Contact tracing in the COVID-19 pandemic

Opinion of the Bioethics Commission

Contact tracing in the COVID-19 pandemic

Opinion of the Bioethics Commission

Vienna, 2020

Imprint

Media owner, publisher and editor:
Secretariat of the Bioethics Commission, Ballhausplatz 2, 1010 Wien
Authors: Bioethics Commission
Translation: MMag. Felicitas Hueber
Vienna, 2020. Date: 8 June 2020

Content

1 Introduction

The COVID-19 pandemic has resulted in massive restrictions and upheavals for individuals, for our society and for our economy. Globally, solutions are being sought to minimize infection rates and, at least in the medium term, to enable us to live with the virus in a way that is as close to the pre-pandemic normality as possible. While the need to develop vaccines and effective drugs against COVID-19 is virtually undisputed, digital methods for keeping track of infection chains – especially applications on mobile phones with Bluetooth and WLAN interfaces ("corona apps") – have proved controversial and have triggered emotionally charged debates. While some see these digital methods as essential tools for containing the pandemic, and some proponents believe their use should be mandatory, critics point out the danger of uncontrolled surveillance that is invisible for the user and of unauthorized use of personal data for political, commercial and other purposes.

Currently, the use of different types of "corona apps" that serve different goals is being discussed in many countries around the world.[1] Besides apps for tracking infection chains, there are a number of other apps related to COVID-19:

- Information apps provide information, for example, about the current restrictions applicable at a particular location or for a particular institution, or about the density of people at a particular location.
- "Data donation apps" are used to disclose mobility data and similar data for pandemic research and public planning purposes.
- Immunity apps (more appropriately called immunity passports, or immunity "licenses"[2]) are used to record the immunity status of individuals for situations where freedom of movement or access to certain places or services depends on immunity.

---

1 Lists with apps etc., which are continuously kept up-to-date, are available at https://www.gsa.europa.eu/GNSS4Crisis (sh. News European Parliament May 15, 2020, Covid-19 tracking apps: ensuring privacy and data protection, https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection) (accessed May 29, 2020); Covid-19 Digital Rights Tracker via Morley et al, Ethical guidelines for COVID-19 tracing apps, Nature May 28, 2020, https://www.nature.com/articles/d41586-020-01578-0 (accessed May 29, 2020); Covid Tracing Tracker (MIT Technology Review): https://www.technologyreview.com/2020/05/07/1001354/how-to-submit-a-change-to-the-covid-tracing-tracker-project/ (accessed May 27, 2020).

2 Persad, Govind, and Ezekiel J. Emanuel. "The Ethics of COVID-19 Immunity-Based Licenses ("Immunity Passports")." JAMA (online May 6, 2020), DOI: 10.1001/jama.2020.8102.; Natalie Kofler, Françoise Baylis, "Ten reasons why immunity passports are a bad idea", Nature 581 (May 28), 379–381, (2020).

- Quarantine apps monitor compliance with quarantine regulations by persons who are required to self-isolate, or even generally monitor compliance with access bans, social distancing regulations and the like by the population.
- Symptom check apps, which record which symptoms infected persons are suffering from in order to better understand the disease, and which make it easier for people with certain combinations of symptoms to detect a possible COVID-19 infection and to self-isolate and have themselves tested at an early stage.

The present statement deals exclusively with apps that serve the purpose of contact tracing (also called proximity tracing apps, exposure tracing apps). The other types of apps related to COVID-19 are not the subject of this statement.

The types of contact tracing apps that are currently most common use Bluetooth signals to indicate which mobile devices (and thus which persons) were in the immediate vicinity of another device. The aim of their application is the digital tracing of possible chains of infection with the aim of notifying and isolating affected persons. In addition, there are approaches based on the use of location data (such as GPS coordinates obtained via mobile phone or WLAN networks) or combining these with Bluetooth-supported proximity tracing.

Linguistically, a distinction is often made in literature between “tracking” and “tracing”. Although these terms are oft treated as synonyms in connection with digital monitoring, the former usually refers to the collection of data that may be used in the future to trace infection chains, i.e. proactive data collection. The second, on the other hand, is called “tracing” in the narrower sense and refers to the retrospective presentation of possible infection paths. In this statement we use the term “tracing” as an umbrella term when both practices are meant; if only one specific function is meant, this will be noted separately.

