The global flood of COVID-19 contact tracing apps: sailing with human rights and data protection standards against the wind of mass surveillance

Irena Nesterova^{1,*}

¹University of Latvia, Faculty of Law, 19 Raina Blvd., Riga, Latvia

Abstract.

Research background: Countries all around the world are rapidly introducing contact tracing apps and other surveillance technologies to tackle the spread of COVID-19 raising serious concerns about human rights and democratic principles.

Purpose of the article: The article aims to analyse how human rights and data protection law regulate the COVID-19 contact tracing apps and reveal the biggest challenges that countries face in applying the essential requirements.

Methods: The article will analyse the legal framework and compare many guidance documents issued by the international organisations, including the Council of Europe, the OECD and many EU institutions on the data protection requirements for contact tracing tools and the main challenges the governments face in different countries.

Findings & Value added: The article will reveal that the existing human rights and data protection standards already impose significant requirements for contact tracing apps requiring to comply with such principles as legality, necessity, proportionality, transparency, purpose limitation, temporariness. Although countries tend to deviate from some of these standards a choice between effective response to crises and fundamental rights should not be made. The article argues that the global flood of digital surveillance technologies requires new regulatory framework and governance mechanisms to enable impact assessment, oversight and monitoring of these technologies both during and after the crises not only to ensure that they are lawful and ethical, but also to limit the dependency of governments on large technology companies as well as to prevent mass surveillance becoming the new normal on a global scale.

Keywords: *Contact Tracing; Covid-19 Apps; Data Protection; Privacy; Surveillance*

JEL Classification: *K24; K32; K38*

* Corresponding author: irena.nesterova@lu.lv

1 Introduction

The COVID-19 pandemic poses unprecedented challenges for health care systems as well as dramatic socio-economic impacts in Europe and around the world. Governments are increasingly looking to data-driven technologies as tools to contain the pandemic. The world is facing the flood of new technologies to better understand the nature of the COVID-19 pandemic and to prevent the spread of the virus.

On 13 March 2020, two days after declaring COVID-19 a pandemic, the World Health Organisation has boosted countries alongside testing, social distancing and other measures to apply contact tracing to prevent infections and save lives [1]. Contact-tracing apps have been widely implemented all around the world, including, in China, Singapore, Australia, the United States and also in the majority of European countries [2]. Contact tracing is a joint and coordinated response of the European Union (EU) member states to COVID-19 pandemic. On 15 April 2020, the European Council and the European Commission adopted Joint European Roadmap stressing that the EU is taking steps to support contact tracing applications as well as the processing of aggregate and anonymised data from social media and mobile network operators as part of the solution to curb the pandemic [3]. A range of other surveillance technologies have also been rapidly developed and deployed to tackle the spread of COVID-19, e.g. facial recognition, thermal cameras, biometric wearables and drones [2]. For example, Italy, Greece, Hungary and Germany have used drones to monitor compliance with physical distancing measures in public spaces. In Croatia drones have also been used to record people's temperature [4].

Although governments have been experimenting with different technologies to tackle the spread of COVID-19, contact tracing apps have sparked the most intense debate. All contact tracing apps aim to retrospectively trace and alert contacts of confirmed infected persons. However, countries have chosen different approaches how to implement them and some countries that rushed to introduce contact tracing apps were later forced to suspend them over privacy concerns, like Norway or to abandon them for Apple and Google model, like the United Kingdom (the UK), Germany and Italy [5, 6].

While new technologies of the processing of personal data can support efforts to monitor and track the spread of COVID-19, they have raised human rights concerns, especially about privacy and data protection. Such applications have in particular created many discussions about the limitations of human rights in times of emergency [7], the potential misuse of personal data collected in response to crises for mass surveillance [5], the dependency on large technology companies as well as reduced democracy [8].

