‘I’m right behind you’: Digital contact tracing under European law

Vera Lúcia Raposo

Abstract
The features of the coronavirus disease 2019 (COVID-19) pandemic demand a new form of contact tracing performed by digital means: digital contact tracing. However, this mechanism raises several issues in light of relevant European regulations, particularly in terms of personal data protection and privacy. The challenge is to have a digital contact tracing model that efficiently and speedily alerts people to potential infection, so they can get tested and isolated as necessary, but that also complies with European legal standards. This paper will address two main issues. First, it will analyse digital contact tracing and its different features from the perspective of data protection and privacy, seemingly the main concern in this domain. Secondly, the paper will analyse the loopholes and benefits of digital contact tracing in the European context, focusing on the tension between privacy, individual liberties and public health to address its legitimacy.

Keywords
COVID-19, digital contact tracing, General Data Protection Regulation, public health, health data

1. Introduction
On 11 March 2020, the World Health Organization (WHO) declared the coronavirus disease 2019 (COVID-19) a pandemic. This highly contagious disease, caused by a new coronavirus, poses various challenges for health authorities. First,
The virus can spread from an infected person’s mouth or nose in small liquid particles when they cough, sneeze, speak, sing or breathe heavily. These liquid particles are of different sizes, ranging from larger ‘respiratory droplets’ to smaller ‘aerosols’.\(^2\)

Second, symptoms may appear some time after infection takes place,\(^3\) allowing infected people to pass the virus on without even knowing that they are infected.\(^4\) Therefore, the best way to restrict the progression of the virus is by avoiding close personal contact, especially with infected people (although some infected people may be asymptomatic). As soon as someone has tested positive, they should inform everyone with whom they have recently been in contact, allowing them to swiftly seek a test and isolate if necessary. This can break the chain of infection.\(^5\)

The use of contact tracing to combat serious infectious diseases is not new. However, it has usually been done manually through interviews with infected people to identify others with whom they have been in contact. This method has some limitations, especially with infectious diseases that can be transmitted in the pre-symptomatic stage.\(^6\) Patients may not remember or be able to identify everyone with whom they have been in contact, especially as some are likely to be complete strangers (for example, people who took the same bus or visited the same shop).\(^7\) Moreover, the number of trained officials required to perform contact tracing for COVID-19 would be prohibitively high given the increasing number of infected individuals.\(^8\) Even with enough staff, the process would simply be too slow to be efficient.\(^9\) These obstacles can be surpassed using digital contact tracing (DCT);\(^10\) that is, contract tracing performed using digital tools.\(^11\)

---

2. World Health Organization, ‘Coronavirus Disease (COVID-19): How Is it Transmitted?’, 9 July 2020, www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-how-is-covid-19-transmitted.
3. C. Ross, ‘Hospitals Turn to Remote Monitoring Tools to Free Up Beds for the Sickest Coronavirus Patients’, StatNews, 25 March 2020, www.statnews.com/2020/03/25/coronavirus-hospitals-weigh-remote-patient-monitoring-tools/.
4. R. Li et al., ‘Substantial Undocumented Infection Facilitates the Rapid Dissemination of Novel Coronavirus (SARS-CoV2)’, 368 Science (2020), p. 491 claim: ‘Nationwide [the authors refer to China] the number of infections during 10–23 January was 16,829 (95% CI: 3797–30,271), with 86.2% (95% CI: 81.6–89.8%) originating from undocumented cases.’
5. M. Casey et al., ‘Pre-symptomatic Transmission of SARS-CoV-2 Infection: A Secondary Analysis Using Published Data’, medRxiv 2020.05.08.20094870 (2020), https://doi.org/10.1101/2020.05.08.20094870; J. Hellewell et al., ‘Feasibility of Controlling COVID-19 Outbreaks by Isolation of Cases and Contacts’, 8 The Lancet Global Health (2020), p. E488.
6. Ferretti et al. state that about 40% to 50% of infections with the new coronavirus happen before the first symptoms appear, Ferretti et al., ‘Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing’, 368 Science (2020), https://doi.org/10.1126/science.abb6936. See also S. Jacob and J. Lawarée, ‘The Adoption of Contact Tracing Applications of COVID-19 by European Governments’, 4 Policy Design and Practice (2021), p. 44.
7. M.M. Mello and C.J. Wang, ‘Ethics and Governance for Digital Disease Surveillance’, 368 Science (2020), p.954.
8. Ibid., p. 954.
9. Ferretti et al., 368 Science (2020), p. 6.
10. The idea of contact tracing is not unknown in European law. See Article 3(a) of Decision n. 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 n. 2119/98/EC Text with EEA relevance (the so-called Health Threats Decision), which provides a definition of contact tracing as an operative concept in EU law: “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, and who are in danger of developing or have developed a disease.’ For details of this decision, see P. Dąbrowska-Klosińska, ‘Tracing Individuals under the EU Regime on Serious, Cross-border Health Threats: An Appraisal of the System of Personal Data Protection’, 8 European Journal of Risk Regulation (2017), p. 700.
11. Ferretti et al., 368 Science (2020), p. 4; L. Du, V.L. Raposo and M. Wang, ‘Correction: COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the Gap for International Pandemic Control’, 8 JMIR Mhealth and Uhealth (2020), p. e23194; R. Rubin, ‘Building an “Army of Disease Detectives” to Trace COVID-19 Contacts’ 323 JAMA...
The paper will analyse DCT from the perspective of data protection and privacy, considering the European regulations in this domain, mostly the General Data Protection Regulation (GDPR), the most important data protection regulation in the European Union (EU). The discussion will be supported by references to the apps developed by several European countries. To date – July 2022 – of the group of 27 Member States, 22 states have adopted a contact tracing app, even though many (Austria, Cyprus, Czechia, Denmark, Finland, Hungary, Malta, Poland) have discontinued it meanwhile. Two of them (Greece and Slovakia) are in the process of doing it and one other (Romania) is exploring this possibility. Only three countries (Bulgaria, Luxembourg and Sweden) have no plans in this regard. The majority of these apps present several common features: they work on both operating systems – Android and iOS – using Bluetooth technology with low energy consumption (Bluetooth Low Energy, BLE), based on the Application Programming Interface (API) developed by the Google-Apple partnership (Google-Apple Exposure Notification – GAEN).

