Morozov 2020). Decades of outsourcing and budget cuts, justified by a dominant political discourse that governments are inefficient, have significantly hampered governments' abilities to adequately provide health, housing, education, transportation, utilities and other essential services, including, in many countries, pandemic crisis response. This situation has been nourished by a narrative of innovation that has focused on the role of the private sector, and in particular the brilliance of a few individual entrepreneurs, as the drivers of technological development and innovation. As the economist Marianna Mazzucato (2015) maintains, this narrative is both factually incorrect—the state, not the private sector, has traditionally assumed the risks of uncertain technological enterprises that led to the development of amongst others, nanotechnology, biotechnology, the internet, and the iPhone— and it creates a powerful and pernicious self-fulfilling prophecy. In some countries at least, it is thus into a vacuum left over by "rolled back" states that tech corporations easily step in to address problems that governments are currently failing to solve. "We need more Googles," the governor of California proclaimed after Google announced it would provide 100,000 Wi-Fi hotspots to support remote education in California (in Elias 2020).

Philanthro-technocapitalism and the need to be grateful

Importantly, in today's philanthrocapitalism (Bishop and Green 2008), and specifically in today's philanthro-technocapitalism, it is not at all easy to discern between what are strictly speaking corporate practices and what are giving practices, what are business aims and what are charitable efforts[13].These converge in novel ways. Well before being approached by Governor Cuomo, Eric Schmidt had already spelled out his vision for surviving the pandemic in an op-ed piece in the Wall Street Journal titled "A Real Digital Infrastructure at Last" (Schmidt 2020). Here, he pleaded for the necessity of accelerating the permanent integration of emerging technologies that are being deployed in the

[12] See https://twitter.com/CNNnewsroom/status/1258065906061791233 and https://www.governor.ny.gov/news/amid-ongoing-covid-19-pandemic-governor-cuomoannounces- collaboration-gates-foundation-develop.

[13] Apple CEO Tim Cook has been very explicit about how commercial and altruistic objectives converge at Apple. When recently asked in an interview why Apple has not set upa charitable foundation like other companies, his answer was that setting up a foundationseparates a company's capacity to produce social value from its core business. This, as he perceives it to be the case with Apple, should be integral to, not disconnected from what a company does (Cook 2019).

current crisis. Among others, technologies for efficient supply and distribution of goods, for remote education, for health and medicine, and a digital infrastructure to support a future economy and education system "based on tele-everything". Perhaps most striking was Schmidt's call on the American population to "be a little more grateful". He writes: "the benefit of these corporations, which we love to malign, in terms of the ability to communicate, the ability to deal with health, the ability to get information, is profound. Think about what your life would be like without Amazon."

Schmidt's plea for more appreciation is not entirely misplaced. Gratitude is to be expected in response to beneficence and charity, and many of the contributions by big tech to the pandemic response have been made as donations or through philanthropic foundations. Gratitude, however, has no place in a social contract. As the sociologist Lindsey McGoey (2015) has poignantly shown in her study of the impact the Bill and Melinda Gates Foundation (BMGF) has had on global health and development, while philanthropies may certainly be well-intentioned and can direct resources to important and often neglected causes, they can have a wide range of negative effects. First, when they are big, they can distort the funding landscape, creating critical energy around one particular area and drawing it away from others[14]. Second, while the amount of funds donated by a foundation like BMGF to global health may seem significant, it pales in comparison to what governments, sustained by taxes, spend on health—even the poorest ones. Philanthropic donations to vaccine development in the current pandemic, while receiving a lot of media attention, are no exception. It should be clear, furthermore, as McGoey and others point out (Reich 2018; Piketty 2020), that charitable gifts are actually donations which are subsidized, again, by tax payers. Both because philanthropists receive tax privileges for donations, and because the taxes they would have been paying on the part of their wealth that is being donated would have gone to various social programs. For these scholars, understood as subsidized donations, big tech philanthropy sits uncomfortably with the fact that these corporations are partially responsible for generating some of the harm to workers and the environment that they purport to solve through philanthropy. Finally, charity can be withdrawn at the whim of the giver. There is no law that compels wealthy individuals to redistribute any of their wealth in charitable ways. Other than expressions of gratitude, a citizen body has little say in the giving practices of philanthropists; that is precisely the problem. As Saint Augustine professed in earlier times, charity is no substitute for justice withheld (McGoey 2020). Contributing to or determining pandemic response? The decimation of the public sector, and the role this plays in facilitating big tech's involvement in the political sphere's pandemic response, is characteristic of the US and the UK more than it is of continental Europe. And indeed, it is mostly in the US and to some extent in the UK that examples of pandemic response partnerships between state or federal actors and tech corporations abound. But it is a mistake to think that the encroachment of these companies into the political sphere is limited to those countries. This, in light of the knock-on effects that the organization of the political sphere in a dominant country like the US has on the rest of the world, and furthermore, in light of the global reach of their operating systems and digital infrastructure (van Dijck et al. 2019; Taylor et al. 2020). In terms of the latter, especially, the Apple/Google API is a case in point.

As explained earlier, the Apple/Google API was presented as a privacy-friendly

[14] McGoey cites the example of charter schools in the US, which the BMGF supported, and which have contributed, according to some analysts, to an increase in educational inequalities.

protocol because it incorporated the main requirements for privacy-preserving contact tracing as expounded by privacy experts; in particular, its adoption of a decentralized model. Its espousal by governments in Europe, furthermore, was in large part influenced by a sustained campaign in favor of decentralized protocols led by activists and academics echoed in statements made by a number of EU bodies. But several reports on discussions that took place between government officials and Apple and Google portray another side of this story, pointing to a power play between sovereign states and the corporations, in which sovereign states had little say. Namely, some government officials claim to have been taken by surprise by the development of the ready-made API at a time when they were already far advanced with their own protocols. Others have depicted a situation in which there was little possibility to shape how the protocol would be adapted to their respective countries.

In France, for example, which had been working on a centralized protocol, officials have reported that when they found out about the Apple/Google API and tried to approach the companies to find workarounds, their attempts were met with staunch reaffirmations that the companies would only work with decentralized technologies (Scott et al. 2020). For a country like France, which insisted on pursuing its national centralized system, this meant open confrontation with the tech companies, and being portrayed in the media as caring less about privacy than the tech companies did (Hern 2020). Similarly, a representative of the Latvian government, which has adopted the Apple/Google API, has openly described discussions with the companies as running "into a Silicon Valley-built brick wall" and has questioned the extent to which Google or Apple should "get to tell a democratically elected government or its public health institutions what they may or may not have on an app" (Ilves 2020). Such frustrations around the need to comply with the rules set out by the companies have been echoed in other countries and federal authorities as well, including the UK and North Dakota in the US (Tometzkis and Meaker 2020). Namely the interoperability gains that come with collaborating with the companies that run the two most important mobile operating systems on the planet meant that going it alone could compromise success. The Apple/Google API is thus also an example of encroachment into the political sphere—here global public health policy.

Effectively, Apple and Google did not just contribute their technical expertise to the pandemic response, but also determined—in some instances over and above sovereign states—which path to take, setting down the conditions for which apps could exist and how governments could use them.

Conclusion

This article has attempted to articulate what is at stake when two of the world's most powerful corporations move into the field of pandemic response management with a development like the Apple/Google API for digital contact tracing. I argued that this is an instance of illegitimate sector creep, or sphere transgression. In this case, a legitimate advantage acquired in the sphere of digital goods—digital expertise—has been converted into advantages in the sphere of health and medicine (where epidemiological expertise should be the main source of legitimacy), and in the sphere of politics (where democratic accountability should be the source of legitimacy). Each of these transgressions presents its own risks. Namely, a crowding out of essential spherical expertise, new dependencies on corporate actors for the delivery of essential, public goods, the shaping of (global)

public policy by non-representative, private actors and ultimately, the accumulation of decisionmaking power across multiple spheres. Such sphere transgressions are not novel to the Apple/Google API case, nor are they limited to these two companies. Rather, they can be identified as a defining characteristic of the digitalization and datafication of society that has been underway in recent decades. Indeed, as more and more sectors of society undergo processes of digitalization, digital expertise becomes an entry ticket to previously autonomous spheres, bringing with it other values and interests and granting newfound power to reshape spheres according to those values and interests.

Sphere transgression can happen in perfectly privacy-friendly ways, such that, as argued, the focus on how privacy-preserving the Apple/Google API is misses the point. Moreover, as these companies increasingly incorporate privacy considerations in their tech development, we need to ask ourselves how privacy-friendliness may actually facilitate sphere transgression, lest our sharpest critical engagements end up weakening rather than strengthening our democracies. This is not to say that the push for privacy in contact tracing and other digital practices is not important, but that when actors like Apple and Google are involved we need a much broader lens through which to consider benefits and trade-offs, and with which to develop new safeguards. Complete sphere autonomy may not be a desirable or feasible solution for a world so deeply connected, and where digital infrastructures and expertise have become so essential. Spheres clearly overlap at times, certainly during a pandemic: to be sure, digital contact tracing can be an important complement within a broad pandemic response strategy, and to be done properly it requires a combination of both epidemiological and technical expertise. Nevertheless, new ways of managing migrations between spheres can and should be developed. By setting down pre-conditions for sphere penetration, in law, professional practice and oversight, we may find the power to protect traditional spherical expertise, enable beneficial combinations of expertise, and keep power in check.

References

1. Ada Lovelace Institute. (2020). Exit through the app store. https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-appstore/. Accessed 25 June 2020.
2. Amazon. (2020). Amazon donating $5 million in devices globally. April 10. https://blog.aboutamazon.com/devices/amazon-donating-5-million-in-devices-globally. Accessed 25 June 2020.
3. Apple. (2020). Privacy-preserving contact tracing. https://www.apple.com/covid19/contacttracing. Accessed 25 June 2020.
4. Ball, K., & Snider, L. (2013). The surveillance-industrial complex: A political economy of surveillance. London: Routledge.
5. Berg, M. (1997). Rationalizing medical work: Decision support techniques and medical practices. Boston: MIT Press.
6. Bishop, M., & Green, M. (2008). Philanthrocapitalism: How the rich can save the world. Bloomsbury: Bloomsbury University Press.
7. Centers for Disease Control and Prevention (CDC). (2020a). Preliminary criteria for the evaluation of digital contact tracing tools for COVID-19. https://www.cdc.gov/

coronavirus/2019-ncov/downloads/php/prelim-eval-criteria-digitalcontact- tracing. pdf. Accessed 25 June 2020.