The article aims to analyse how human rights and data protection law regulate the COVID-19 contact tracing apps and reveal the biggest challenges that countries face when applying the essential requirements. The article first analyses the conditions for restrictions and limitations of human rights and emphasises the duty to comply with human rights and fundamental freedoms in times of emergency. Second, it introduces the data protection standards for the use of contact tracing apps developed both at EU and international level. In addition to such exploration, it also provides some suggestions.

2 Obligation to comply with human rights standards in times of emergency

It is well understood that the measures required to combat the virus will unavoidably infringe human rights and fundamental freedoms. Continuous access to data and systematic monitoring of individuals by contact tracing and similar apps entail a serious interference with the rights to privacy and protection of personal data [4].

Although considerable attention by data supervisory authorities and experts were given to emerging approaches for data collection and data protection requirements for contact tracing apps, that will be explored further in the next section, impact of contact tracing apps goes beyond protection of data as they also invade privacy [7]. Article 8 of the European Convention of Human Rights (the ECHR) includes the protection of a wide range of elements of our private life including – (i) a person’s physical, psychological or moral integrity, (ii) his privacy and (iii) his identity and autonomy [9]. Surveillance technologies, including contact tracing apps can have an impact on these categories, however these concerns have received little attention and public debate. Moreover, in addition to impact on the rights to privacy and data protection, tracking and tracing apps and health apps also may have an impact on other human rights such as the freedom of assembly and association, and the right to non-discrimination [7].

There are absolute rights which cannot be justifiably infringed under any circumstances, such as the right to life that is threatened by the COVID-19 pandemic. At the same time most human rights, including the right to liberty, the right to privacy, the right to data protection, can be restricted, however under certain conditions. According to the ECHR such interests as the protection of health and public safety are recognized as grounds for the justification of interference with these rights, however such limitations are allowed if they are “in accordance with the law” or “prescribed by law” and are “necessary in a democratic society” for the protection of the objective (para. 2 of Articles 8 to 11). The last condition also requires that interference with rights must be proportionate to the legitimate aim pursued and that it is the least restrictive mean for achieving that aim [9]. These requirements for the limitations of rights are common in all other human rights instruments.

While during the times of emergency some restrictions may be justified and imposed based on the usual provisions for limitations in the interest for the protection of health, states may also need to adopt measures of exceptional nature that would require derogation from their obligation to respect certain rights under international human rights instruments. According to Article 15 (1) of the ECHR “in time of war and public emergency threatening the life of the nation” states may take measures derogating from its obligations under the ECHR to the extent “strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.” The possibility to derogate from certain rights is included also in other international human rights instruments.

Derogations are seen as appropriate way to deal with such emergency as COVID-19 pandemic as they help to ensure transparency and accountability in times of emergency [7]. According to Article 15 (3) of the ECHR a state “availing itself of the right of derogation must keep the Secretary General of the Council of Europe fully informed of the measures which is taken and the reasons therefore”. However, only few states have used this option. As of 28 August, 2020, only ten of the Council of Europe’s 47 Member States, including three EU Member States - Latvia, Estonia and Romania - announced derogations from the provisions of the ECHR [10]. It should not be assumed that a state derogating from its obligations automatically violates the human rights, while states simply limiting human rights on public health grounds do not [7].

There is no derogation from the rule of law and democratic principles during the state of emergency. Derogations may never justify any action that goes against the paramount requirements of lawfulness, proportionality, necessity and non-discrimination. As indicated by the Council of Europe, the principle of legality prescribed that states action must be in accordance with law. The principle of necessity requires that emergency measures must be capable of achieving their purpose with minimal alteration of normal rules. Moreover, any legislation enacted during the state of emergency should also include clear time limits on the duration of these exceptional measures as the main purpose of such state of emergency

regime is to contain the development of the crises and return, as quickly as possible, to the normality. States may continue to apply certain measures also after the state of emergency, but they would fall under the ordinary limitations [11].