Simultaneously, the paper will analyse the challenges posed by DCT in light of other legal norms (apart from the ones on data protection) applicable in the EU. It will focus on the tension between privacy, individual liberties and public health, aiming to clarify if any of these vortices has enough power to subdue the others.

The paper has two main targets, the second being a consequence of the first: (1) to analyse the different features of DCT in light of EU law; (2) based on that analysis, to recommend the more suitable features for contact tracing apps in light of EU law.

2. Different models of DCT in light of European law

A. What kind of data to use: Personal data or aggregated data?

Aggregated data are compiled or summarized individual data, typically used to identify trends, report statistics or conduct comparative studies. ‘Aggregation implies that variation at the individual.
level is lost’, 16 that is, that data are anonymized,17 as the individuals concerned cannot be identified. A DCT app using purely anonymized data would fall outside the scope of the GDPR, which protects only personal data, as stated in Article 2 of the GDPR. However, if these originally anonymized data were to become identifiable (which might happen),18 the protection provided by the GDPR would be reinstated.19

The European Data Protection Board (EDPB)20 has a clear preference for the use of aggregated data:

[p]ublic authorities should first seek to process location data in an anonymous way (i.e., processing data aggregated in a way that individuals cannot be re-identified), which could enable the generation of reports on the concentration of mobile devices at a certain location (‘cartography’).21

Nonetheless, it is nearly impossible to perform DCT only with aggregated data, that is, anonymous data.22 Moreover, there is no guarantee that anonymization is irreversible. Artificial intelligence might offer a way to identify the data subject.23 Thus, not even the use of aggregated data would solve all data protection issues.

Whenever personal data are involved regulations on data protection must intervene. DCT raises issues in light of the GDPR24 because it processes personal data; that is, ‘information relating to an identified or identifiable natural person’ (Article 4(1) of the GDPR). DCT may involve the processing of location data, which can be considered personal data according to the definition provided in Article 4(1) of the GDPR, which expressly refers to location.25

16. G. Pawitan and D.G. Stee, ‘Exploring a Relationship Between Aggregate and Individual Levels Spatial Data Through Semivariogram Models’, 38 Geographical Analysis (2006), p. 310.
17. Anonymized data are data that cannot be linked to an identified or identifiable person or persons through reasonable effort (reasonable in both objective and subjective terms). For details of anonymization techniques in light of the GDPR, see S.Y. Esayas, ‘The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the “All or Nothing” Approach’, 6 European Journal of Law and Technology (2015), https://pdfs.semanticscholar.org/10ad/477010c69308daad00fe7f7b6bbf849457dd.pdf.
18. We know now that even alleged anonymization can be reversed, leading one to question if there is such a thing as true anonymization. See L. Rocher, J.M. Hendrickx and Y.A. de Montjoye, ‘Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models’ 10 Nature Communications (2019), p. 3069.
19. D. Van Der Eycken, ‘Europe’s Plan for Contact Tracing Apps Against COVID-19’, KU Leuven (2020), www.law.kuleuven.be/citip/blog/europes-plan-for-contact-tracing-apps-against-covid-19/.
20. European Data Protection Board, ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’, 21 April 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en, para. 10, 11, 13, 28, 29, 32, 33, 44.
21. European Data Protection Board, ‘Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak’, adopted on 19 March 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf, p. 2.
22. D. Van Der Eycken, ‘Europe’s Plan’.
23. L. Rocher, J. Hendrickx and Y.-A. de Montjoye, 10 Nature Communications (2019), p. 3069.
24. On the general scope of the GDPR, see P. Voigt and A. Von Dem Bussche, The EU General Data Protection Regulation (Springer, 2017), p. 9. Note that the GDPR does not apply to matters of public security (Recital 16, GDPR), and it might be stated that a pandemic is one of such matters (I. Genna, ‘EU Privacy and Data Protection in the Age of the Coronavirus’, IBA (2020), www.ibanet.org/Article/NewDetail.aspx?ArticleUid=115b6b76-ce62-4be0-a67c-73252ec82f2c.
25. Cf. M. Finck and F. Pallas, ‘They Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR’, 10 International Data Privacy Law (2020), p. 11.
B. Should the app be mandatory or voluntary?

1. A legal ground for DCT under the GDPR. Under European law, the decision on whether the app should be mandatory or voluntary depends on the selected legal ground for data processing. The GDPR allows for the processing of personal data in some circumstances, set in Article 6(1). First of all, when ‘the data subject has given consent to the processing of his or her personal data for one or more specific purposes’ (Article 6(1)(a) of the GDPR), based on the information to be provided under Articles 13 and 14 of the GDPR. Other legal ground can be found in Article 6(1)(c) (‘processing is necessary for compliance with a legal obligation to which the controller is subject’), based on the understanding that Member States are obliged to prevent and combat cross-border health threats in light of the Health Threats Decision, a milestone in the EU for preventing and combatting public health emergencies. Article 6(1)(d) (‘processing is necessary in order to protect the vital interests of the data subject or of another natural person’) has also been invoked as a possible legal ground on the assumption that DCT is necessary to protect infected individuals and provide them with speedy care and information. A different legal ground for data processing can be found in Article 6(1)(e) of the GDPR: when data processing is ‘necessary for the performance of a task carried out in the public interest’. If this is the legal ground for DCT, the basis for the processing must be established either by EU law or by national Member States (Article 6(3) of the GDPR).

If the legal ground is found in Articles 6(1)(c) or 6(1)(e) of the GDPR, an additional requirement is demanded: an EU law or national law to act as a legal base for the data processing. The law in question must provide for adequate safeguards of privacy, taking into account the impositions of the GDPR, such as the duty to provide all relevant information to the data subject, limitations on the number and type of data collected and stored, and definitions of responsibilities.

If Article 6(1)(a) of the GDPR is not used as the legal basis to implement DCT, consent is not necessary. Nevertheless, consent might still be required. Both the European Commission and the EDPB argued that consent should be sought, even if consent is not the selected legal ground.