8. Centers for Disease Control and Prevention (CDC). (2020b). Digital contact tracing tools for COVID-19. https://www.cdc.gov/coronavirus/2019-ncov/downloads/digital-contacttracing. pdf. Accessed 25 June 2020.
9. Cerulus, L. (2020). Huwaei joins China's Big Tech donation spree in Europe. Politico, March 25. https://www.politico.eu/article/huawei-joins-chinas-big-tech-donation-spree-ineurope/. Accessed 25 June 2020.
10. Check, H. (2015). Why biomedical superstars are signing on with Google. Nature,526(7574), 484–485.
11. European Commission (EC) (2020). Commission Recommendation (EU) 2020/518 of 8 April 2020. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626. Accessed 25 June 2020.
12. Cook, T. (2019). Interview with J. Cramer. CNBC https://www.cnbc.com/2019/01/08/appleceo- tim-cook-interview-cnbc-jim-cramer-transcript.html?__source=twitter%7Cmain. Accessed 25 June 2020.
13. Couldry, N., & Mejias, U. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. Television & New Media. https://doi.org/10.1177/1527476418796632.
14. Nuffield Council on Bioethics (NCB). (2020). Ethical Considerations in Responding to the COVID-19 Pandemic. https://www.nuffieldbioethics.org/assets/pdfs/Ethical-considerationsin- responding-to-the-COVID-19-pandemic.pdf
15. Counterpoint Research. (2020). Coronavirus: Why are there doubts over contact-tracing apps? https://www.counterpointresearch.com/coronavirus-doubts-contact-tracing-apps/. Accessed 25 June 2020.
16. Criddle, C. and Kelion, L. (2020). Corona virus contact-tracing: The world split between two types of apps. BBC, May 7. https://www.bbc.com/news/technology-52355028. Accessed 25 June 2020.
17. Dave, P. (2020). WHO readies coronavirus app for checking symptoms, possibly contact tracing. Reuters, May 9. https://uk.reuters.com/article/health-coronavirus-who-apps/whoreadies- coronavirus-app-for-checking-symptoms-possibly-contact-tracingidUKKBN22L06L. Accessed 25 June 2020.
18. DeepMind. (2020). Computational predictions of protein structures associated with COVID-19. April 8. https://deepmind.com/research/open-source/computational-predictionsof- protein-structures-associated-with-COVID-19?ref=hackernoon.com. Accessed 25 June 2020.
19. The Economist. (2020). Countries are using apps and data networks to keep tabs on the pandemic. The Economist, March 26. https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-datanetworks- to-keep-tabs-on-the-pandemic. Accessed 25 June 2020.
20. EDPS (European Data Protection Supervisor). (2020). EU digital solidarity: A call for a pan-European approach against the pandemic. https://edps.europa.eu/sites/edp/files/publication/2020-04- 06_eu_digital_solidarity_covid19_en.pdf. Accessed

25 June 2020.

21. Elias, J. (2020). California governor says, 'We need more Googles' as company offers free Wi-Fi and Chromebooks to students. CNBC April 1. https://www.cnbc.com/2020/04/01/coronavirus-google-offers-wi-fi-chromebooks-tocalifornia-students.html. Accessed 25 June 2020.
22. Facebook. (2020). Data for Good. https://dataforgood.fb.com. Accessed 25 June 2020.
23. Ferreti, L., et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science,368, 6491.
24. Fitzgerald, M. and Crider, C. (2020). Under pressure, UK government releases NHS COVID data deals with big tech. OpenDemocracy June 5. https://www.opendemocracy.net/en/underpressure- uk-government-releases-nhs-covid-data-deals-big-tech/. Accessed 25 June 2020.
25. Frieden, T. (2020). A video conversation on the coronavirus with Tom Frieden with STAT's Helen Branswell. https://www.statnews.com/2020/04/13/video-chat-conversation-on-thecoronavirus-with-tom-frieden/. Accessed 25 June 2020.
26. Frohlich, H., et al. (2018). From hype to reality: Data science enabling persnalized medicine. BMC Medicine,16, 150. https://doi.org/10.1186/s12916-018-1122-7.
27. Goldenfein, J., Green, B., Viljoen, S. (2020). Privacy versus health is a false trade-off. Jacobin April 17. https://jacobinmag.com/2020/04/privacy-health-surveillance-coronaviruspandemic-technology. Accessed 25 June 2020.
28. Grothaus, M. (2020). Bill Gates announces his foundation will focus 'total attention' on COID-19 pandemic. Fast Company, April 27. https://www.fastcompany.com/90497398/billgates- announces-his-foundation-will-focus-total-attention-on-covid-19-pandemic. Accessed 25 June 2020.
29. Hern, A. (2020). France urges Apple and Google to ease privacy rules on contact tracing. The Guardian, April 21. https://www.theguardian.com/world/2020/apr/21/france-applegoogle- privacy-contact-tracing-coronavirus. Accessed 25 June 2020.
30. Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. Computer Law and Security Review,29, 509–521 https://doi.org/10.1016/j.clsr.2013.07.004.
31. Hinch, R. et al. (2020). Effective configurations of a digital contact tracing app: A report to NHSX, 14 April 2020. https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Report%2520- %2520Effective%2520Configurations%2520of%2520a%2520Digital%2520Contact%2520 Tracing%2520App.pdf. Accessed 25 June 2020.
32. Hoepman, J.H. (2020). Stop the Apple and Google contact tracing platform (or be ready to ditch your smartphone). https://blog.xot.nl/2020/04/11/stop-the-apple-and-google-contacttracing- platform-or-be-ready-to-ditch-your-smartphone/. Accessed 25 June 2020.
33. Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID- 19 pandemic. Nature Medicine,26, 463–464. https://doi.org/10.1038/s41591-020-0832-5.

34. Ilves, I. (2020). Why are Google and Apple dictating how European democracies fight coronavirus? The Guardian, June 16. https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-europeandemocracies-coronavirus?CMP=Share_AndroidApp_Tweet. Accessed 25 June 2020.

35. Kelion, L. (2020). NHS rejects Apple-Google coronavirus app plan. BBC, April 27. https://www.bbc.com/news/technology-52441428. Accessed 25 June 2020.

36. Klein, M. (2007). The shock doctrine: The rise of disaster capitalism. New York: Allen Lane.

37. Klein, M. (2020). Screen New Deal. The Intercept, May 8. https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shockdoctrine/. Accessed 25 June 2020.

38. Kurian, T. (2020). How Google Cloud is helping during COID-19. https://cloud.google.com/blog/topics/inside-google-cloud/how-google-cloud-is-helpingduring-covid-19. Accessed 25 June 2020.

39. Lawrence, F. et al. (2020). How a decade of privatization and cuts exposed England to coronavirus. The Guardian, May 31. https://www.theguardian.com/world/2020/may/31/how-a-decade-of-privatisation-and-cutsexposed- england-to-coronavirus. Accessed 25 June 2020.

40. Lee, A. (2020). If Bluetooth doesn't work for contact-tracing apps, what will? Wired, April. https://www.wired.co.uk/article/bluetooth-contact-tracing-apps. Accessed 25 June 2020.

41. Leprince-Ringuet, D. (2020). The world's first contact-tracing app using Google and Apple's API goes live. ZDNet, May 28. https://www.zdnet.com/article/the-worlds-firstcontact- tracing-app-using-google-and-apples-api-goes-live/. Accessed 25 June 2020.

42. Leswing, K. (2020). Stanford teamed up with Apple to release an app that connects first responders to drive-through COVID-19 tests. CNBC, April 9. https://www.cnbc.com/2020/04/09/stanford-apple-app-connects-first-responders-to-covid-19-tests.html. Accessed 25 June 2020.

43. Lucivero, F., Hallowell, N., and Johnson, S., Prainsack, B., Samuel, G., and Sharon, T. (2020). Covid-19 and Contact Tracing Apps: Ethical challenges for a social experiment on a global scale. Journal of Bioethical Inquiry.

44. Magalhaes, J.C. and Couldry, N. (2020). Tech giants are using this crisis to colonize the welfare system. Jacobin, April 27. https://www.jacobinmag.com/2020/04/tech-giantscoronavirus- pandemic-welfare-surveillance. Accessed 25 June 2020.

45. Mazzucato, M. (2015). The entrepreneurial state: Debunking public vs. private sector myths. New York: Anthem Press.

46. McGee, P., Murphy, H. and Bradshaw, T. (2020). Coronavirus apps: the risk of slipping in to a surveillance state. Financial Times, April 28 https://www.ft.com/content/d2609e26- 8875-11ea-a01c-a28a3e3fbd33. Accessed 25 June 2020.

47. McGoey, L. (2015). No such thing as a free gift: The gates foundation and the price of philanthropy. New York: Verso. 48. McGoey, L. (2020). Bill Gates and the price of philanthropy: An interview with activism Munich. https://www.youtube.com/watch?v=ruR5FK8HN5Q

49. Meaker, M. and Tokmetzis, D. (2020). Coronavirus apps show governments can no longer do without Apple or Google. The Correspondent, June 22. https://thecorrespondent.com/546/coronavirus-apps-show-governments-can-no-longer-dowithout- apple-or-google/417112964268-93dd1b76. Accessed 25 June 2020.

50. Mol, A. (2008). The logic of care: Health and the problem of patient choice. New York: Routledge.

51. Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. Nature. https://doi.org/10.1038/d41586-020-01578-0.

52. Morozov, E. (2020). The tech 'solutions' for coronavirus take the surveillance state to the next level. The Guardian, April 15. https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilancestate- digital-disrupt. Accessed 25 June 2020.

53. Nissenbaum, H. (2010). Privacy in context. Stanford: Stanford University Press.

54. O'Neil, C. (2020). The Covid-19 tracking app won't work. Bloomberg 16 April. https://www.bloomberg.com/opinion/articles/2020-04-15/the-covid-19-tracking-app-won-twork. Accessed 25 June 2020.

55. Otterman, S. (2020). As the Nation Begins Virus Tracing, it Could Learn from this N.J. City. The New York Times, May 21. https://www.nytimes.com/2020/05/21/nyregion/contacttracing- paterson-nj.html. Accessed 25 June 2020.

56. Parker, I. and Jones, E. (2020). Something to declare? Surfacing issues with immunity certificates. https://www.adalovelaceinstitute.org/something-to-declare-surfacing-issueswith- immunity-certificates/. Accessed 25 June 2020.

57. Parker, M., et al. (2020). Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. Journal of Medical Ethics. https://doi.org/10.1136/medethics-2020-106314.

58. European Parliament. (2020). EU coordinated action to combat the COVID-19 pandemic and its consequences. https://www.europarl.europa.eu/doceo/document/TA-9-2020- 0054_EN.pdf. Accessed 25 June 2020.

59. Piketty, T. (2020). Capital and ideology. Boston: Harvard University Press.

60. Piper, K. (2020). Bill Gates's efforts to fight coronavirus, explained. Vox, May 4. https://www.vox.com/future-perfect/2020/4/14/21215592/bill-gates-coronavirus-vaccinestreatments-billionaires. Accessed 25 June 2020.

61. Pols, J. (2012). Care at a distance: On the closeness of technology. Amsterdam: Amsterdam University Press.

62. Rahman, Z. (2020). Black Lives Matter protester aren't being tracked with Covid-19 surveillance tech. Not yet. The Correspondent, June 3. https://thecorrespondent.com/507/black-lives-matter-protesters-arent-being-tracked-withcovid-19-surveillance-tech-not-yet/569187644025-767f5154. Accessed 25 June 2020.