Regardless of whether the measures take the form of ordinary limitations or derogations, they must be legitimate, necessary and proportional to the threat posed by COVID-19 pandemic and be limited in time. The governments should examine the necessity, proportionality and effectiveness of apps developed to fight the pandemic, before they are made available to the public. While the apps may contribute to the right to health, the intended protection depends entirely on their effectiveness and reliability. However, determining whether the interventions are proportional is complicated by complex trade-offs, e.g. between effectiveness and privacy, the lack of evidence and clear understanding what proportionality demands [12, 13]. Despite these difficulties, there should not be made a choice between effective response to crises and fundamental rights.

The new technologies, including the use of big data and AI in contact tracing raises concerns not only about curtailment of human rights but also regarding the continuous use of these tools for mass surveillance purposes after the crises. The COVID-19 pandemic has strengthened and justified a shift to more intense and penetrating forms of surveillance culture. It is likely that this process will have long-reaching cultural, political, and economic impacts and will fundamentally reshape the structures of the societies which emerge and our personal affective lives [5].

States should strive to adopt a long-term strategy for the management of the pandemic that does not rely on the continued limitation or restriction of human rights and fundamental freedoms. States should establish regulatory frameworks or clarify existing ones to ensure the temporary character of surveillance technologies, including by introducing sunset clauses [12, 14]. Constant scrutiny should be applied by legislative bodies, courts, international community and civil society to new technologies introduced to respond to the crisis. Close monitoring of the use of contact tracing apps and other new technologies both during and after the pandemic is necessary not only to avoid the curtailment of human rights but also to prevent mass surveillance measures from becoming the new normal.

3 Data protection standards for COVID-19 contact tracing apps

As it was revealed in the previous section, to be compliant with human rights contact tracing apps must be legitimate, necessary, proportional and time bound. However, there is a further question, what requirements governments and developers should follow to meet these underlying principles. To address this question, many international, EU and national institutions developed guidance on how to uphold data protection standards in the development and use of contact-tracing apps to support governments and app developers.

At EU level, on 16 April, 2020, the European Commission published two important guidance documents to support a common coordinated approach to the use of contact tracing apps across all member states. The e-Health Network of EU member states with support of the European Commission developed the EU toolbox for the use of mobile applications for contact tracing and warning [15]. Along with the toolbox, the European Commission adopted Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection [16]. On 21 April, 2020, European Data Protection Board (EDPB) also adopted guidelines on the use of location data and contact-tracing tools in the context of the COVID-19 outbreak [17]. These documents set out minimum data protection standards that contact tracing apps should meet to comply with EU privacy and data protection legislation.

A number of guidelines were adopted also by other international organisations. On 21 April, 2020, the Council of Europe published a joint statement on digital contact-tracing [18]. On 23 April, 2020, the Organisation for Economic Co-operation and Development (OECD) released “Tracking and tracing COVID: Protecting privacy and data while using apps and biometric” [19].

These documents identify a list of common minimum data protection requirements for contact tracing apps. The European Union Agency for Fundamental Rights (FRA) indicates 14 requirements that are found in all or most of the above mentioned documents: 1) proven effectiveness prior to development; 2) voluntary; 3) prior impact assessment; 4) privacy by design; 5) specified purpose and legal basis; 6) open source code (transparency); 6) data minimization and accuracy; 7) technical accuracy of contact detections; 8) anonymised and pseudonymised data; 9) security against cyber attacks; 10) no location data; 11) regular independent oversight; 12) interoperability; 13) deactivation and deletion after the pandemic; 14) accountability and responsibility of actors [4].

In theory, a contact tracing app should satisfy all the above-mentioned requirements. At the EU level, the overview published by the European Commission in July 2020 shows that although there is a strong consensus among the member states about part of the requirements, e.g. voluntariness and temporariness, some requirements are not followed or there are different approaches applied by states [20].

As concerns legislation, some EU Member States have prepared specific legislation for contact tracing apps to provide a legal basis for processing data in the mobile applications and to clarify the processing of personal data as well as to allow public authorities to offer a mobile application. However, many states do not have in place and are not preparing specific legislation and some of them deny the need for such legislation [4].