Even more problematically, DCT involves data concerning health (as defined in Article 4(15) of the GDPR), a particularly sensitive type of personal data, whose processing is generally

26. See also Article 4(11), Article 7 and Article 9(2)(a) GDPR.
27. Cf. P. Dąbrowska-Kłosinska, 8 European Journal of Risk Regulation (2017), p. 708.
28. Meanwhile, there is a Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, 11.11.2020 COM(2020) 727 final 2020/0322 (COD).
29. P. Dąbrowska-Kłosinska, 8 European Journal of Risk Regulation (2017), p. 708.
30. Therefore, the fact that the app requires a user’s consent does not mean that consent is the legal ground for data processing.
31. European Commission, Commission Recommendation of 8.4.2020 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) 2296 final (2020), https://ec.europa.eu/info/sites/info/files/recollection_on_apps_for_contact_tracing_4.pdf, recitals 7, 10 and 14.; European Commission, ‘Communication from the Commission Guidance on Apps Supporting the Fight Against COVID 19 Pandemic in Relation to Data Protection’, 2020/C 124 1/01, C/2020/2523, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29, para. 3.2.
32. European Data Protection Board, ‘Guidelines 04/2020’, para. 10, 11, 13, 28, 29, 32, 33, 44.
33. According to the Court of Justice of the European Union (CJEU), in Case C-101/01 Criminal proceedings against Bodil Lindqvist, ECLI:EU:C:2003:596, para. 50, the expression ‘data concerning health’ must have a broad interpretation ‘so as to include information concerning all aspects, both physical and mental, of the health of an individual’ (the Court was referring to the previous Directive on Data protection, but the same is valid for the GDPR).
forbidden under Article 9(1) of the GDPR. This ban can be waived under certain circumstances, but special protection for data concerning health is still required (Recital 53 of the GDPR). The processing of health-related data is permitted with the specific consent of the data subject (Article 9(2)(a) of the GDPR). It is also allowed when ‘processing is necessary for reasons of substantial public interest’ (Article 9(2)(g) of the GDPR), ‘necessary for the purposes of preventive or occupational medicine’ (Article 9(2)(h) of the GDPR) or ‘necessary for reasons of public interest in the area of public health’ (Article 9(2)(i) of the GDPR). The COVID-19 pandemic clearly fulfils at least one of these conditions, especially the last one, which seems the most suitable legal ground for a pandemic scenario.35

2. The position of EU institutions. Both the guidelines developed by the EDPB36 and the communications from the European Commission37 state that DCT should be voluntary.38 The Commission clarifies that not only the downloading of the app but also the use of its different functionalities should depend on the data subject’s consent: ‘[t]he installation of an app on a user’s device should be voluntary; a user should be able to give their consent to each functionality of an app separately.’39 The action of downloading the app must be distinguished from the action of having the data processed.40 Whereas downloading the app requires previous consent, the subsequent processing of data might be based on personal consent or on any of the remaining legal grounds applicable to the situation, as established in Article 6 of the GDPR.

Even if data processing ends up being grounded on a different legal basis from Article 6(1)(a) of the GDPR, this does not mean that the data subject has no say in the process. Consent can still be required, even if this is not the legal ground for data processing. In addition, the exclusion of consent does not exclude other rights, such as the right to be provided with information (Article 13 of the GDPR), the right to access the data (Article 15 of the GDPR), the right to rectification (Article 16 of the GDPR), the right to be forgotten once the data processed are no longer necessary (Article 17 of the GDPR), the right to restriction of processing (Article 18 of the GDPR) and other rights provided by the GDPR.

3. Effectiveness of voluntary apps. Basing DCT on consent raises two issues: one concerning effectiveness (a strict requirement of voluntariness might jeopardize the purpose of the app) and

---

34. These three legal grounds for processing must have a basis in EU or national law. In Article 9(2)(h) of the GDPR this basis can also be a contract with a healthcare professional.
35. Cf. V.L. Raposo, ‘Que a Tecnologia Esteja Conosco Nestes Tempos de COVID-19 (Legitimidade da STAYAWAY COVID no Ordenamento Jurídico Português)’, 164 Revista do Ministério Público (2020), p. 9. Analysing the possible legal grounds for DCT, V. Dias et al., ‘Avaliação de Impacto sobre a Protecção de Dados do Sistema Stayaway Covid’, Porto (2020), https://stayawaycovid.pt/wp-content/uploads/AIPD_STAYAWAY_v2.0_11_08_2020.pdf, p. 35.
36. About the voluntary nature of DCT, European Data Protection Board, ‘Guidelines 04/2020’.
37. European Commission, ‘Coronavirus: Guidance to Ensure Full Data Protection Standards of Apps Fighting the Pandemic’, Press Release, European Commission, 16 April 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_669; European Commission, ‘Communication from the Commission’, para. 3.2.
38. Also underlying the voluntariness of all aspects of DCT (carrying a smartphone, downloading the app, reacting to the app alerts, sharing data), see A. Dubov and S. Shoptaw, ‘The Value and Ethics of Using Technology to Contain the COVID-19 Epidemic’, 20 The American Journal of Bioethics (2020), p.W7; I.G. Cohen, L.O. Gostin and D.J. Weitzner, ‘Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension’, 323 JAMA (2020), p. 2371. Sustaining mandatory DCT in some situations (namely international travelling): L. Du, V.L. Raposo and M. Wang, 8 JMIR Mhealth and Uhealth (2020) , p. e23194.
39. European Commission, ‘Coronavirus’, para. 3.2.
40. D. Van Der Eycken, ‘Europe’s Plan’.
the other concerning the relative importance of different values (should data protection and privacy prevail over public health?). 41

A decisive criterion to consider when deciding if the app should be mandatory or voluntary is its effectiveness, which, in turn, depends on the threshold of effectiveness, that is, how many people will have to use the app to achieve positive results. The first approach to this question claimed that effective results could only be achieved with a substantial number of users. A study by the University of Oxford pointed to 60% population coverage, which so far has not happened in Europe (in fact, nowhere in the world). Nowadays, however, this objection is greatly weakened. First, it became clear that different studies came to different conclusions. For instance, Abueg et al. concluded that DCT apps present positive results even with low percentages of adherence: it is enough for 15% of the population to use the app to reduce mortality by 6% and infections by 8%. This conclusion is reinforced by examples of positive outcomes reached in countries with lower usage percentages. Secondly, because eventually the authors of the Oxford study came to clarify their conclusions, stating that even a small percentage of users allows beneficial results:

Even with lower numbers of app users, we still estimate a reduction in the number of coronavirus cases and deaths [...] If you have 10% of people using the app, then the chance of contact between two people being detected is 10% of 10%, which is 1% — a tiny fraction. What we found in the simulation was that that actually isn’t the case. We’ve been working to understand why we actually see benefits of usage accruing. 46

A possible solution would be to keep DCT voluntary but make the use of the app a precondition to benefitting from several services in everyday life. For instance, only people using the app could be allowed to access cinemas, restaurants or taxi services. Ultimately, using the app could even be a condition to receive medical care. However, such false voluntariness is not a desirable solution, and the European Commission states that refusing to participate in DCT cannot carry any negative consequences for the individual. 48

41. On this issue see E. Seto, P. Challa, and P. Ware, ‘Adoption of COVID-19 Contact Tracing Apps: A Balance Between Privacy and Effectiveness’, 23(3), Journal of Medical Internet Research (2021), p. e25726.
42. University of Oxford, ‘Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us Out of Lockdown’ (2020), www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.
43. Germany reported 14.4% adherence, Italy 7.2%, France 3.1% (S. Chan, ‘COVID-19 Contact Tracing Apps Reach 9% Adoption in Most Populous Countries’, Sensor Tower (2020), https://sensortower.com/blog/contact-tracing-app-adoption).
44. M. Abueg et al., ‘Modeling the Effect of Exposure Notification and Non-pharmaceutical Interventions on COVID-19 Transmission in Washington State’, 4 npj Digital Medicine (2021), https://doi.org/10.1038/s41746-021-00422-7.
45. A review of the percentages of adoption of EU in several EU countries and the results reached by each of them in A. Blasimme, A. Ferretti and E. Vayen, ‘Digital Contact Tracing Against COVID-19 in Europe: Current Features and Ongoing Developments’, Frontiers in Digital Health (2021), https://doi.org/10.3389/fdgh.2021.660823.
46. P.H. O’Neill, ‘No, Coronavirus Apps don’t Need 60% Adoption to Be Effective’, MIT Technology Review (2020), www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.
47. For instance, China’s ‘health code’ system is not mandatory in theory, but it is in practice, as without a health code, citizens can hardly go on with their daily lives (R. Zhong, ‘China’s Virus Apps May Outlast the Outbreak, Stirring Privacy Fears’, The New York Times, May 26 2020, www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html).
48. European Commission, ‘Communication from the Commission’, para. 3.2.
4. **The opt-out model.** A way to ensure that DCT complies with consent requirements but effectively achieves public health purposes is to use an opt-out model\(^{49}\) (whereby the app is downloaded by default and those who oppose it must express their opposition)\(^{50}\) instead of an opt-in model (whereby the user has to download the app, as proposed by the Commission).

The opt-out model would increase efficiency by ‘encouraging’ people to use the app, as this does not come naturally, and people tend to go along with what already exists by default. Mello and Wang offer the example of Singapore:\(^{51}\) although its population meets all the requisites for widespread use of the app (a population with informatic literacy whose members are accustomed to public intrusions into private life), only 20% of Singaporean smartphone users have downloaded the app.\(^{52}\)

The problem is that the opt-out model is excluded by the GDPR whenever consent is the legal basis for data processing (Articles 6(1)(a) and 9(2)(a) of the GDPR). When that is the case the subject’s consent must comply with very strict requisites. Recital 32 of the GDPR clearly states that consent must be unambiguous; that is, an affirmative action on the part of the data subject is required. As expressly stated by this recital, ‘[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent’.

Therefore, the legal basis for this specific data processing should not be consent, in line with what has been suggested by the EU. Assuming a different legal basis is selected, consent can (and should) be asked but it won’t be subject to such demanding requirements. In particular, it will allow the opt-out model and a more flexible solution in case of withdrawal, excluding the requirements of Articles 7(3) and 17(1)(b) of the GDPR.\(^{53}\)

**C. How should the app operate?**

The operating mode of digital contact tracing apps can vary a lot in regard to the type of technology used (GPS or Bluetooth), the data collected (location or proximity) and the roles of central sources and individual devices (centralized or decentralized). The option between these features must comply with the general data protection principles, listed in Article 5 of the GDPR.\(^{54}\)

1. **The principles of the GDPR.** The first set of principles comprises lawfulness, fairness and transparency (Article 5(1)(a) of the GDPR). Lawfulness requires data processing to be performed based on

---

49. Mello and Wang are in favour of the opt-out solution because it ‘is the least restrictive alternative’ (M.M. Mello and C.J., Wang, 368 Science (2020), p. 954). See also D. Castro and E. Chivot, ‘Turn Contact Tracing Apps on by Default—Europeans Shouldn’t Need to Opt In’, IAPP (2020), https://iapp.org/news/a/turn-contact-tracing-apps-on-by-default-europeans-shouldnt-need-to-opt-in/.

50. ‘Downloaded by default’ means that no one gives the order to download, it happens automatically when some other event (for instance, an update in the operating system) triggers the download, even though the user of the device can subsequently delete the app.

51. Singapore has the voluntary app Trace Together (www.tracetogether.gov.sg/).

52. M.M. Mello and C.J., Wang, 368 Science (2020), p. 954.

53. See L. Bradford, M. Aboy and K. Liddell, ‘COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes’, 7 Journal of Law and the Biosciences (2020), p. 1(aa034); V.L. Raposo, 164 Revista do Ministério Público (2020), p. 9.

54. European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (European Union, 2018), p.115. These are general principles of data protection, many of which are also stressed by the Council of Europe in its guidelines (Council of Europe, ‘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, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7).
one of the legal grounds specified in Article 6 of the GDPR. Fairness requires that data are collected in an unbiased way, not by tricking the data subject (that is, the app’s user). From the moment data are collected, the data subject must be fully aware of the purposes for which data will be used.