63. Reich, R. (2018). Why philanthropy is failing democracy and how it can do better. Princeton: Princeton University Press.

64. Reisinger, D. (2018). Apple has hired nearly 50 medical doctors in wellness push. Fortune, December 13. https://fortune.com/2018/12/13/apple-hires-medical-doctors/. Accessed 25 June 2020.

65. Robbins, R. (2020). The White House is pinning its hopes on health tech to save the day.

Can it deliver? STAT, March 18. https://www.statnews.com/2020/03/18/coronavirus-whitehouse- pinning-hopes-on-healthtech/? utm_source=STAT+Newsletters&utm_campaign=e4b0e3649ehealth_tech_COPY_01&utm_medium=email&utm_term=0_8cab1d7961-e4b0e3649e- 151653869. Accessed 25 June 2020.

66. Ross, C. (2020). 5 burning questions about tech efforts to track Covid-19 cases. STAT April 18. https://www.statnews.com/2020/04/15/coronavirus-digital-contact-tracing-techquestions/. Accessed 25 June 2020.
67. Roth, A. et al. (2020). Growth in surveillance may be hard to scale back after pandemic, experts say. The Guardian, April 14. https://www.theguardian.com/world/2020/apr/14/growth-in-surveillance-may-be-hard-toscale-back-after-coronavirus-pandemic-experts-say. Accessed 25 June 2020.
68. Schmidt, E. (2020). A real digital infrastructure at last. Wall Street Journal, March 27. https://www.wsj.com/articles/a-real-digital-infrastructure-at-last-11585313825. Accessed 25 June 2020.
69. Schwartz, A. (2020). How EFF evaluates government demands for new surveillance. https://www.eff.org/deeplinks/2020/04/how-eff-evaluates-government-demands-newsurveillance- powers. Accessed 25 June 2020.
70. Scott, M, Braun, E. Delcker, J. and Manancourt, V. (2020). How Google and Apple outflanked governments in the race to build coronavirus apps. Politico, May 15. https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/. Accessed 25 June 2020.
71. Sharon, T. (2016). The Googlization of health research: From disruptive innovation to disruptive ethics. Personalized Medicine,13(6), 563–574.
72. Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake? Big Data & Society. https://doi.org/10.1177/2053951718819032.
73. Sharon, T. (2020). Beyond hostile worlds: The multiple sphere ontology of the digitalization and Googlization of health. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3633371
74. Taylor, L., Sharma, G., Martin, A., & Jameson, S. (Eds.). (2020). Global data justice and COVID-19. London: Meatspace Press.
75. Timmermans, S., & Mauck, A. (2005). The promises and pitfalls of evidence-based medicine. Health Affairs,24(1), 18–28.
76. Tometzkis, D. and Meaker, M. (2020). We were told technology would end Covid-19 lockdowns, but the truth is there's no app for that. The Correspondent. https://thecorrespondent.com/502/we-were-told-technology-would-end-covid-19-lockdowns-but-the-truth-is-theres-no-app-for-that/66389901600-2c9929bb. Accessed 3 June 2020.
77. Troncoso, C. et al. (2020). White paper on Decentralized Privacy-Preserving Proximity Tracing. https://github.com/DP-3T/documents/blob/master/DP3T%2520White%2520Paper.pdf. Accessed 25 June 2020.
78. Vaidhyanathan, S. (2011). The googlization of everything (and why we should worry). Berkeley: University of California Press.
79. van Dijck, J., Poell, T., & de Waal, M. (2019). The platform society: Public values in a connected world. Oxford: Oxford University Press.

80. Vaughn, A. (2020). Bluetooth may not work well enough to trace coronavirus contacts. New Scientist, May 12. https://www.newscientist.com/article/2243137-bluetooth-may-not-workwell- enough-to-trace-coronavirus-contacts/. Accessed 25 June 2020.

81. Verily. (2020). New Baseline COVID-19 Research Project launches to advance scientific understanding of virus, with initial focus on antibody testing. May 18 https://blog.verily.com/2020/05/new-baseline-covid-19-researchproject.html?utm_source=STAT+Newsletters&utm_campaign=3fdf688da3-health_tech_COPY_01&utm_medium=email&utm_term=0_8cab1d7961-3fdf688da3-151653869. Accessed 25 June 2020.

82. Volpicelli, G. (2020). Inside Dominic Cumming's coronavirus meeting with big tech. WIRED, March 12. https://www.wired.co.uk/article/dominic-cummings-coronavirus-bigtech. Accessed 25 June 2020.

83. Walzer, M. (1983). Spheres of justice: A defense of pluralism and equality. New York: Basic Books.

84. World Health Organization (WHO). (2020). Digital tools for COVID-19 contact tracing. https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex- 2020.1. Accessed 25 June 2020.

Acknowledgements

I would like to thank Frederik Zuiderveen Borgesius and Barbara Prainsack for commenting on earlier versions of this paper and the other members of the Digital Good team, Andrew Hoffman, Marjolein Lanzing and Lotje Siffels, for insightful discussions on this topic before and during corona times. I also thank the two reviewers who provided thoughtful suggestions for improvement and increased accuracy. Funding This work was supported by the European Research Council, Grant Number 804985.

Sjef van Erp

Who "Owns" the Data in a Coronavirus Tracing (and/or Tracking) App?

Abstract: To combat the spread of the COVID-19 virus, e-health has taken a sudden leap forward. Already use cases were studied to see if by means of advanced IT tools, particularly e-health applications (apps), patients could be monitored from their homes so they did not need to visit a hospital for frequent checks. The corona pandemic gave rise to the rapid development of tracing (and/or tracking) e-health apps, which allow quickly finding the source of an infection as well as others who might have been infected because they were in the close vicinity of someone who became ill. The development and widespread use of these apps makes it even more urgent than it already was to answer questions regarding to whom the data gathered through such apps belong and what belonging means. Can the owner of the mobile device be considered the "owner" of the data, what does "ownership" then mean, do other stakeholders (such as health care providers, public health authorities) also have a claim to "ownership"?

Introduction: e-health and coronavirus apps

As could have been expected in a rapidly expanding hybrid world, in which physical reality integrates with digital and virtual reality, lockdowns and forced physical isolation to combat the COVID-19 virus have resulted in an incredibly fast changing use of Internet Technology. We suddenly find online meetings no longer a surrogate for "real" meetings and we get used to, whenever possible, working at and from home to avoid running the risk of being infected by leaving the place where you live. All at once, e-health gains momentum, as doctors experience difficulties getting in touch with their patients in hospitals. Studies have already been conducted about the use of mobile phone or tablet applications (apps) to monitor patients while at home, but these were for the most part so-called "use cases" meant to test the app and see if the results are at least comparable to actual physical meetings with a patient[1].

[1] Cf., as examples, Paul Wicks (et al.), 'Innovations in e-health' (2014) 23 Qual Life Res 195; Lisa Abbott and Saxon Smith, 'Smartphone apps for skin cancer diagnosis: Implications for patients and practitioners' (2018) 59 Australasian Journal of Dermatology 168. It is interesting to note that Wicks (et al.) see the patient as the owner of the data. On p. 201 they write: "Privacy data protection and ownership is a major concern of any Internet-based application. The balance between the patient as the owner of data and the medical and academic profession's documentation and use of the data must be struck, with patient confidentiality always at the forefront without impeding the development of innovative solutions." Medical professionals seem quite aware of the problems regarding control over (access to) patient data.

[*] Reproduced with gracious permission of the Author. The original text was published in Ewoud Hondius, Marta Santos Silva, Andrea Nicolussi, Pablo Salvador Coderch, Christiane Wendehorst, Fryderyk Zoll (eds.) Coronavirus and the Law in Europe (Intersentia 2020), and is available, together with many other contributions related to the same topic, in open access, at the following page: https://intersentia.com/en/coronavirus-and-the-law-in-europe.html

Sometimes these apps already reached the stage of accepted tools in medical care, such as apps which allow you to take a picture of your skin, send it digitally to a health service provider whose servers, supported by Artificial Intelligence, perform an algorithm based check to see if, for example, there was a possibility of skin cancer. E-health uses all the possibilities offered by the Internet of Things which, by gathering data through sensors, makes data collection and data analysis possible where it would have been unthinkable before[2].

It can, therefore, not come as a surprise that in response to the COVID-19 pandemic the medical profession together with software developers began considering how e-health tools could be used during this pandemic. Regular patients were to stay at home as much as possible and there was an urgent need for monitoring them from a distance. Such distance monitoring was also considered to be a perfect tool for combatting the pandemic and the obvious technological response was to build a mobile phone application that would do just that. If persons infected with the virus could be found quickly and if others who had been in contact with them sufficiently long enough to be also at risk could likewise be discovered fast, then this would be a powerful instrument in the fight against the virus. The result is the worldwide development and rapid introduction of coronavirus apps, which "follow" people possibly infected with the COVID-19 virus. Such "following" can mean monitoring on a real time basis, monitoring through analysis of a (potential) patient's data history (for example by looking at behavioural patterns) or a combination of both. As a consequence, e-health no longer is an area for medical specialists, e-health software developers and lawyers specialised in health law but entered the world of essentially all of us. Thus, bringing the hybrid world of e-health with its integrated digital and physical reality not only very close to our homes, but even into our homes, and not only for the younger generations within a population but for all of us.

Make no mistake. This new hybrid world (in the case of the coronavirus apps: the world of e-health apps) is just as real as the old physical world, but it demands a different mindset to actually see and fathom what its effects are on us and what its wider societal, economic and political consequences are. Of course, we will all accept that what happens on a physical screen is "real" (the screen is physically there, the images can be seen, sounds can be heard), but it is different from a painting where you can feel the actual image (and not a projection of that image) by physically touching the canvass. A painting is physical and static. However, a computer screen, although physical, is meant to create impressions on our mind, which we consider to be equal to an impression of, for example, a painting. But, although we can certainly touch the screen, the images as such cannot be touched; they are not made of paint, but the result of software which projects these images on our screen so we will accept them as "real". Computer images are virtual and dynamic. Our law, and my focus in this contribution is more specifically on property law, still takes this old physical and static perception of reality as its foundation. We expected to have time for reconsidering these old and established values, policy choices, principles, notions, concepts and ground rules, developed over several centuries, to see whether they would fit in this new virtual and dynamic world. If they would not fit, we expected to have

[2] See Martina Barbero (et al.), Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability (European Union 2017) Final Report. A study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte, 347, discussing Real-Time Location Services (RTLS) used for patient and asset tracking.

time for considering either adaptation of existing rules or the development of new rules. The COVID-19 pandemic, by causing an incredibly fast rise of e-health in the form of coronavirus apps, shows, however, that time is running out, we need to give answers now. In this contribution, I will focus on the legal nature of the data gathered by the COVID-19 apps. More precisely, I will question whether these data can "belong" to (be "owned" by) anyone or are the data to be considered "res nullius", what does "belonging" ("owning") mean and, if data can belong to anyone, to whom do they belong. To put it differently: I will look both at the possible existence of a property entitlement concerning data gathered by coronavirus apps and, if such entitlement can be accepted, what its content is and to whom such entitlement should be allocated.