To ensure compliance with data protection rules, a data protection impact assessment (DPIA) of contact tracing apps should be carried out and made public. EDPB indicates that the DPIA must be carried out before implementing contact tracing apps as they involve processing of health data on a large scale, the systematic monitoring and use of new technological solution that is likely to result in a high risk to the rights and freedoms of natural persons [17]. Prior and ongoing involvement of data protection authorities (DPAs) in the development and assessment of contact-tracing apps is also important to ensure data protection compliance. While many EU Member States consulted DPAs on the use of contact-tracing apps, many member states didn't carry out prior data protection impact assessment. The lack of prior assessment of apps raised transparency, accountability, data protection and privacy concerns [4].

Some criteria might go beyond the strict requirements stemming from the data protection framework as they aim at ensuring the highest level of transparency, e.g. open source code or publicly available impact assessment [17]. The report by the European Commission reveals that for about two thirds of the national apps, the source code and technical specifications are made public [20]. The high level of transparency is essential for social acceptance, public scrutiny and trust of contact tracing apps. One of the major challenges is ensuring a broad public acceptance and therewith a wide usage that is precondition for the effectiveness of the app.

The effectiveness of any contact-tracing system depends on wide public support. It is believed that the level of support can be increased also by opting for a data-minimizing solution [21]. Emerging approaches for collecting and processing data for contact tracing apps have been subject to intense public debate.

The Council of Europe as well as the EDPB and the European Commission has indicated that the information of the proximity between persons can be obtained without locating them, digital contact tracing should be done on the basis of connection records between devices rather than on the basis of location data [16 - 18]. As it is recommended, in

most EU Member States, contact-tracing apps are based solely on the processing of Bluetooth proximity data, but in some countries apps have requested access to location data. For example, Norway has suspended its contact tracing app after data protection authority announced that it poses a disproportionate threat to user privacy, including by using location data [5].

While there is consensus on what data should not be used, there has been much debate about how data should be collected, stored and processed. Contact tracing apps may rely on centralized or decentralized approach. Apps relying on centralized architecture send data collected by a user's phone to a central database controlled by a public authority, e.g. national health agency, where contacts are matched, whereas decentralized approaches instead match contacts on the user's device [22, 14]. The European Commission and EDPB do not specifically advocate either approach, but the decentralised solution is considered to be more in line with the minimisation principle [17]. Most EU member states have chosen decentralized approach, with users' data produced and stored locally on their device, however in some Member States apps used centralized approach, where users' data are stored and processed on a central server [4].

Most of the EU member states followed publicly available protocols while developing an approach for their national contact tracing mobile application. The first proximity-tracing framework was the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) that foresaw a centralised mechanism. Subsequently, a consortium composed of several international experts from academia and research institutions, proposed a decentralized alternative: the Decentralised Privacy-Preserving Proximity Tracing (DP-3T). Then Apple and Google announced that they would develop Exposure Notification Application Programming Interfaces (APIs) based on the decentralised approach and also indicated that it will not support centralized app architectures. Although many states initially favoured centralised approach, after Apple and Google announcement a number of states, e.g. the UK, Italy and Germany gave up building a centralized app and instead switched to this decentralised approach. Many other European states, e.g. Latvia, Estonia, Finland, Austria, Ireland, the Czech Republic and Switzerland, also invented apps based on the Apple and Google's decentralised model [5]. Furthermore, Apple has released so called Exposure Notification Express in an update for iOS 13,7 operating system for iPhones, letting their users carry out contact-tracing without the need to download an official Covid-19 app. This keeps a log for fourteen days of other phones detected via Bluetooth and serves an alert if one or more of their users is later diagnosed to have the virus. It is intended that local public health authorities will determine what the notification says, for instance to advise the user to download app for further guidance. As of September 2020, Google is planning to follow Apple with a parallel scheme of its own for Android [6]. The above described episodes show the role that tech giants play in relation to decisions of governments and dependency on them for implementing large scale digital solutions that pursue public interests and lead to questions far beyond fundamental rights concerns, i.e. the necessity to limit the dependency of these large technology companies and digital sovereignty [8].