The fact that contact tracing uses technical aids – such as information and communication technologies – is not new in itself. What is new about the so-called “corona apps” is on the one hand the possibility of automating some or even all of the steps that were previously performed by humans. This is an advantage when the volume of cases processed is high and tracing must be fast in order to isolate affected persons and thus stop the spread of the virus. On the other hand, the proactive character is also new, since a large amount of contact data is collected and processed as a precautionary measure, of which only a very small part is actually relevant for infection. The data collection and the theoretical potential for monitoring and discrimination associated with such proactive and automated contact tracing bring with it a number of ethical, legal and socio-political challenges. These are the subject of the present statement.

2 Containment of epidemics through contact tracing

Contact tracing – i.e. tracing physical instances of contact that an infected person has had with other people during the contagious phase of the disease – is an established and recognized means of epidemic control. This method has, for example, contributed significantly to the containment of the Ebola epidemic.[3] The primary aim is usually to test or isolate contact persons as quickly as possible in order to stem the spread of the disease. In addition, research interests play an important role, since only by tracing infection chains is it possible to better understand a disease. This is the only way to take responsible political steps to focus restrictive measures on those areas where they are necessary and proportionate.

2.1 Classic ("manual") contact tracing

In classic contact tracing, as has been done for a long time on the basis of Section 5 of the Austrian Epidemics Act, the contacts relevant to infection are determined individually ("manually") by employees of the health authorities in the event of an infection. This is usually done by interviewing both the infected person him- or herself and people in his or her environment (employer, family members, etc.) and – subsequently – the contact persons thereby identified. Information and communication technologies can also play a role in such "manual" tracing, e.g. if the contacts during the infectious phase are reconstructed in consultation with the person who has tested positive based on their digital calendar, chat histories and the like.

Classic contact tracing is extremely personnel- and resource-intensive. The employees entrusted with the task require comprehensive training. In general, the time factor is essential so that contact persons can be identified and isolated before infected contact persons spread the virus further. Ideally, this form of contact tracing is combined with on-site testing and – if there is a sufficiently high probability of infection – with issuing a notification of isolation, at least until the situation has been clarified.

Difficult ethical issues may arise, particularly where confidentiality is involved. Contact tracing can reveal extremely sensitive information (e.g. concerning extramarital

3 World Health Organization (WHO), Implementation and management of contact tracing for Ebola virus disease. Emergency Guideline (2015), https://apps.who.int/iris/bitstream/handle/10665/185258/WHO_EVD_Guidance_Contact_15.1_eng.pdf;jsessionid=6E13ABBDB48EC4E2D153FA7803CF45F9?sequence=1 (accessed May 23, 2020).

affairs, illegal employment relationships, etc.). In this regard, a rule of thumb can be that the identity of the individual in question who has tested positive may and must be disclosed to persons with whom he or she has come into contact if this is necessary in order that those persons may be interviewed in a targeted manner. Neither the way in which the person who has tested positive could have been infected, however, nor the identity of other contact persons, may be revealed.

Furthermore, visited persons will only be willing to disclose contacts if they can be sure that information disclosed for the purpose of contact tracing cannot be used against them in any legal or official proceedings. In this respect, the exclusion of such information as evidence in court proceedings should therefore be considered.

2.2 Contact tracing by operators of facilities

Proactive contact tracing (i.e. tracking in the literal sense of the word) by the operators of particular facilities means collecting data (or preparing data for disclosure that were collected for other reasons) on the users of the relevant facility which can then be used to trace contacts if the need arises. A classic example would be the recording of the presence of employees in the workplace by employers. This can be done in an analog way using attendance lists and occupancy plans (which employees sometimes fill in themselves), or digitally, for example by requiring employees to register with their own chip card when entering a room or taking up a workstation.

COVID-19 containment measures that are already common practice in workplaces and a number of other contexts could in principle be transferred to many institutions. It is conceivable, for example, that the identity and seating number of theatergoers or restaurant guests could be recorded, or that hotel guests could register with their room card and thus with their identity when they use a certain section of the spa area.

Differences exist not only in the way that the data are collected (entirely analog, digital, in a standardized data format), but also in the further processing of the data. For example, data can be forwarded to a central office, or remain in the respective institution and be disclosed only upon request by the health authority (“enhanced manual tracing”).