The so-called "Fourth Industrial Revolution" (Industry 4.0)

The rise of the digital economy with its virtual reality is the result of developments which are relatively recent. It still took us quite some time from the era of mechanisation, the steam engine and water power to the rise of mass production and the widespread use of electricity, but it took less time to develop electronic and IT systems and automation. In today's world developments even go so fast that, if you do not follow changes very closely, "recent" innovations have already been overtaken by others. Those who saw the introduction of the fax machine, also witnessed its exit. In order to give a proper response to such changes, lawyers need to understand – at least at a technically superficial, but basic level – advances regarding cyber-physical systems, Distributed Ledger Technology (including so-called smart contracts), Artificial Intelligence and the Internet of Things. These are the stages from the First to the Fourth Industrial Revolution, as described by Schwab, where the latter stage is happening all around us and who knows where it will end?[3]

This is all going on at such a pace that for many lawyers developments seem problematic to follow and difficult to comprehend, making it hard to learn how to live with it let alone start thinking about redesigning the law to adapt it for this new hybrid world. It seems as if either you belong to this new world, and then you depend on having access to the Internet and your attitude is having a flexible mindset to understand what is going on, or you do not belong to this world, which cuts you off from the hybrid world that others join. Being an outsider to this new world not only may happen at a mental level but also – more than we in Europe sometimes tend to think – at a physical level. Third world countries have a far less developed IT structure than can be found in, for example, the European Union, North America and China. All of this echoes how we look at the use of IT and e-health as part of modern medicine. The COVID-19 pandemic has created (and still creates) havoc in countries all over the world and, pressed by an urgent need to react and prevent the spread of the disease against a background where, until now, no effective – preventive or curative – medication has been found, it is very understandable that IT solutions are looked at. In order to stop the spread of the virus, it is of utmost importance to identify new infections and to trace back infection chains. Because spreading happens, as far as we know at present, primarily through human interaction, it is this interaction which needs to be monitored and regulated. Monitoring requires tracing and/or tracking. In the advancement of ideas about how people could be traced and/or tracked, so as to prevent

[3] See Klaus Schwab, The Fourth Industrial Revolution (Penguin Random House 2016); Klaus Schwab, Nicholas Davis, Shaping the Future of the Fourth Industrial Revolution: A guide to building a better world (Penguin Random House 2018).

them from spreading the virus and make certain that they undergo medical treatment, IT technology is proving to be a prime facilitator[4].

Where societies have become or are in the process of becoming more affected by technological change and, consequently, develop into information societies, a large part of the population will most likely use a mobile phone. These phones can only work if they are connected to a wider network, which allows following them. Localisation data is gathered by, among others, telephone providers and has turned out to be a very valuable source of information which can be used for various purposes.

Thus, the idea to develop a mobile phone application ("coronavirus app"), which collects information about where a person was and with whom that person has been in relatively close contact, appears simply a logical step in a hybrid and data driven society. However, the data which are collected by using these so-called coronavirus apps are not only a source of personal information about your private life (where you were, with whom you were in close contact) but also a source of information relevant from the perspective of public health and the dire need to do research about the virus in order to find curative medication. The gathered data are therefore next to being primarily of a personal nature also of non-personal (general interest: public health) nature. In other words: the use of coronavirus apps brings to the surface a deep conflict between on the one hand the need to protection of everyone's personhood by shielding people from having to give up their privacy regarding personal location and contact data, for they are part of how they live and who they are, and on the other hand the interest of public health and medical research, not to forget further societal and economic interests.

From a more traditional legal viewpoint, all of this is confusing. The law, particularly property law, leans towards revolving around what we can find in the physical world outside us and from that perspective property lawyers encountered grave difficulties when dealing with intangible things, such as monetary claims and the outcomes of human creativity. In some legal systems, monetary claims were not considered to be "things" and could for that reason not be owned, but as monetary claims represent considerable monetary value one could be "entitled" to the claim and the claim could be offered as security for a loan. Regarding the products of human creativity, it was also clear that such products represented considerable economic value and also could not be ignored. Because these products were even further away from the objects of traditional property law than monetary claims, the final outcome of the theoretical struggle was to consider the law that governs these products as a new, separate legal area with its own framework, although – very much like we saw with claims – not infrequently mimicking traditional property law.

In the case of the fundamental building blocks of the digital economy: data, questions about their legal status have become even more pressing than earlier problems caused by the growing economic importance of monetary claims and human creativity. All of the problems, which I mentioned earlier, triggered by the growing impact of IT on our lives, are coming together here. The world has become hybrid, with both real and digital aspects which more and more interact and even integrate. This hybrid world functions on the basis of technology, both physical (hardware) and non-physical (software), that results in data, which by their very technical nature can be copied, combined, shared etc. in ways which

[4] See 'BKC Policy Practice: Digital Pandemic Response Provides Practical Guidance, Expert Opinion for Decision Makers | Berkman Klein Center' (28 July 2020) https://cyber.harvard.edu/story/2020-07/bkc-policy-practice-digital-pandemic-responseprovides-practical-guidance-expert accessed 10 August 2020

until relatively recently were inconceivable in the real world. Data provides a meaning to us and about us, in other words: information, is now so readily available that it seems as if we as human beings are now also becoming hybrid personalities. We have a real life and a life in virtual environments, and also these lives are now merging and becoming hybrid. Our physical lives are reflected in our virtual lives to such a degree that data IT companies perhaps might know more about us than we do ourselves. As such this requires that we are protected against the unlimited and unjustified use of data which affect us as a person (privacy and data protection), but it can also not be denied that these very data are part of the present digital economy (and consequently the free flow of non-personal data) and might be of crucial importance from the perspective of public health. The rapid development of coronavirus apps has brought issues to the forefront even more pressing than they already were and has resulted in an academic debate even more intense than it already was. From the perspective of coronavirus apps this results in the following two questions. What is the legal status of location and contact data? To whom, if any, do they belong? And if they can belong to someone, who, upon a balance of interests, is entitled to these location and contact data?

What are "tracing" and "tracking" apps?

Before I will embark upon an attempt, while concentrating on coronavirus apps, to offer a methodology towards answering questions about a possible framework for entitlements ("ownership") to data, first some clarification about the technical side of these apps must be given.

There is a difference between a "tracing" and a "tracking" app, although apps at the same time could do both. If an app permits tracing, this means that it is possible, retroactively, to find out where a person, on whose phone the app is installed, has been and with whom that person was in contact. The latter can be done in several ways, but one way is using Bluetooth technology. The use of this technology requires that mobile phone users allow their phones to be connected via Bluetooth.

Whenever the mobile phones come within one another's vicinity for a relatively longer period of time, the phones store an anonymous code which links the two persons as having been present at a particular time in a particular spot. As soon as one of the persons reports in the app on his/her phone that (s)he has become ill, the phone will send a message to everyone stored on that phone who through the Bluetooth codes can be traced back as having been in close contact with that person. Technically the message that someone is ill might also be sent to a central server that then copies the various anonymous Bluetooth codes stored on the infected person's phone, which server will be checked regularly by other apps to find out whether 'their' code is now in the database, warning that a risk of contamination exists. This whole process can be done without the persons involved knowing anything else about one another but for the risk of getting infected. Another possibility is that the data are not first only stored on your mobile phone but directly on a central government server. An advantage could be that the government, in the interest of public health, then also has the information about people falling ill, but at the same time, there is a clear privacy threat, as the government could find out which contacts a particular person had. Anonymity would no longer be guaranteed. A further step towards government involvement is when the app is not tracing, but actually tracking you. In that case, the mobile phone transmits location data to a central government server, which can

follow everyone using the mobile phone with the app installed. That allows government authorities to contact persons directly who have been in touch with COVID-19 infected phone users. Apps can also do both: allow tracing, next to tracking[5].

A government could also, of course, demand direct access to the location data which are being stored by telecom providers, without an app having been installed, but from a European perspective that would be highly problematic considering the rigorous protection mechanism laid down in the General Data Protection Regulation (GDPR) and the law governing telecommunications providers[6].

Stakeholders

Medical health apps are part of a rapidly developing medical technology or "medtech" market: the use of modern IT as part of diagnosing, preventing and curing disease[7].

Internet Technology is seen as both an effective and efficient tool in medical science. That these apps could turn out to be a valuable tool for medical care is, of course, primarily relevant for patients and healthcare providers, such as family doctors and medical specialists, but that these apps also could increase efficiency and become cost-cutting tools is very relevant for health insurers and governments[8].

[5] See Patrick Howell O'Neill, Tate Ryan-Mosley and Bobbie Johnson, 'A flood of coronavirus apps are tracking us. Now it's time to keep track of them.', presenting an MIT Technology Review Covid Tracing Tracker, MIT Technology Review 7 May 2020 https://www.technologyreview.com/2020/05/07/1000961/launching-mittrcovid-tracing-tracker/ accessed 16 July 2020; cf. also the various contributions on tracing and tracking apps as part of MIT's 'Privacy in the Pandemic' series https://slate.com/tag/privacy-in-the-pandemic accessed 16 July 2020.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), [2016] OJ L119/1.

[7] Cf. Martina Barbero (et al.), Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 345.

[8] See, e.g., Kimberly van den Bergen (et al.), The future of the medical technology market. Addressing challenges and utilising opportunities (Rotterdam 2018), a report prepared for the Dutch government and presented to the lower house ("Second Chamber") of the Netherlands Parliament. One of the tendencies signalled in the report is "patient ownership". On p. 16 the report states: "The position of patients/consumers is changing and driven by the digital transformation, personalised care, remote healthcare, regulation and the focus on prediction and prevention. Patients are no longer simply recipients of healthcare, but are selfmanaging emancipated participants, in combination with their social network. There is and will be an increased focus on patient centeredness and patient ownership: patients are seen as co-producers of data as they increasingly have health technologies available to actively measure certain (surrogate) outcomes and aspects which are meaningful for their daily lives, and which enable active engagement." It can be assumed that "ownership" here was not used in a legal sense, but to explain how a patient experiences the use of "his/her" data. Still, the fact that the term ownership is used expresses a wider feeling that data are not just there, they are not "res nullius" and do belong to someone.

Furthermore, these apps provide important information necessary for developing new medicines or new methods of treatment and, therefore, also the pharmaceutical industry has a stake. Next to the pharmaceutical industry, stakeholders can also be producers of medical equipment. Blood pressure measuring instruments can be built into smart watches which, being part of the Internet of Things, may send the information gathered to the developer of the smartwatch, the software developer or others with an interest in these data. So-called "health apps" are already used widely by, for example, long distance runners and others who are interested in their personal health and well-being. The development of coronavirus apps was, considering this rapid expansion of medtech among the general public, as such only a logical next step. However, unlike health apps which you can download from Google Play or the App Store, checking your heart beat, the distance you walk on a day etc., coronavirus apps are no longer purely about patient-centred care[9].