Regardless of the chosen technological solution, a key concern is whether these apps can help to manage the spread of the virus, i.e. about effectiveness that has been questioned by various actors. There is currently insufficient evidence to support the use of digital contact tracing as an effective technology to support the pandemic response. The effectiveness of these apps depends of their download and consequent use. Researchers at University of Oxford (UK) have suggested that 60% of a country's population would need to have and use a contact tracing app to make it effective [23]. The European Commission has also admitted that it is too early to evaluate the uptake and effectiveness of apps in EU Member States [20].

If an app is ineffective, it becomes unnecessary, and thus unlawful and unethical. Apps that are no longer beneficial should be improved or suspended. A review and exit strategy must be in place to establish when and how fast this should happen [24, 25]. The assessment of the apps should be conducted by an independent body, such as a regulator or an ethics advisory board, and not by the designers or the government itself and be guided by experts in different fields, i.e. computer sciences, data sciences, health and behavioural sciences, social sciences, ethics and law.

To address the above-mentioned concerns, states should introduce impact assessment of contact tracing apps and other surveillance technologies that addresses not only impact on human rights and fundamental freedoms, in particular privacy and data protection, but also ethical and social implications as well as the impact on the rule of law and democracy. Countries should adopt regulatory framework that sets out procedures to carry out such assessment both for proposed and existing technologies as well as establish monitoring and oversight mechanisms.

4 Conclusions

While governments are increasingly looking to data-driven new technologies as tools to contain the pandemic, these technologies, including contact tracing apps, may constitute a serious interference with human rights, in particular privacy and data protection. Even in the times of emergency, measures that restrict human rights must be legitimate, necessary and proportional to the threat posed by COVID-19 pandemic and be limited in time and there should not be made a choice between effective response to crises and human rights. States should strive to adopt a long-term strategy for the management of the pandemic that does not rely on the continued limitation or restriction of fundamental rights and freedoms.

While surveillance technologies, including contact tracing apps, invade privacy, psychological and moral integrity, the emerging approaches for data collection and data protection requirements for contact tracing apps have attracted the most attention. There is a strong consensus among European countries about some of the requirements stressed in the guidance documents of the international and EU institutions, e.g. voluntariness, at the same time other requirements are not followed or there has been different approaches applied, e.g. on the non-usage of location data and conducting impact assessment. Some requirements from EU and international institutions might go beyond data protection rules, e.g. open source code and publicly available impact assessment, however they help to ensure transparency that is essential for social acceptance, trust and usage of contact tracing apps and therewith for the effectiveness of the app. The search for the right approach for collecting, storing and processing data for contact tracing apps, e.g. preferring decentralized approach instead of centralized approach, reveals positive examples of effective collaboration between private sector and public sector for collective benefit and ability to find effective technological solution for complying with data minimisation and other data protection principles. At the same time these examples, in particular Apple and Google model, raise new crucial issues about the need to respect digital sovereignty and limit the dependency on large technology companies.

Adequate regulatory frameworks and governance mechanisms should be established around contact tracing apps and other surveillance technologies. States should carry out impact assessment both for the proposed and existing technologies that addresses not only impact on human rights, in particular privacy and data protection, but also ethical and social implications and the impact on the rule of law and democracy. States should also establish monitoring and independent oversight mechanisms by engaging broad participation of relevant stakeholders as well as clear requirements for transparency. Close monitoring of impact, efficiency and necessity of contact tracing apps and other new technologies both

during and after the pandemic is crucial not only to avoid the curtailment of human rights and democratic principles but also to prevent mass surveillance measures from becoming the new normal. These measures could help to change the direction of the wind and ensure sailing towards the world where human rights and freedoms are respected rather than arriving at the age of surveillance.

This work is an output of the research project and has been financially supported by the specific support objective activity 1.1.1.2. “Post-doctoral Research Aid” of the Republic of Latvia (Project No.1.1.1.2/VIAA/1/16/196 “Striking the Right Balance between Privacy and Security in Cyberspace: Building Strong Data Protection Standards across Europe”), funded by the European Regional Development Fund.