Transparency entails the provision of information to both the data subject and the public. In some situations, however, the data controller may be excepted from informing the data subject, as established in Article 14(5) of the GDPR. One such case is when it ‘proves impossible or would involve a disproportionate effort’ (Article 14(5)(b) of the GDPR) to provide such information. This exception might offer a seductive way to avoid complying with some of the requirements imposed by the GDPR. However, the former Article 29 Data Protection Working Party (Article 29 Working Party) clarified that the situation where it ‘proves impossible’ under Article 14(5)(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus, if a data controller seeks to rely on this exemption, it must demonstrate the factors that actually prevent it from providing the information in question to data subjects.55

Moreover, data processing must be done in a manner open to public scrutiny. For instance, the algorithms used by the app must be made public and frequently supervised to ensure accuracy.56 The developers of the Portuguese app StayAway Covid tried to be as transparent as possible: the source code and the data protection impact assessment were made public, the National Cybersecurity Centre participated in the code audit and a prior consultation with the supervisory authority was carried out.57

The principle of purpose limitation (Article 5(1)(b) of the GDPR) requires that data are used for a specific and clear purpose and prevented from being used for different purposes. The data controller must guarantee that the data will not be used (either during the pandemic or afterwards) by employers, insurance companies, immigration services, law enforcement or any other public or private entity to take actions harmful to the data subject. Ultimately, DCT could become a tool for mass surveillance in the hands of governments. A more commendable purpose of the use of data collected by DCT is scientific investigation, eventually to develop effective vaccines58 or a way to successfully treat COVID-19. Yet no matter how laudable this purpose may be, scientific investigation is not the aim of DCT. Researchers should only use the data for medical investigation under the requites outlined in the GDPR.59

The principle of data minimization (Article 5(1)(c) of the GDPR) involves several conditions. First, when possible, anonymized or pseudonymized data should be used.60 These two concepts must not be confused: it is impossible to identify an individual from anonymized data, but this is not true for pseudonymized data. Therefore, pseudonymized data are still ‘personal data’ in light of Article 4(1) of the GDPR, and thus remain under the rules of the GDPR (Recital 28 of the

---

55. Article 29 Working-Party, ‘Guidelines on Transparency under Regulation 2016/679’, adopted on 29 November 2017, as last revised and adopted on 11 April 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, para. 59.
56. A. Dubov and S. Shoptaw, The American Journal of Bioethics (2020), p. W7.
57. V.L. Raposo, 164 Revista do Ministério Público (2020), p. 9.
58. As far as we know, the data obtained by DCT were not used in the development of the existing vaccines.
59. The paper will not develop the issue of subsequent data uses related with research, but see E.S. Dove and J. Chen, ‘Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis’ 10 International Data Privacy Law (2020), p. 117.
60. On the processes of anonymization and pseudonymization, see R. Akerkar, ‘Privacy and Security in Data-Driven Urban Mobility’, in J. Darmont and S. Loudcher (eds), Utilizing Big Data Paradigms for Business Intelligence (Hershey, 2018), p. 113.
GDPR). Second, only data considered necessary for the envisaged goal can be used. Unnecessary information (for example, a person’s identity, usernames, passwords, marital status, full medical history and financial records) cannot be collected. Moreover, effective DCT does not require the locations of the app’s users, but merely proximity information. Third, measures should be taken to prevent a user from being identified by those who are notified. It has been argued that the only information communicated to an app user should be where and for how long the suspected contact took place, but even this might not be necessary; instead, we could have a model in which solely the existence of a suspected contact is communicated. In addition, the information should be kept on the user’s device (the decentralized model), and only shared with health authorities if the user tests positive for COVID-19. The information should not be shared with the app’s host or with any other third party.

The principle of accuracy (Article 5(1)(d) of the GDPR) is linked to the reliability of the data. To ensure that the data are correct (and thus that they lead to accurate public health decisions), control mechanisms must be put in place, not only to identify erroneous data but also to amend observed errors. Moreover, the principle of accuracy rests on the precision of the algorithm used, an aim that can only be achieved through constant monitoring by experts to avoid false positives or false negatives. Public trust, which is crucial to the success of DCT, relies on accuracy.

The principle of storage limitation (Article 5(1)(e) of the GDPR) requires that data are kept only for a certain period. Ultimately, the deadline to cease DCT and destroy the data that have been stored is established by the principle of necessity: when the pandemic is deemed controlled, DCT will no longer be necessary. The need for the DCT app to be exceptional is emphasized by both the EDPB and the European Commission. When the pandemic is deemed controlled, the current restrictions on privacy must be withdrawn, the DCT app must be deactivated (which the European Commission suggests should happen automatically, with no need for the user to uninstall the app) and the data collected by DCT must be destroyed without further use or at least anonymized. It should be defined in advance in which scenario the pandemic will be considered ‘controlled’ (a threshold of 60% for herd immunity, for example), and this is a decision that must be taken in light of existing epidemiological knowledge.

However, there might be valid reasons to keep the data. Parker et al. argue that these data may offer a valuable resource to protect future generations from harm in the event of, for instance, future pandemics. Indeed, Article 5(1)(b) of the GDPR states that some data may be stored for

61. Ibid., 106.
62. European Commission, ‘Communication from the Commission’, para. 3.2.
63. World Economic Forum, ‘Good Data Data-sharing, Public Trust and Willingness,’ Briefing Paper April 2021,://www3.weforum.org/docs/WEF_Good_Data_2021.pdf.
64. Cohen et al. suggest that the DCT app could be designed to automatically uninstall and erase all stored data (I.G. Cohen, L.O. Gostin and D.J. Weitzner, 323 JAMA (2020), p. 2371).
65. European Data Protection Board, ‘Guidelines 04/2020, para. 48; European Data Protection Board, ‘Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak’, p. 3.
66. European Commission, ‘Communication from the Commission’, para. 3.7.
67. Ibid., para. 3.2.
68. It should be defined beforehand which entity will be in charge of destroying them.
69. This threshold is given merely as an example to illustrate my thesis. For detail about the threshold for herd immunity, see V.L. Raposo, ‘What to Do in the Next Pandemic Outbreak: Natural Herd Immunity Versus Lockdown (Lessons Learned from Covid-19)’, 29 Journal of Law and Medicine (2022), p. 260.
70. M. Parker et al., ‘Ethics of Instantaneous Contact Tracing Using Mobile Phone Apps in the Control of the COVID-19 Pandemic’, 46 Journal of Medical Ethics (2020), p. 427.
specific purposes, that is, ‘archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’, following the safeguards stated in Article 89 of the GDPR, namely anonymization or pseudonymization. Public health is not among these purposes, but scientific research could be used as a justifying purpose.