Certain types of “corona apps” can also be used for contact tracing on the initiative of the operators of facilities. These can, for example, require users of the facility in question to scan a QR code (event code) issued by the facility, or conversely, the facility can scan a code on the user’s mobile phone. This in turn allows for very similar functionalities to those we know from proximity tracing (see 2.3), the use of which is currently widespread, such as the automated sending of warning messages to the mobile phones of the users concerned. The method addresses more specifically the phenomenon of “super-spreader events”, i.e. situations in which often only a single infected person infects a large number of other people “in one go” (cf. media reports on après-ski bars, choir rehearsals, cocktail parties, family celebrations). It also has advantages in situations in which it is not possible to carry a mobile phone with you all the time, but a “check-in”

and “check-out” at the entrance is possible (e.g. sauna, hot tub). Depending on how detailed the definition of “events” is (e.g. a table in a restaurant or a box in a theater can also have its own code), this method may offer a higher degree of reliability than proximity tracing using automated digital handshakes.

2.3 Decentralized digital contact tracing

Completely decentralized contact tracing using “corona apps” involves a broad-based reconstruction of physical contacts of a certain minimum duration and spatial proximity that is not limited to specific groups of people or situations.

The combination of a wide range of differently designed apps is conceivable. Differences are first of all in the definition of an infection-relevant contact (duration of contact, distance, time span covered) and in the technology used to detect it (precise GPS localization of all app users or communication between the terminals via “digital handshakes”). There are also differences in the authentication of the users during the installation of the app (no authentication, IP address, strong authentication), in the conditions under which a COVID-19 infection is detected via the app (mandatory or voluntary, confirmed by health personnel or not), and generally in the storage of the relevant data (centralized or decentralized in the respective end device).

Another difference is between apps that, if a user tests positive for COVID-19, automatically inform the contact persons registered via the app network about their risk of infection and the obligation to isolate or test themselves (track and trace apps), and those that do not. Apps in the latter group necessitate “enhanced manual tracing”: they give health authorities access to the proximity protocols of the apps of individuals who have tested positive, yet leave it up to the health authorities to manually track the infection chains and contact possible further infected persons. From a data protection perspective, the latter models are less desirable, as they lead to the direct identification of contact persons by the authorities.

3 Ethical and legal requirements for tracing apps

Ethical considerations are based on a canon of values, which in particular is also expressed in fundamental rights.[4] In this context the protection of human dignity, life and health as well as the freedom of the individual are of great importance, and as such, these values and the associated ethical principles, such as autonomy, justice, and informational self-determination, must also be the primary guides to action when using apps in the context of containing a pandemic. This does not mean that citizens should unquestioningly agree to the use of a "corona app" and be directly or indirectly forced to use it (see below 4). However, it also cannot mean that such apps should not be further developed and made available to as many people as possible – provided that diverse issues regarding the protection of civil liberties, prevention of misuse of the collected data (e.g. for surveillance purposes) or meaningful epidemiological evaluation are solved. On the contrary, the use of a particular technology to contain a pandemic can, depending on the situation, be the "less severe means" to avoid more far-reaching encroachments on fundamental rights, such as the fundamental right to freedom of movement or freedom of assembly. However, this requires trust on the part of citizens in the technology and its application and in the processing of data by state authorities. This means that measures must be rigorously implemented to make "corona apps" epidemiologically meaningful, explainable, evidence-based and safe for citizens and their privacy. Another currently unresolved issue in the use of these apps is their technical maturity and reliability, so that ongoing and critical evaluation is necessary. In addition, there must be a clear time limit on the collection of data, as well as the embedding in an overall strategy for dealing with the pandemic. Some of these points will be examined in more detail below.[5]

---

4 See also: Cohen, I.G., Gostin, L.O. and Weitzner, D.J., Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension JAMA.

5 On the ethical evaluation of tracing apps, see also Contact tracing as an instrument in pandemic control – central aspects from an ethical perspective, Opinion No. 33/2020 of April 6, 2020 of the Swiss National Ethics Committee in the field of human medicine (NEK), https://www.nek-cne.admin.ch/inhalte/Themen/Stellungnahmen/NEK-stellungnahme-Contact_Tracing.pdf; World Health Organisation (WHO), Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim Guidance of May 28, 2020, https://www.who.int/publications-detail/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1; Jeffrey Kahn and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies (ed.), Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance (2020), https://muse.jhu.edu/book/75831.