Stakeholders regarding access to data collected by coronavirus apps are, therefore, next to obviously the (potential) patients themselves, health care providers, health insurers, health authorities, governments, the pharmaceutical industry, producers of medical equipment, hardware and software developers. With regard to software developers, we see great interest from the global tech industry, such as Google and Apple. Their initiative is, of course, to be supported, as both companies are active players on global data markets and, because of their access to extremely big data, are perhaps more than many of us aware of the enormous worldwide impact which the COVID-19 pandemic has. Also, they did not develop an app as such but, in their own words an "Exposure Notification system in service of privacy-preserving contact tracing"[10].

However, both Google and Apple are US based companies and in light of the growing tendency towards de-globalisation, economic disintegration as a result of growing nationalism, isolationism and a call for regaining sovereignty, there might come a moment where political and strategic concerns are given precedence over idealist interests. Political data analytics might then take over from national patient-centred care analytics. It is, therefore, not unthinkable that a patient's health data (hopefully at least in an anonymised or pseudonymised format) might flow across the world to be used for research purposes in a foreign jurisdiction only for its own internal strategic purposes. Such a government is of course not a legitimate stakeholder, but even as an illegitimate interested party it should not be ignored. Finally, when looking at who the stakeholders are regarding coronavirus apps, we must take into account that the European Union is an internal market where freedom of establishment and free flow of non-personal data exists, and where within the Schengen area the freedom exists to cross borders without being checked. Although these freedoms have been curtailed as part of national lockdown measures, still people work, travel and go on holiday crossborder.

Within such an area of free travel, it is crucial that national coronavirus apps also work outside the countries for which they were developed. This is why the European Commission has become very active in at least coordinating the efforts by Member

[9] Cf. Lucienne Berenschot (et al.), The role of medical technologies and devices for patient-centred care (Rotterdam 2018), a report prepared for the Dutch government submitted to the lower house ("Second Chamber") of the Netherlands Parliament. It seems as if the widespread use of tracing or tracking apps was not really on the minds of the drafters. A possible global pandemic was outside their vision.

[10] See https://www.apple.com/covid19/contacttracing accessed 16 July 2020.

States to develop coronavirus apps. Together with the Member States the European Commission developed a European Union (EU) toolbox to promote common standards, gave guidance on data protection and as part of the European eHealth Network presented "Interoperability guidelines for approved contact tracing mobile applications in the EU"[11].

Thus, we need to add the European Union itself as another stakeholder concerning the data which result from such apps. In certain respects also the World Health Organisation (WHO) is a stakeholder, given the worldwide nature of the pandemic, but the WHO is largely dependent on the cooperation of states regarding the gathering of data.

The difficulty with coronavirus apps is that the various stakeholders at the same time have shared interests (preventing or curing a disease) and diverging interests, more specifically health, commercial and public (societal, economic) interests, next to the reality that the apps potentially or perhaps already even actually are of great political relevance.

We all agree that we are, directly and indirectly, affected by the COVID-19 pandemic, we all want to avoid becoming ill and that, once infected, we do not harm others by spreading the disease. However, we seem to deeply disagree when it comes to being traced or even tracked, because contact and localisation data resulting from tracing and tracking apps can also very well serve different aims than medtech purposes considering the diverse and sometimes opposing interests of stakeholders.

Although the collected data are raw facts which gain meaning and can only be made useful in light of the purpose for which these data are being analysed, perhaps after having been combined with other data, still control over these raw facts is of vital importance for all interested parties.

Given the diversity of stakeholders and considering the possibility that data once collected could easily be used for other than purely medical purposes, no longer with the interests of patients as the underlying aim, fundamental legal questions have to be asked. To my mind the first, and all others enveloping, question is: to whom belongs the data in the first place or phrased differently: Who "owns" the data? What does "belonging to" and "owning" mean in this respect? These are questions about (a) what the object of ownership is, (b) who the subjects can be holding a right of ownership, (c) the content of an "ownership" right and (d) the relationship with others who also perhaps also hold rights in such an object. This is the heartland of property law, although not what might be called "classical" property law dating back to an era where first copying texts in monasteries and then using the printing press was already a revolution in disseminating information. Data as "res nullius" or part of "dominium eminens"?

Although data flows across borders, EU Member States have been developing their own versions of COVID-19 apps. Defending public health was (and to a greater or lesser degree frequently still is) seen as, primarily, an area strictly for national policy. The result

[11] See Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, [2020] OJ L114/7. In their own words the European Commission requires coronavirus apps to be tracing apps, which "must be voluntary, transparent, temporary, cybersecure, using temporary and pseudonymised data; they should rely on Bluetooth technology and approved by national health authorities, and be interoperable across borders as well as across operating systems." For more information on the other aspects of EU policy mentioned see: https://ec.europa.eu/digital-singlemarket/en/news/coronavirus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu accessed 16 July 2020.

was, except for a shared debate on privacy and data protection, a tendency to move away from European integration and sometimes even international coordination towards returning to old-style public international law notions of sovereignty. In such a view data about a country's citizens are seen as somehow "belonging" to that territory and are, therefore, what the Australian government called with regard to criminal intelligence a "national asset"[12].

It is interesting to see that also Germany seems to approach data ownership questions from the perspective of sovereignty, but then sovereignty from an individual perspective. In a discussion paper from the German Ministry for Traffic and Digital Infrastructure it is stated that a "Digitale Souveränität" exists[13]. The paper, however, does not use the term "sovereignty" in the public international law sense, but as meaning "wirtschaftliche, positive Verwertungsmöglichkeit" (an economic and positive opportunity to make data valuable).

But even if sovereignty is limited in the way as is done by this German government paper on digital sovereignty, such personal sovereignty can only be given and defended by a state acting under its public international law sovereignty. Data are then, consequently, "things" under the control of the state and the state can, as a consequence, limit their transfer cross-border and can take data from individual citizens in the public interest. This is clearly the idea underlying the control of data flows in countries which created or are creating digital firewalls around them, demanding that data which are created, processed, analysed and transferred must remain on servers within that state's territory. Depending on the political system and data content, the state in this view also has the right to control such content and intervene if deemed necessary in the interest of public policy, public morals or the political foundations upon which the state is built.

I will leave aside here the economic debate about public goods, which are both non-

[12] Australian Criminal Intelligence Commission, Australian Criminal Intelligence Management Strategy 2017–20, Intelligence partnerships for a safer Australia (Commonwealth of Australia, 2017), for example on p. 3. See Lyria Bennett Moses, 'Who owns information? Law enforcement information sharing as a case study in conceptual confusion', (2020) 43(2) UNSW Law Journal 615, 618, 635. It seems that no one is arguing that data belong to no one and are "res nullius", although it has been argued that personal data might be qualified as existing outside the realm of commerce ("res extra commercium"), see Václav Janeček and Gianclaudio Malgieri, 'Commerce in Data and the Dynamically Limited Alienability Rule', in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), Data as Counter-Performance: Contract Law 2.0? (Hart/Nomos 2020). It resembles arguing that data are part of a state's eminent domain or "dominium eminens": "The state's right to exercise sovereignty and direct control over its territory, or any part thereof." Definitions taken from Aaron Fellmeth and Maurice Horwitz, Guide to Latin in international law (OUP 2009, online 2011). On the history of the eminent domain doctrine see Katherine McFarland, 'Privacy and Property: Two Sides of the Same Coin: The Mandate for Stricter Scrutiny for Government Uses of Eminent Domain' (2004) 14 BU Pub Int LJ 142, 144.

[13] "Eigentumsordnung" für Mobilitätsdaten?, 86. It seems as if in questions regarding data ownership the term "sovereignty" is becoming just as ambivalent as the term "ownership". See also on the confusing use of the term "sovereignty" Julia Pohle, 'Digitale Souveränität' in Tanja Klenk, Frank Nullmeier and Göttrik Wewer (eds.) Handbuch Digitalisierung in Staat und Verwaltung (Springer VS forthcoming), also available electronically https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435017 accessed 16 July 2020.

excludable and non-rivalrous. This aspect is particularly relevant when we could also consider academic researchers to be stakeholders. Indirectly they certainly are, as national health authorities will need input from academic and clinical research. The difficulty with e-health data gathered by coronavirus apps is that, if the app is technically only a tracing app, the data on the phone may for the time being only have been shared with a specific group of other mobile phone users who also have their Bluetooth function switched on. In that case only a limited number of data copies exist, limiting and thus excluding access and securing privacy. Nevertheless are the data still of a non-rivalrous nature[14].

This all may sound like a state with hardly any political freedoms, but it should be realised that no state accepts data flows with objectionable (i.e. criminal) content. States do intervene to protect citizen's fundamental rights and freedoms if data contains abusive substance, criminal law enforcement agents are given access to data as part of a criminal investigation and civil law enforcement agents may access a person's assets in judicial enforcement proceedings at the request of a creditor against his/her debtor(s). So to some degree we accept that the state has some form of eminent domain also regarding data as expression of its sovereignty. In the European Union this implies that, as far as Member States transferred their sovereignty to the Union as part of its developing internal market, the EU may also, albeit to the extent limited by the European treaties, control data flows and in fact this is precisely what the EU does. I only need to refer to the ePrivacy Directive, General Data Protection Regulation (GDPR), the Regulation on the free flow of nonpersonal data and the Directive on Open Data and the Re-use of Public Sector Information[15].

It is within the framework of both these regulations that the EU is considering whether it can oblige governments and businesses to share information[16].

[14] Cf. David Blumenthal, Characteristics of a public good and how they are applied to health caredata, in Claudia Grossmann et al. (eds.), Clinical Data As the Basic Staple of Health Learning : Creating and Protecting a Public Good: Workshop Summary (National Academies Press 2010) 139.

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerningthe processing of personal data and the protection of privacy in the electronic communicationssector (Directive on privacy and electronic communications), [2002] OJ L201/37 (to be replaced by a Regulation on Privacy and Electronic Communications); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), [2016] OJ L119/1, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, [2018] OJ L303/59 and Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), [2019] OJ L172/56 (replacing, from 17 July 2021, Directive 2003/98/EC of the European Parliament and of the Council, OJ L345/90 and Directive 2013/37/EU of the European Parliament and of the Council, OJ L175/1). See also the Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (COM(2019) 250 final).

[16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions

"Ownership" of data?

In academic debates about the legal status of data, using the term "ownership" seems to provoke immediate and deep conflicts of opinion between public lawyers, particularly public lawyers focussing on privacy and data protection, and private lawyers[17].

Merely using the term "data ownership", even when it is argued that we need to find a balance between shielding a person's privacy and giving proper weight to the interests of market participants who are in fact dealing in data for commercial purposes, is seen by some privacy lawyers as coming close to a contention which is inherently objectionable. The argument is that when data are so connected with an individual that they can be seen as part of one's personhood and are, therefore, 'personal data', a reference to marketability (this being equal to accepting data "ownership") by itself comes close to a violation of someone's human rights, and reduces a person from a subject to an object.