The principles of integrity and confidentiality (Article 5(1)(f) of the GDPR, in connection with Article 32(1) of the GDPR) require appropriate security measures to be put in place, namely cryptographic techniques to prevent undue access (by employers, insurance companies or pharmaceutical companies, for example). Appropriate security measures must be put in place to guarantee security by default (continuous compliance with the highest security standards) and security by design (implementation of security measures from the very first moment of data processing)71 (Article 25 of the GDPR). The data anonymization process is not easy and even small details can reveal the person’s identity.72 If the level of cybersecurity is too low, the app becomes a danger in itself.73 For instance, in April last year, there was a data breach involving the Dutch app: the app source code was published online, which led to the exposure of 200 names, email addresses and passwords.74

The last of the data protection principles of Article 5 of the GDPR is the principle of accountability (Article 5(2) of the GDPR), according to which the data controller (public or private) and its role and responsibilities should be clearly defined. In this regard, the European Commission recommends that a public authority serves as the DCT data controller.75 Moreover, affected individuals should be provided with efficient judicial mechanisms to enforce their rights.

The features of this particular form of data processing led to the conclusion that it might pose a high risk to the rights and freedoms of natural persons. Features such as its implementation by new technologies, whose possible consequences and loopholes have not yet been properly identified, its use of especially sensitive data (health-related data), and its large-scale implementation raise concerns. Thus, it is necessary to perform a data protection impact assessment according to Article 35 of the GDPR.

2. Tracking proximity or location. Location data76 identify a target’s latitude and longitude at a specific time. Location information can be obtained from various sources, such as telecommunication companies, other companies that offer digital services (social networking sites, search engines)77 and specific apps that collect relevant data. Every time we use a mobile phone, we release location information.
data (otherwise the phone would not work): the phone connects to a cell tower, mapping our movements for the telephone company, with an accuracy level of a few hundred metres. Location can also be tracked using GPS, with a few metres’ accuracy. This method is very common among apps, both those that require location data to operate and those that do not require location information but still ask for it.78

The collection of proximity data or location data depends on the specific technology used by the app: GPS or Bluetooth. Bluetooth is a wireless technology for short-distance data exchange. An app performing DCT via Bluetooth collects not location data, but only data on users’ proximity to other app users and the time and duration of their contact. Users are identified by anonymized codes that can change periodically. If a person is identified as being infected, users who have been in close physical contact with him/her are tracked and receive a risk alert, so they can self-quarantine, get tested and eventually enter isolation if necessary.

In contrast, DCT using a satellite – that is, the Global Positioning System (GPS) – tracks the location of every user, and therefore collects information on people’s movements. A privacy breach would thus have much more serious consequences, as location can reveal a lot about a person.

Furthermore, Bluetooth and GPS contact tracing also differ in their accuracy.

Realistically, GPS accuracy ranges from 5 to 20 m in the open sky (whereas Covid-19 can spread within a 1-m distance).79 However, such accuracy is achieved only in the absence of obstacles, such as high buildings or thunderstorms, and GPS is barely functional indoors. Moreover, GPS contact tracing does not indicate whether, for example, two people are sitting on the same sofa or whether they are in different rooms, separated by a wall.

Bluetooth is the most precise technology,80 but even this model can lead to mistakes. For instance, it cannot determine whether a user is wearing personal protective equipment, which, if used, would reduce the risk of infection. Experts point out that trusting implicitly in the strength and duration of a Bluetooth signal can easily lead to false negatives81 or false

78. It is important to distinguish between DCT using data collected from providers of services related to the information society (namely apps that require these data to operate) and DCT using data collected by electronic communication service providers (mobile telecommunication operators), which in this case would be location data. In the latter case, DCT must comply with the ePrivacy Directive (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)). The Directive is currently being amended (Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, COM/2017/010 final – 2017/03 (COD)). About the compliance with the Directive see F. Boehm et al., ‘Tracking and Tracing Apps and Data Protection in the Content of the COVID-19 Pandemic: Data Protection Requirements and Recommendations for the Deployment of COVID-19 ‘Tracking and Tracing apps’ (FIZ Karlsruhe, 2020), www.fiz-karlsruhe.de/sites/default/files/FIZ/Dokumente/FIZnews/tracking_app_EN_20200428.pdf.

79. The ‘safe distance’ for COVID-19 is 2 metres, and even this may not be enough (R.C. Schroter, ‘Social Distancing for Covid-19: Is 2 Metres Far Enough?’ 369 British Medical Journal (2020), p. m2010). Some apps consider ‘close contact’ one metre distance (the StopCovid app, in France), while others opted for two metres (the StayAway Covid, in Portugal).

80. Privacy International, ‘Bluetooth Tracking and COVID-19: A Tech Primer’, Privacy International, 31 March 2020, https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer.

81. The false negatives come usually connected to the critic of a ‘false sense of security’ (L. Moerel, ‘Contact Tracing Apps: Why Tech Solutionism and Privacy by Design Are not Enough’, IAPP, (2020), https://iapp.org/news/a/contact-tracing-apps-why-tech-solutionism-and-privacy-by-design-are-not-enough/), an argument which could as easily be invoked to attack the use of masks, hand washing and even vaccination, because in the end they can all make us feel ‘falsely’ safe.
positives. Note, however, that the mere notification does not necessarily mean the person is infected and so the user should receive additional information on how to behave.

The main problem is that location data are never really anonymous. They can reveal a user’s religion (is the user in a mosque?), sexual orientation (is the user in a gay bar?) and political ideology (is the user in the headquarters of a right- or left-wing political party?). Thus, the EDPB recommends using an app that offers proximity alerts (for infected users) via Bluetooth but does not reveal the location. Proximity data merely reveals that the devices were close to each other, but not where they were.

3. Centralized or decentralized model?. In a centralized DCT system, information uploaded to the app is kept on a remote server (a central source operating as a single server) that receives information from the app’s users, matches this information and notifies the users of other devices in cases of infection. The central database gathers a great deal of information that may be misused, even by authorities, and may also, therefore, become an appealing target for hackers. ‘If the central server is compromised, the entire network is’. Thus, privacy is a relevant concern under this model.