References

1. World Health Organisation. (2020, 13 March). *WHO Director-General's opening remarks at the media briefing on COVID-19 - 13 March 2020*. <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-mission-briefing-on-covid-19---13-march-2020>
2. Couch, D. L., Priscilla R., Komesaroff P.A. (2020). COVID-19 — Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, Early access
3. European Commission, the European Council. (2020). *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
4. FRA. (2020). *Coronavirus pandemic in the EU - Fundamental Rights Implications - Bulletin 2*. Luxembourg: Publications Office of the European Union, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf
5. Craglia, M., de Nigris S., Gómez-González, E., Gómez, E., Martens, B., Iglesias, M., Vespe, M., Schade, S., Micheli, M., Kotsev, A., Mitton, I., Vesnic-Alujevic, L., Pignatelli, F., Hradec, J., Nativi, S., Sanchez, I., Hamon, R., Junklewitz, H. (2020). Artificial Intelligence and Digital Transformation: early lessons from the COVID-19 crisis. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121305/covidai_jrc_science_for_policy_report_final_20200720.pdf
6. Kelion, L. (2020, 2 September). *Coronavirus: Apple iPhones can contact-trace without Covid app*. <https://www.bbc.com/news/technology-53987928>
7. Spadaro, A. (2020). COVID-19: Testing the Limits of Human Rights. *European Journal of Risk Regulation*, 11(2), 317–325.
8. Tamar, S. (2020). Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers. *Ethics and Information Technology*, Early acces.
9. European Court of Human Rights. (2020). *Guide on Article 8 of the Convention – Right to respect for private and family life*. https://www.echr.coe.int/documents/guide_art_8_eng.pdf
10. European Court of Human Rights. (2020). *Derogation in time of emergency*. https://www.echr.coe.int/Documents/FS_Derogation_ENG.pdf

11. Council of Europe. (2020). *Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis*. Council of Europe. <https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40>
12. Nijssingh, N., van Bergen, A., Wild V. (2020). Applying a Precautionary Approach to Mobile Contact Tracing for COVID-19: The Value of Reversibility. *Journal of Bioethical Inquiry*, Early access.
13. van Kolfschooten, H., de Ruijter, A. (2020). COVID-19 and Privacy in the European Union: A Legal Perspective on Contact Tracing. *Contemporary Security Policy*, 41(3), 478–491.
14. Culnane, C., Leins, K. Rubinstein, B.I.P. (2020). Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 through technological interventions. *Medical Journal of Australia*, 213(1), 6-8.
15. E-health Network. (2020). *Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States*. European Commission. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf
16. European Commission. (2020). Communication from the Commission. *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. European Commission. https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf
17. EDPB. (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
18. Council of Europe. (2020). *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*. Council of Europe. <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7>
19. OECD. (2020). *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics*. OECD. <https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/>
20. European Commission. (2020). *Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020*. European Commission. https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf
21. Abeler, J., Backer, M., Buermeyer, U., Zillesen, H. (2020). COVID-19 Contact Tracing and Data Protection Can Go Together. *Jmir Mhealth and Uhealth*, 8(4), 1-5.
22. Ahmed, N., Michelin, R.A., Xue, W., Ruj, S., Malaney, R., Kanhere, S.S., Seneviratne, A., Hu, W., Janicke, H., Jha, S.K. (2020). A Survey of COVID-19 Contact Tracing Apps. *IEEE Access*, 8, 134577–134601.
23. University of Oxford. (2020, 16 April). *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown*. <https://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>
24. Morley, J., Cowls, J., Taddeo, M., Floridi, L. (2020). Ethical Guidelines for COVID-19 Tracing Apps. *Nature*, 582(7810), 29–31.

25. Federica, L., Hallowell, N., Johnson, S., Prainsack, B., Samuel, G., Sharon, T. (2020). COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale. *Journal of Bioethical Inquiry*, Early access