It has been argued that the Internet is in a process of recreating a feudal society where an elite group governs others who must serve their economic interests. This is called the "feudal Internet"[18].

Next to this split between public and private lawyers, we can see a further divide, throwing the debate even into further upheaval, caused by a fundamentally dissimilar approach, so it seems, towards legal thinking resulting from differing legal traditions, especially Civil Law and Common Law. Civil lawyers are inclined, as they are trained to think in more theoretical and systematic terms, to look at the debate from the viewpoint of trying to reach a consistent terminological framework which fits with the needs of legal practice. Common lawyers, however, are trained to think more from the perspective of problem solving, which however needs to be done in a conclusive way to convince those

Towards a common European data space ({SWD(2018) 125 final}, COM(2018) 232 final); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data (COM(2020) 66 final). On p. 29 and 30 of the Communication on a European Strategy for Data, the European Commission proposes to create a "Common European health data space". Whether the "sharing" or "pooling" of data will always be beneficial has already been questioned. See the report published by the European Commission, Directorate-General for Competition: Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, Competition Policy for the digital era, Final report (Publications Office of the European Union 2019), where next to pro-competitive advantages also anti-competitive aspects are being considered.

[17] See for an overview of the debate from the position of European Union and property law Andreas Boerding (et al.), 'Data Ownership—A Property Rights Approach from a European Perspective', (2018) 11 J. Civ. L. Stud., available at: https://digitalcommons.law.lsu.edu/jcls/vol11/iss2/5 accessed 16 July 2020.

[18] See Sascha D. Meinrath, James W. Losey and Victor W. Pickard, 'Digital feudalism, Enclosures and erasures from digital rights management to the digital divide', Commlaw Conspectus 2011, 423; Natalie M. Banta, 'Property Interests in Digital Assets: The Rise of Digital Feudalism', 38 Cardozo L. Rev. 1099. In relatively recent Western history, a most horrific example of dehumanisation and denial of personhood is the Dred Scott case, in which the US Supreme Court ruled that slaves had no standing in court, lacking US Citizenship, Dred Scott v. Sandford, 60 U.S. 393 (1856).

involved that the outcome is based on solid arguments and not on haphazard thoughts. Still, even within the two traditions, another difference of approach can be found. Sometimes the arguments are highly formalistic and dogmatic, sometimes more flexible and open to changing times. Let me first give two examples of the rather formalistic approach, one from a Civil Law jurisdiction another one from a Common Law jurisdiction. The German Civil Code (BGB) states in § 90: " Only corporeal objects are things as defined by law." § 903 states: "The owner of a thing may, to the extent that a statute or third-party rights do not conflict with this, deal with the thing at his discretion and exclude others from every influence. The owner of an animal must, when exercising his powers, take into account the special provisions for the protection of animals." The question whether data can be an object of ownership, is to be answered in the negative. Data is not a "thing" according to § 90 and can, in light of § 903, not be owned. In spite of the elaborate discussions in German legal literature on this question, this to my mind is the essence of the dogmatic debate[19].

Interestingly enough, a comparable methodology can be found in recent Australian literature, but not from the perspective of private law but criminal law[20].

If the starting point for the analysis (including interviews with law enforcement agencies) is the suggestion that "rather than searching for a coherent conception of information ownership, what matters is clarity around the rules for allocating the power to make decisions with respect to information and allocating responsibilities for information"[21], then the final conclusion of the interviews and the following theoretical analysis is an almost given fact. Data ownership does not exist.

European Union law certainly agrees with the latter statement when it comes to existing EU law regarding data as such. Neither the ePrivacy Directive, the General Data Protection Regulation (GDPR), the Regulation on a Framework for the Free Flow of Nonpersonal Data, the EU's laws on intellectual property, nor the Trade Secrets Directive contain a framework for accepting ownership of data outside the protection of personal data, trade secrets and software[22].

[19] Cf. Andreas Boerding (et al.), 'Data Ownership—A Property Rights Approach from a European Perspective', (2018) 11 J. Civ. L. Stud.,available at: https://digitalcommons.law.lsu.edu/jcls/vol11/iss2/5 accessed 16 July 2020, 359.

[20] See Lyria Bennett Moses, 'Who owns information? Law enforcement information sharing as a case study in conceptual confusion', (2020) 43(2) UNSW Law Journal 615.

[21] Lyria Bennett Moses, 'Who owns information? Law enforcement information sharing as a case study in conceptual confusion', (2020) 43(2) UNSW Law Journal 615, 624: "The law enforcement community includes individuals with two different understandings of what 'ownership' of information might mean. Each of these two conceptions of ownership comes with common means of identifying the entity that 'owns' information and articulating the consequences of that ownership. In particular, ownership as an allocation of power or control over information generally suggests a single owner, whereas ownership as the allocation of responsibilities for information may involve multiple owners. This suggests that, rather than searching for a coherent conception of information ownership, what matters is clarity around the rules for allocating the power to make decisions with respect to information and allocating responsibilities for information."

[22] For databases see Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, [1996] OJ L77/20, for software see Directive 2019/790/EU of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ 2019, L 130/92 (effective 7 June 2021) and for trade secrets see

Several reports have been published on this, and they all come to the same conclusion, with which the European Commission is now apparently agreeing[23]. However, this leaves the question unanswered whether data as such can be owned and if the European Union still should not introduce such a notion. Given that, at least for the time being, no unambiguous EU law in this area exists, answers can only be given at the level of the Member States, resulting in the need for a comparative legal examination. Such a comparative exercise, in light of socio-economic reality, might lead to a badly needed flexible and open mind, which is not held captive – not excluding being inspired! – by past dogmatic thinking. In that respect the recently expressed view by the European Commission that stakeholders do not favour a "data ownership" type of right is remarkable, considering that it is immediately followed by admitting that we do need rules on access. To my mind, there is hardly any difference between ownership and access.

What is, given the nature of data, ownership else but being in control of access, portability, transfer or erasure (including the desisting from control or processing of data)? What else, to put it differently, than the right to manage data in an environment where several people at the same time may have concurring or competing rights to access, portability, transfer and erasure?[24] I must admit that the term "ownership" and particularly the use of that term in English has an inherently ambivalent meaning. In (particularly American) English you can "own" a management process next to "owning" your car. The meaning of the term in a legal sense is also not clear, to put it mildly, certainly not from a comparative viewpoint[25].

Where in Germany, ownership is limited to the most extensive right concerning physical things, in France, ownership can also be the most extensive right with respect to

Directive 2016/943/EU of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, [2016] OJ L157/1.

[23] Cf. also, next to Martina Barbero (et al.), Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability; Benoit Van Asbroeck, Julien Debussche and Jasmien César, Building the European Data Economy. Data Ownership. White Paper (Bird & Bird 2017), Data Ownership. A new EU right in data. Supplementary Paper (Bird & Bird 2017). See recently the view of the European Commission in their Communication Towards a common European data space, 9: "In general, stakeholders also do not favour a new 'data ownership' type of right, with a range of inputs indicating that the crucial question in business-to-business sharing is not so much about ownership, but about how access is organised."

[24] Martina Barbero (et al.), Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 386, discussing the nexus between data ownership, access to and use of data, and the interoperability of services in Industry 4.0 in general and In such an environment, ownership of data means management of access, and it seems as if the European Union is moving into that direction.

[25] Cf. Yael Emerich, Droit commun des biens: perspective transsystématique (Montreal : Éditions Yvon Blais, 2017), p. 241 ff. (discussing the "notion" – not the "concept" – of a thing ("bien"); Sabrina Praduroux, 'Objects of property rights: old and new' in Michele Graziadei and Lionel Smith (eds.), Comparative Property Law (Cheltenham and Northampton: Edward Elgar, 2017), p. 51 ff. Remarkably enough, although the book was published in 2017, Praduroux does not devote any attention to the enormously important role of data and the data economy.

immaterial things, such as a claim. There is clearly a legal diversity from a comparative law perspective[26].

Nevertheless, without on the one hand becoming too elusive and on the other hand falling in the abyss of technicalities, my approach is to look for common thought patterns or, if you wish, stepping stones or signposts.

Property law is about legal relations between a subject and a considerable and relevant group of other subjects regarding an object. Property rights have a far greater effect than rights arising from contracts, tort or unjust enrichment. These latter rights are between two or more specific persons, where one person has a right which corresponds with an obligation resting on another person.

Interestingly enough, the law regarding such personal rights does not seem to focus on the right itself but, more negatively, on the corresponding duty and is called the law of "obligations". The law of property is more positive, it focuses on what the holder of the right can do and is only negative when it regulates how others can be excluded, but even that appears to be a positive exclusion. In the law of property, the rights conferred on a person are against a group of other persons, in Civil Law terminology even the whole world ("erga omnes"). These other persons have a duty to accept such property right[27].

This makes a property right very strong and this is why it is given the qualification "absolute" to distinguish it from more personal rights, which are qualified as "relative". The terms "absolute" and "relative" express the strength of the right by delineating against whom it can be invoked. To put it differently: also absolute rights are relative in the sense that a subject can only have rights against other subjects. Saying that a property right is a right in a thing is therefore an unfortunate expression. A property right concerns the legal position of a subject vis-à-vis other subjects regarding an object. Another question is, as we already saw, which objects the law recognises, in other words: which legal objects does the law accept? Can only physical things be legal objects, can monetary claims or the products of human creativity be a legal object too? And finally, also the subject who has such a property right concerning an object is defined by the law: only natural and legal persons can be a legal subject. Taken all of the above together we see that legal systems, given the absolute nature of property rights, not only limit the number and content of these rights but also the number and content of legal objects and the various categories of legal subjects. Traditionally, it is argued that limiting the number and content of property rights is at the heart of the doctrine of the "numerus clausus" of property rights. The law lays down in mandatory format which rights are possible as having absolute effect, what the content of these rights is and how these rights are created, transferred and extinguished. This numerus clausus doctrine, therefore, has both a substantive and a procedural side. However, what has been forgotten is that, when the law defines or describes – depending upon how

[26] Although Christian v. Bar, Gemeineuropäisches Sachenrecht (Volume I, C.H. Beck 2015, Volume II, C.H. Beck 2019) seems to imply that property law underlies an overall legal-dogmatic theory and system. For a brief overview of definitions of ownership in various legal systems see Christian v. Bar, Vol. I, 499. See also: Sjef van Erp and Bram Akkermans (eds.), Ius Commune Casebooks for the Common Law of Europe. Cases, Materials and Text on Property Law (Hart Publishing 2012), 211.

[27] Cf. for a further analysis: Williem Loof, Of trustees and beneficial owners. An inquiry into the proprietary aspects of trusts and trust-like devices from a European private law perspective (Datawyse/Universitaire PersMaastricht, 2016), 36.

the legal system approaches its basic concepts and terms – the number and content of absolute rights, the object of such right is part of the definition. By being an element of the definitional framework, the object qualifies what the right's content is, as the right only concerns that particular object. It could, therefore, be said that the object is a "qualifier" of the right, it gives shape to what the right means[28].