In contrast, in the decentralized system, all information is kept on the user’s smartphone, which also notifies other devices in the event of infection without the intervention of a central server. The most common decentralized version of DCT relies on Bluetooth Low Energy technology. Let’s take the case of the Google-Apple API (application programming interface), which operates using a decentralized model. When two devices equipped with this technology come into proximity, they both emit and receive (and register) the so-called ephemeral identifiers (EphIDs). Thus, if an app user tests positive for COVID-19, his/her device will be able to show recently registered (within 14 days) EphIDs from other devices. This information will allow the identification of nearby devices and analysis of the potential level of infection risk. No central device receives the information; all devices play a similar role. The difference between the centralized and the decentralized model is not so much the existence of a centralized server, which exists also in some decentralized models, but where the main tasks of contract tracing (the generation of

82. A. Soltani, R. Calo and C. Bergstrom, ‘Contact-Tracing Apps Are not a Solution to the COVID-19 Crisis’, Tech Stream, (2020), www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.
83. Y.-A. de Montjoye et al., 3 Scientific Reports (2013), p. 1376. For instance, the DCT mechanism in place in South Korea involves the disclosure of an infected individual’s location such that it is possible to identify the person in question (H.E. Kim, ‘Coronavirus Privacy: Are South Korea’s Alerts too Revealing?’, BBC News Korean, (2020), www.bbc.com/news/world-asia-51733145). Location data are also used to track people’s movements in China, India, Israel and Iceland.
84. This information can, nonetheless, be misleading. Location data frequently fail to provide the exact location; thus, the user might be near one of these spots, but not exactly inside, and in that case the deduction made might be completely wrong.
85. On the drawbacks of Bluetooth technology, see Privacy International, ‘Bluetooth Tracking’.
86. European Data Protection Board, ‘Guidelines 04/2020’, para. 8, 27.
87. Adopted by Japan, Singapore, Australia, France and originally in the UK.
88. S. Rossello and P. Dewitte, ‘Anonymization by Decentralization? The Case of COVID-19 Contact Tracing App’, European Law Blog, 25 May 2020, https://europeancelawblog.eu/2020/05/25/anonymization-by-decentralization-the-case-of-covid-19-contact-tracing-apps/.
89. Google, API for Exposure Notifications, https://developers.google.com/android/exposure-notifications/exposure-notifications-api.
90. S. Rossello and P. Dewitte, ‘Anonymization by Decentralization?’.
unique identifiers, the calculation of the percentage of epidemiologic risks) are executed. These tasks can take place either in the central server or on each device.91

These features have important implications for data anonymity. The definition of data as anonymous depends on the understanding of this concept. The former Article 29 Working Party stated that for data to be considered anonymous, it must be impossible to reidentify the data subject.92 According to this definition, if there is a way, no matter how costly and difficult, to reverse the anonymization procedure, the data are not anonymous. However, this theory is not compatible with the wording of the GDPR93 or the case law of the CJEU,94 which do not require it to be absolutely impossible to reverse the anonymization; it is sufficient to demonstrate that this could not be done without making an excessive effort and/or using illegal means.95

In the centralized system described above, the end user may be identifiable.96 As information about an end user accumulates, it becomes easier to identify him/her.97 In other words, under the centralized system, there exists, at least in theory, the possibility of identifying and tracking a user. Data are not truly anonymous, merely pseudonymous.98

In contrast, in a decentralized system, all information is kept on users’ smartphones. Thus,

91. European Parliament, ‘National COVID-19 Contact Tracing Apps’, (2020), www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf. In fact, most of the so-called decentralized systems are actually semi-decentralized (Dias et al., (33)), since they still use a central server, but not for core tasks.

92. ‘Anonymisation results from processing personal data in order to irreversibly prevent identification’ (Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, p. 5).

93. Recital 26, GDPR: ‘To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.’

94. Judgement of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779, para. 46 (regarding Recital 26 of Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). See also M. Finck and F. Pallas, ‘10 International Data Privacy Law (2020), p. 18.

95. However, some national data protection authorities have a more demanding understanding and define anonymized data as the ones in which it is impossible, in practice, to identify the person. This is, for instance, the position of the CNIL, the French data protection authority (CNIL, L’Anonymisation de Données Personnelles, (2020), www.cnil.fr/fr/lanonymisation-de-donnees-personnelles).

96. S. Rossello and P. Dewitte, ‘Anonymization by Decentralization?’.

97. Ibid.: ‘It would probably be less time-consuming and cheaper for the server to re-identify a user (by tracing his/her location) in a centralised approach’.

98. The DP-3T Project, ‘Security and Privacy Analysis of the Document “PEPP-PT: Data Protection and Information Security Architecture”’, GitHub (2020), https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architecture%20-%20Security%20and%20Privacy%20Analysis.pdf, p. 2.

99. The DP-3T Project, ‘Decentralized Privacy-Preserving Proximity Tracing Overview of Data Protection and Security Version’, GitHub, (2020), https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf, p. 8.
This makes the data ‘nearly anonymous’.\textsuperscript{100} For these reasons, the decentralized model presents less risk in terms of security breaches.\textsuperscript{101} The EphIDs of each app user are generated by his/her personal secret key, not by an external source. In addition, the calculation of risk takes place solely on the end user’s device; therefore, risk-related information never leaves the device,\textsuperscript{102} which allows for better compliance with the principle of data minimization. Moreover, the entire technological design of the decentralized systems is based on privacy concerns (privacy by design),\textsuperscript{103} which allows better compliance with the principles of data minimization and purpose limitation.\textsuperscript{104}

The guidelines of the EDPB\textsuperscript{105} and the European Commission\textsuperscript{106} do not express a clear preference for either model, leaving the decision up to national authorities, but the European Parliament recommended the decentralized data storage.\textsuperscript{107} In the EU most countries adopted the decentralized model. The notorious exception is France, which insists on the centralized model, a feature that probably explains its very low percentage of adherence.\textsuperscript{108}

3. A recommended DCT model for Europe

A recommended model of DCT for Europe, that is, a model that complies with EU law requirements, is a voluntary app based on the decentralized system,\textsuperscript{109} operating via Bluetooth and providing solely proximity data. The opt-out model is recommended to motivate adhesions, but it can only be implemented assuming that the legal ground for data processing is not the data subject’s consent (Articles 6(1)(a) and 9(2)(a) of the GDPR). Compliance with the GDPR and with other EU