This is, furthermore, done against the background that only natural or legal persons can be holders of a right. A clear example is the Netherlands Civil Code. In article 5:1 ownership is being defined as the most complete right which a person can have regarding a thing. What a thing is can be found in article 3:2, where it is defined as physical objects prone to human control. The definition of ownership is qualified by the object of the right with, furthermore, a reference to natural persons by demanding that human control be the yardstick. The qualification, and consequently limitation, of the right by including the type of object in its definition implies that different types of "most complete" rights can be created, depending on the object. This is, both from a historical and from a comparative point of view, nothing new.

Before the French Revolution, the Civil Law knew the distinction between "dominium directum" and "dominium utile". The dominium directum was the superior's right to collect rent from the person actually using the land (inferior), a situation of duplex dominium. After the French Revolution a different type of ownership was introduced: dominium plenum, although the French Cour de Cassation decided in the famous Caquelard c. Lemoine case that the definition of ownership in article 544 of the French Civil Code was an expression of French common law ("droit commun"), but did not exclude other types of ownership, as pre-existed under the customary law of Normandy[29].

The Cour de Cassation affirmed its approach in two more recent cases regarding the Maison de Poésie, introducing a new property right the "droit réel de jouissance spéciale" (property right of special use)[30].

[28] For a further analysis see Sjef van Erp, Ownership of data and the numerus clausus of legal objects, in Sandra Murphy and Padraic Kenna (eds.), eConveyancing and title registration in Ireland (Dublin: Clarus Press, 2019), p. 125-140.

[29] Caquelard c. Lemoine, Req. 13 februari 1834, D. 1834, 1, 218, S. 34, 1, 205. The decision is very short and reads as follows : "Sur le premier moyen, tiré de la violation des articles 544, 546, 552 et 691 du Code civil, et 607 de la coutume de Normandie: Attendu, en fait, qu'après avoir, dans ses motifs, reconnu formellement à Caquelard et à Lemoine un droit de copropriété sur la berge ou chaussée dont il s'agit, et avoir expliqué la nature et les limites respectives de ce droit, d'après les faits et les circonstances particulières de la cause, et notamment l'origine commune des deux usines, la possession réciproque, l'intérêt commun à la conservation de la berge, la charge de l'entretenir, et l'appréciation de certains actes, l'arrêt attaqué reconnaît et déclare de nouveau, dans son dispositif, le même concours de propriétaires et les limites respectives de leurs droits; ce qui écarte l'application des articles 691 du Code civil, et 607, coutume de Normandie; Attendu, en droit, que les articles 544, 546 et 552 du Code civil, sont déclaratifs du droit commun relativement à la nature et aux effets de la propriété, mais ne sont pas prohibitifs; Que ni ces articles, ni aucune autre loi, n'excluent les diverses modifications et décompositions dont le droit ordinaire de propriété est susceptible;"

[30] Maison de Poésie I, Cass Civ 3ème 31 October 2012, no. 11-16304 and Maison de Poésie II, Cass. 3ème civ. 8 September 2016, n° 14-26.953.

It is also interesting to note that in the recent Belgian property law reform also a more flexible and open approach towards the doctrine of numerus clausus can be found[31].

Article 3:3 new Belgian C.C. on the one hand enumerates which property rights are recognised under Belgian law and that only the legislator can change this list but on the other hand, it is made clear in article 3:1 new Belgian C.C. that this provision is of a non-mandatory nature, allowing parties to deviate, except for the definitions and unless the legislative text provides otherwise. As I already indicated, the numerus clausus doctrine is inherently linked with the concept of ownership.

It contains not only that the number and content of property rights is limited, but it also contains a limitation regarding the object of the right as well as the subject. There can only be one subject and not several, except in situations of, for example, co-ownership in which full ownership is shared. The policy choice behind the Civil Law numerus clausus doctrine is to prevent fragmentation of ownership. This becomes clear when looking at the definition of ownership in, for example, the new Belgian Civil Code. In article 3:50 ownership is defined as the most complete right, given to a legal subject (the "owner") directly, to use, benefit and alienate the object of such right, however as limited by legislation and the rights of third parties. The French version of article 3:50 new Belgian Civil Code reads: "Le droit de propriété confère directement au propriétaire le droit d'user de ce qui fait l'objet de son droit, d'en avoir la jouissance et d'en disposer. Le propriétaire a la plénitude des prérogatives, sous réserve des restrictions imposées par les lois, les règlements ou par les droits de tiers."

What objects can be is defined in a rather indirect and somewhat complicated way; an expression of today's uncertainties as to what may constitute an object of property law. First of all, a distinction is made between legal objects and legal subjects. According to article 3:38 things (in French: "choses") must be distinguished from animals, objects and animals must be distinguished from persons. Article 3:40 states that things ("choses") can be material and immaterial, to which article 3:41 adds that objects (in French: "biens") in their widest sense can be anything that can be appropriated, including patrimonial rights.

Article 3:39 makes clear that animals, although having a protected legal status, are not things.

Furthermore, the new code distinguishes public property ("biens publics") from private property ("biens privés") as separate legal objects by stating in article 3:45 that public property belongs to the private domain, unless meant to be used in the public domain. A reference to who can be the owner of public property has deliberately not been given. This does not necessarily have to be a public legal person[32].

The Explanatory Memorandum further clarifies that the legislator was guided by the

[31] The text of Book 3 new Belgian Civil Code, containing the new law of property can be found at http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2020020416&tabl e_name=wet (Dutch version), http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=202002041 6&table_name=loi (French version) accessed 16 July 2020. The new law will enter into force on 1 September 2021.

[32] Wetsontwerp houdende invoeging van Boek 3 "Goederen" in het nieuw Burgerlijk Wetboek/Projet de Loi portant insertion du Livre 3 "Les biens" dans le nouveau Code civil, Belgische Kamer van Volksvertegenwoordigers/Chambre de Représentants de Belgique, 31 October 2018, Doc 54 3348/001, 111. The full legislative file can be found under number 55K0173.

need to follow technical evolution and scientific progress combined with pragmatism[33].

Still, from the perspective of the question whether data can be owned, the new provisions do not result in an obvious reply. If personal data are considered to be part of someone's personality, does article 3:38 then prevent the conclusion that data can be owned, even though the new Belgian Civil Code shows a very open, flexible and pragmatic approach as to what can be an object of ownership? Furthermore, defining ownership following the classical triangle "usus, fructus, abusus", qualified by a classical description of what can constitute a legal object, counterbalances the open numerus clausus approach. The new code does not really tell us whether ownership also could mean access, portability, transfer and erasure of data. The new legal framework could result in two completely contradictory approaches, depending upon how the judiciary would relatively value the classical definition of ownership in light of the explicitly open policy regarding the numerus clausus. It could mean that the content of what ownership is in fact results in undoing the flexibility earlier created regarding the numerus clausus doctrine. It could, however, also mean that the openness of the numerus clausus approach must have its beneficial impact also on the content of the right of ownership. As far as I can see, there is no clear answer yet. All of this shows how difficult it is for a legislator, bound – even with the awareness that flexibility is badly needed – by the format of setting rules, to create rules providing workable answers for our fast developing hybrid society. It also raises the question whether perhaps in the area of data ownership case law should be preferred.

A look at the Common Law will immediately show that, if a property law system is primarily caselaw based, it becomes very complicated, depending on a myriad of cases functioning against a plethora of separate statutes. Answers to fundamental questions might take a very long time after a period of conflicting decisions and ensuing uncertainty. To avoid such overcomplication, an overall legislative framework seems unavoidable. The question, however, is how to formulate such a framework. The Common Law might not provide an adequate solution from a formal point of view, but it does provide possible answers from a substantive viewpoint. In the Common Law, no unifying and overall concept of "property" and "ownership" exists. The law is object dependent, and a distinction must be made as to land and personal property (next to, of course, intellectual property). In land law, at least in theory, ownership can only exist at the level of the Crown, but generally speaking rights in land are "held" by a subject. This is the direct result of the historical foundations of this part of the Common Law in feudalism, not unlike as can be found on the Continent of Europe before the French Revolution. Another layer, on top of this feudal origins, has been created by the development of Equity, which supplements the older established common law in a strict sense. Since 1925, according to Section 1 of the Law of Property Act 1925, in England & Wales, the common law estates in land are freehold and leasehold, next to which equity has created its own rights in land. The prime example of the coming together of common law and equity, of course, being the trust[34].

Also with regard to personal property, no unitary concept of ownership is recognised,

[33] Wetsontwerp houdende invoeging van Boek 3 "Goederen" in het nieuw Burgerlijk Wetboek/Projet de Loi portant insertion du Livre 3 "Les biens" dans le nouveau Code civil, 102 and 104.

[34] Williem Loof, Of trustees and beneficial owners. An inquiry into the proprietary aspects of trusts and trust-like devices from a European private law perspective (Datawyse/Universitaire PersMaastricht, 2016), 54.

but "title". Title is relative, it expresses that the entitlement of one subject is stronger than that of another. What we see is an object driven property law with right holders who have entitlements with varying degrees of (in Hohfeldian terminology) rights, powers, privileges and immunities[35].

There can be several "owners" with differing rights, sometimes in competition with one another, not unlike in pre-French Revolutionary law was recognised in Continental legal systems with the acceptance of duplex dominium and in line with older French case law accepting that a different types of fragmented ownership remained in existence next to the concept of ownership in the French Civil Code. The latter again shows that a classical Civil Law approach in which only the legislator can create property rights is running the risk that it turns a property law system into a straightjacket, thwarting future legal development. In today's world, we do not need a conservative and counter-progressive attitude towards property law, but we want pragmatism and flexibility against a background of recognised values, policy choices, principles, notions and concepts, and ground rules. Values such as stability and predictability; policy choices such as protecting fundamental human rights and promoting the development of commerce; principles such as numerus clausus, transparency and hierarchy; notions and concepts of core property rights; and ground rules such as that no one can transfer more rights than you have and that older rights have priority over younger rights. From a substantive viewpoint, the Common Law offers such a pragmatic and flexible approach by its historic focus on the objects of property law and its acceptance of a variation of property rights, which can co-exist and be in competition at the same time. So how would a possible framework regarding data "ownership", meaning a right to access, portability, transfer and erasure, look like? Unbundling "ownership" as access management Each and every property law system will be confronted with the following four basic questions: (a) What is the nature of a property entitlement (what distinguishes property rights from rights against one or more specific persons), (b) who can be a subject of property law (a "legal" subject), (c) what can be an object of property law (a "legal" object) and, in light of the foregoing, (d) which property rights does a legal system recognise? To give a very straightforward reply to the question what the nature of property rights is, it can be said that a property right protects the right holder against claims by a relevant and considerable group of other subjects. This includes both the traditional Civil Law and Common Law systematisation. The Civil Law considers the distinction between personal rights and real rights as essential, whereby real rights are rights "erga omnes", i.e. against the whole world. This might sound very principled, but it is in fact highly theoretical, because most of the world is not really interested in the objects around a subject. What matters are the subjects in your direct or indirect vicinity, which comes much closer to the Common Law's less absolutist and more relative approach.

The questions asked above, although they can be distinguished, are closely connected. If we take as our starting point for analysing the right of ownership, then defining it as the maximum of power over a physical asset, it inevitably becomes crucial to know if an asset is physical or not to find out whether you are the owner (or not). If, on the contrary, we take the object as our point of departure, we could then look at who is involved as stakeholder and, considering the nature of the object and who the stakeholder are, consider any rights which the legal system may confer while accepting this object as a "legal" object and the relevant stakeholders as "legal" subjects. It is the latter, object based, approach which I

[35] Wesley Newcomb Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) 23 Yale L J 16.

would advocate regarding data or, to put it more precisely, at least regarding digital assets: a cluster of data sufficiently separate from other data to be considered an individual object to fulfil the leading property law principle of transparency, more particularly specificity, as it must be clear as to which object a property right exists. If a sufficiently described object is absent, claiming that a subject has "ownership" of such an object is meaningless and without any effect. The question "I own", demands a reply to the question: "What do you own?". In my view data on a mobile phone, created by a corona app, are sufficiently limited in size and content that they can be considered, and hence qualify, to be at least a digital asset and hence a possible object of property law. Regarding who can be legal subjects, we must look at the various categories of stakeholders, considering the interests which they represent. The most important stakeholder is, first and foremost, the person on whose mobile phone the app has been installed and activated. The data concern such a person directly and immediately. Other stakeholders are third persons having been close enough to an infected person that they are now running the risk of becoming ill themselves. Stakeholders are also health authorities who need to know about how the disease is spreading; otherwise, they cannot react in the interest of public health. Closely linked to national health authorities are health providers who must be aware of the fact that a particular person has been in contact with an infected person and, consequently, might also be ill. Finally, it could also be argued that, by accepting that health authorities are stakeholders and, therefore, entitled to some right in the data, this likewise applies to a national government in the interest of public health. Furthermore, the pharmaceutical industry should not be ignored. Without their research laboratories, production facilities and manufacturing capacity, no vaccine can be created and mass-produced. From that perspective, commercial interests at least to some degree run parallel to, although they are not equal to, public health interests.

The overview of stakeholders makes clear that an overall framework for a right creating a property entitlement in data, more specifically a digital asset, that is enforceable against a relevant and considerable group of third persons cannot be an absolute and exclusive right for only one stakeholder. The same conclusion must be drawn from the perspective of the object. The intangible, fluid, non-rivalrous nature of data brings with it that it can be copied easily without the original holder of the data losing his/her own set of data. Whenever data are becoming mixed, already because of the combination itself, several stakeholders may be involved. Some because they pool data (for example by together using an online platform), others because together they co-generate enhanced data (for example by analysing raw data sets with other data sets, thus creating value added data)[36].

Considering the above arguments about legal objects and legal subjects of a possible ownership right in data gathered by a coronavirus app, the entitlement itself cannot be absolute in the classical sense of the legal term as understood in the Civil Law tradition but must be relative in nature. We need to look at this from the perspective of each category of stakeholders. Let me, as the obvious example, focus on the person whose mobile phone collected data by using a coronavirus app, which, with the user's permission, were later sent to a central server which could be checked by other phone users who also installed such an app. Following a timeline, various types of interests in the data may be distinguished. At first, the interest is strictly personal, and the right attached can be full control over the data ("ownership"). After allowing the data to be transmitted to a central server, they become

[36] Nicholas Terry, 'Legal issues relating to data access, pooling and use` in Claudia Grossmann et al. (eds.), Clinical Data As the Basic Staple of Health Learning : Creating and Protecting a Public Good: Workshop Summary (National Academies Press 2010) 151.

nonpersonal and consequently, competing rights can be attached. The latter type of rights can be of two kinds: of a public or of a commercial character and in some cases of a mixed nature. Given the character of the object (intangible, a cluster of data, e-health data relevant for third parties and for public health authorities), a flexible and open approach as to the content of the right must be sought which must include a time factor. As long as the data are on the user's phone, only the user is "owner", allowing only the user access, portability, transfer and erasure. Afterwards, ownership is fragmented over relevant third parties, such as health authorities and health providers. This process of fragmentation, or in European law terminology: unbundling, demands a management structure of data "ownership" whereby it could be argued that at the end it all comes down to time management of access, because portability, transfer and erasure (including the desisting from control or processing of data) are essentially all different aspects of giving, not-giving or ending access, with degrees of access varying over time[37].

Access management based on unbundling of ownership not only is a legal but also a strategic tool and as such it can contribute to a balanced distribution and allocation of rights. Following that methodology is nothing new from the perspective of EU law. It is a frequently used instrument to open up markets and break monopolies. Examples can be found with regard to public transport (rail), gas and electricity markets and telecommunications[38].

The starting point for unbundling is that no one single stakeholder or market participant should have full control over data. This can be done by splitting up a market, services or service providers to create competition. Such unbundling can be done in several ways through legal, operational, informational and ownership unbundling. Legal and ownership unbundling can go hand in hand and is intended to divide control over several market participants. Operational unbundling implies splitting up operations over several independent legal entities, and informational unbundling implies making information accessible to other market participants. The latter approach can be found in recent policy papers by the European Commission to create European common data spaces and promote, perhaps even oblige, data sharing between business and governments, and among businesses[39].

One of these common data spaces should be in the area of health data. Such informational unbundling can be done by giving others than those who create data access. At the same time, by giving access also ownership unbundling has been achieved. However, a clear and workable legal framework regarding time management of access rights must then be in place.

[37] For a further elaboration of my views regarding management as data ownership see Sjef van Erp, 'Management as Ownership of Data' in: Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), Data as Counter-Performance: Contract Law 2.0? (Hart/Nomos 2020).

[38] For public transport see the "Fourth railway package": https://ec.europa.eu/transport/modes/rail/packages/2013_en, for gas and electricity see the so-called "Third energy package": https://ec.europa.eu/energy/topics/markets-andconsumers/ market-legislation/third-energy-package_en and for telecommunications see https://ec.europa.eu/competition/sectors/telecommunications/overview_en.html accessed 16 July 2020.

[39] See the Communication Towards a common European data space ({SWD(2018) 125 final}, COM(2018) 232 final) and the Communication A European strategy for data (COM(2020) 66 final).

Concluding remarks

We must turn away from a negative approach towards data "ownership". Instead, we should start thinking about how to protect rights in data from the perspective of all those having personal, public or commercial interests. The law would then again become a realistic tool in a fair and equitable allocation of rights in data. By taking the model of ownership unbundling as part of a wider effort towards distributing data ownership rights over the various stakeholders, we can build a clear and workable framework within which data can be created and processed.

With regard to data gathered by the use of coronavirus apps, it is evident that the subject whose mobile phone is collecting contact data by using Bluetooth technology must be seen as originator of the data and therefore the prime person entitled to access, transfer, portability and erasure. However, it should not be forgotten that the purpose for which the data are gathered is of a public health nature. When analysing who could also be entitled to the gathered data we must take into account (a) all interests (private, public, commercial) involved, (b) the nature (personal or non-personal) of the collected data, (c) the purpose for which these data are collected (protecting public health) and how these purposes fit within both (d) the rule of law protecting our privacy and (e) our market-based economies. Finally, we should not deny the crucial role which governments have to play when societies become socially and economically disrupted because of a pandemic as we experience today. In such a situation, markets might fail and begin to disfunction (for example because of hoarding) and academic researchers, together with the pharmaceutical industry, will have to find adequate solutions at the shortest possible notice. It is then in the interest of all that governments through their health authorities become an important stakeholder in the data collected by tracing (and/or tracking) apps. From that perspective it can be argued that such data are a "national asset" and that digital sovereignty not only means that an individual should have control over its "own" data but that also the state claims sovereignty over such data. That could, as an utter consequence, result in an approach under which the state would be allowed to "expropriate" collected data in the general interest, subjects being safeguarded against unjust interference with their data through the general principles governing expropriation. Such expropriation could take place against individual citizens but also against anyone else having access to data, including commercial parties. Forced sharing of data, as discussed in EU documents, might prevent such a situation.

We urgently need a Data Act with a positive approach towards "ownership" of data, laying down clear rules on access management, portability, transfer and erasure, protecting individual's personal data, but also structuring the development of data markets and laying the foundations to justify state interference and consequently a state's right to obtaining data access in the interest of public health. This Data Act must also provide a solid framework for a fair and equal allocation of data. That framework should, however, be flexible, accepting that "ownership" of data is not the same as ownership of physical assets, that several subjects can have differing rights in data, varying over time and that such rights may coincide. A classical 19th century, post-French Revolutionary, property law approach will not work anymore. The Civil Law will need a return to a fragmented notion of ownership in line with the Common Law[40].

[40] Cf. also Sjef van Erp, 'Fluidity of ownership and the tragedy of hierarchy. A sign of a revolutionary evolution?', (2015) 4 European Prop L J 56.

ROMA TRE
UNIVERSITÀ DEGLI STUDI

The volume presents the results of a research project (named "Legafight") funded by the Luxembourg *Fond National de la Recherche* in order to verify if and how digital tracing applications could be implemented in the Grand-Duchy in order to counter and abate the Covid-19 pandemic. This inevitably brought to a deep comparative overview of the various existing various models, starting from that of the European Union and those put into practice by Belgium, France, Germany and Italy, with attention also to some Anglo-Saxon approaches (the UK and Australia). Not surprisingly the main issue which had to be tackled was that of the protection of the personal data collected through the tracing applications, their use by public health authorities and the trust laid in tracing procedures by citizens. Over the last 18 months tracing apps have registered a rise, a fall, and a sudden rebirth as mediums devoted not so much to collect data, but rather to distribute real time information which should allow informed decisions and be used as repositories of health certifications.

Elise Poillot is Full Professor of Civil Law in the University of Luxembourg and has written extensively in the fields of Consumer law and comparative European law. She has spearheaded pan-European research on clinical legal teaching.

Gabriele Lenzini is the Head of the Interdisciplinary Research group in Sociotechnical Cybersecurity (IRiSC) at SnT, University of Luxembourg and is extensively engaged in the modelling, analysis, and design of secure and trustworthy computing systems.

Giorgio Resta is Full Professor of Comparative Law in the Roma Tre University and is the author of numerous books and articles in the field of personality rights. He has recently co-edited an ample commentary to the GDPR, published by Giuffré - Francis Lefebvre.

Vincenzo Zeno-Zencovich is Full Professor of Comparative Law in the Roma Tre University and is author or editor of over twenty volumes devoted to legal issues of ICT, data protection, and media.

RomaTrE-Press
2021