\textsuperscript{100} Ibid., p. 2.
\textsuperscript{101} P. De Filippi, ‘The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies’, 7 Journal of Peer Production (2016), p. 4; A.C. Myers and B. Liskov, ‘Protecting Privacy Using the Decentralized Label Model’, 9 ACM Transactions on Software Engineering and Methodology (2000), p. 410. The added value of centralized models was acknowledged by the United Kingdom late in the process: originally the centralized system was used, but later on it was switched to the decentralized system due to privacy concerns (D. Skoll, J.C. Miller and L.A. Saxon, ‘COVID-19 Testing and Infection Surveillance: Is a Combined Digital Contact-Tracing and Mass-Testing Solution Feasible in the United States?’, 1 Cardiovascular Digital Health Journal (2020), p. 152).
\textsuperscript{102} S. Rossello and P. Dewitte, ‘Anonymization by Decentralization?’.
\textsuperscript{103} Ibid.
\textsuperscript{104} The centralized approach might nonetheless have an advantage: it would give scientists more data on the epidemiological development of the infection. However laudable this goal might be, it is not the objective of DCT.
\textsuperscript{105} European Data Protection Board, ‘Guidelines 04/2020’, para. 42.
\textsuperscript{106} European Commission, ‘Communication from the Commission’.
\textsuperscript{107} European Parliament, ‘EU Coordinated Action to Combat the COVID-19 Pandemic and its Consequences. European Parliament resolution of 17 April 2020 on EU Coordinated action to Combat the COVID-19 Pandemic and its Consequences’ (2020/2616(RSP)), P9_TA(2020)0054, www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf, Recital 52.
\textsuperscript{108} S. Mageit, ‘France Launches New Contact Tracing App, TousAntiCovid’, Healthcare IT New, (2020), www.healthcareitnews.com/news/emea/france-launches-new-contact-tracing-app-tousanticovid.
\textsuperscript{109} Looking into the European experience in this regard, we can see that countries that launched privacy focused apps, based on decentralized models, managed to obtain high percentages of adherence: the German ‘Corona-Warn-App’ had 6.5 million downloads within 24 h of launch and the Irish COVID Tracker was downloaded by 37% of the country’s adult population in the first week (D. Skoll, J.C. Miller and L.A. Saxon, ‘COVID-19 Testing’, p. 152).
regulations is the best way to reinforce citizens’ trust and thus encourage the use of the app in the event that it is voluntary (as it should be).\textsuperscript{110}

The API launched by Apple and Google fulfils many of the privacy requirements that have been pointed out in the EU\textsuperscript{111} and abroad: \textsuperscript{112} (a) the app is voluntary, based on the opt-in model; (b) it is prohibited to collect or use GPS location data from the phone; (c) Bluetooth beacons and keys cannot reveal the user’s identity or location; (d) users are prevented from identifying the person who has tested positive; (e) the apps based on this protocol ping at least once every 5 min as long as Bluetooth is enabled; each ping contains the device current Rolling Proximity Identifiers,\textsuperscript{113} but these will change every 10–20 min to reduce the risk of pings being used by others to track people’s location; (f) the apps will be used solely for notification of exposure to a suspicious contact in the context of the fight against the pandemic carried out by public health authorities; (g) no other use of user data is permitted, including targeted advertising.\textsuperscript{114} Such features seem to meet the criteria of privacy by design.

These technical specifications made the Google-Apple API very attractive in the EU and most European countries use it as the standard for their national apps. Although all these apps share the main protocol, each country has developed its specific features for all the other aspects not included in this API.\textsuperscript{115} As for the features that are part of the API, they must be accepted as they come and cannot be changed by national authorities. Notably, two high tech companies (with dubious past in terms of data protection), are the ones to set up the path for a secure model (as secure as it can be) of digital contact tracing.\textsuperscript{116}

In the end, DCT apps were far from successful, namely due to the very low rate of adherence,\textsuperscript{117} motivated by several reasons, from battery draining to fears of privacy threats. Even though positive results can be reached even with low adherence rates, this is one of those cases in which the more, the better. Had the apps been better received by the community, the results would certainly have been different.

\begin{small}
\begin{enumerate}
\item On the discussion about voluntary and mandatory apps see our studies Du et al., 8 \textit{JMIR Mhealth and Uhealth} (2020); Raposo, \textit{Medicine and Law} (2022).
\item T. Scantamburlo et al., ‘Covid-19 and Contact Tracing Apps: A Review Under the European Legal Framework’, (2020) eprint arXiv:2004.14665, 2020 (working paper).
\item Y. Bengio et al., ‘The Need for Privacy with Public Digital Contact Tracing During the COVID-19 Pandemic’, 2 \textit{The Lancet Digital Health} (2020), p. e342.
\item Rolling Proximity Identifiers are ‘privacy preserving identifier derived from the Temporary Exposure Key and sent in the broadcast of the Bluetooth payload. The identifier changes about every 15 min to prevent wireless tracking of the device’ (Apple-Google, ‘Exposure Notification Bluetooth® Specification Preliminary’, Subject to Modification and Extension, (2020) https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf?1, p. 3).
\item B. Cyphers and G. Gebhart, ‘Apple and Google’s COVID-19 Exposure Notification API: Questions and Answers’, Electronic Frontier Foundation, (2020), www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers; V.L. Raposo, 164 \textit{Revista do Ministério Público} (2020), p. 9.
\item M. Rahman, ‘Here Are the Countries Using Google and Apple’s COVID-19 Contact Tracing API’.
\item Interestingly – and surprisingly – private companies such as Google and Apple – companies, moreover, with a ‘suspicious past’ in terms of privacy – became seen during the pandemic as ‘trustful’ agents – at least, worthy of greater trust than governments. For detail about this paradox, see T. Sharon, ‘Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech’s Newfound Role as Global Health Policy Makers’, 23 \textit{Ethics and Information Technology} (2020), p. 45.
\item L. Horvath, et al. ‘Adoption and Continued Use of Mobile Contact Tracing Technology: Multilevel Explanations from a Three-Wave Panel Survey and Linked Data’, 12 \textit{BMJ Open} (2022), p. e053327.
\end{enumerate}
\end{small}
Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Universidade de Macau (grant number MYRG2019-00035-FLL).

ORCID iD
Vera Lúcia Raposo https://orcid.org/0000-0001-7895-2181

Author Biography
Vera Lúcia Raposo is Assistant Professor at the Faculty of Law of Coimbra University, member of the Centre of Biomedical Law and the Centre of Human Rights from the Faculty of Law of Coimbra University, and part-time supervisor at the Centre for Medical Ethics and Law, at the University of Hong Kong.