3.1 Epidemiological appropriateness of a given measure

The first prerequisite for any measure designed to contain the pandemic is its epidemiological appropriateness, whereby the accuracy of the measure plays a decisive role. Previous experience with a number of "corona apps" points to the problem of false negative results in which the app cannot detect corona cases.[6] For example, the "Stop Corona App" developed by the Austrian Red Cross in cooperation with Accenture has a number of reasons for false negative results, i.e. corona cases that the app cannot detect. This could occur in the following cases:

- A COVID-19-positive person does not have an app, does not have his or her mobile phone with him or her at the time of the infectious contact, has Bluetooth deactivated, etc.
- The infectious contact is too short to be registered by the app (e.g. on public transport or when jogging by).
- The infectious contact took place earlier than 54 hours before the notification of illness (e.g. because symptoms were not correctly interpreted until later).
- A COVID-19 positive person is asymptomatic and never gets tested or (for whatever reason) does not report his or her test result via the app.
- COVID-19 is not transmitted by close physical contact but by some other means (e.g. lubricant or aerosol infection).

There are also many reasons for "false-positive results", i.e. the opposite case, that cases that are not corona cases are evaluated as such by the app. This could be the case for the following reasons:

- A person has rashly issued a warning via the app (e.g. misinterpreted symptoms, otherwise overreacted or acted out of improper motives).
- A registered contact was objectively not likely to lead to infection (e.g. partition wall, sitting back to back in public transport)

While false positive results are more or less part of the nature of contact tracing and as such are not alarming, too many cases being wrongly categorized as corona cases leads to frustration and generally to a loss of motivation and trust among users. False-negative results are particularly harmful if the app causes a "reverse placebo effect", i.e. people who have false confidence that they are protected by using the app or that they are

6 For example, there are reports in the media that despite six million downloads in over four weeks, the Australian COVIDSafe app has only led to the identification of a single infected person and that the experience in Singapore also seems sobering, https://www.tagesschau.de/ausland/australien-coronavirus-app-103.html.

doing their part to contain the virus, refrain from taking preventive measures against infection (distance, mechanical protection).

Both false-negative and false-positive results should therefore be minimized as much as possible by an appropriate system design. For example, it would have to be ensured that people who test positive for COVID-19 do in fact issue a warning message via the app, e.g. under official supervision. In addition, measures would have to be taken to ensure that those who receive a warning also undergo a test (see also 3.2).

3.2 Embedding in an overall strategy (system view)

To combat COVID-19, a comprehensive approach to pandemic containment is needed that consists of many components and can only be meaningfully assessed in its entirety. The focus of media attention on "corona apps" distracts from the fact that they can only function as building blocks in a larger concept. The components of such a concept include not only the still indispensable "manual" tracing, but also a test strategy, an isolation strategy and an adequate communication strategy.

The immediate purpose of the application should be the rapid isolation of potentially infected persons and the targeted allocation of testing resources, e.g. by asking mobile phone owners who receive a warning to isolate themselves and be tested immediately. This requires the availability of sufficient, easily accessible and free testing facilities that produce reliable results relatively quickly. The more cumbersome it is for warned persons to undergo a test, the longer they have to wait for test results and have to cancel professional appointments or the like, the less willing they are to respond to a warning. Effective measures against the stigmatization of people who have tested positive can also increase their willingness to respond to warnings.

An appropriate public communication strategy is indispensable for the success of an app. This begins with clear communication about the fact that owning the app does not protect against personal infection and cannot replace protective measures. It also includes balanced communication about the importance of a warning message and the steps to be taken as a result. Communication should build trust and avoid panic, as well as provide incentives to immediately go into isolation and be tested. Several warning levels – depending on the intensity of exposure – are to be recommended ("exposure risk calculation", "exposure risk score"). Overall, this communication strategy should not only be understood as an "information campaign" to convince the public of the usefulness of the apps; rather, spaces for sharing of experiences, questions, and suggestions from the public should also be created.

3.3 Suitability in a cross-border context

People are mobile, and national borders – especially within the Schengen area or within the European Union – have been gradually reopening since May 2020. It is therefore essential for an up-to-date protection concept that the app in question not only function within national borders, but that a solution is used that works across borders[7] or at least that the interoperability of different systems is ensured.[8]

3.4 Impact assessment and evaluation

The implementation of a contact tracing strategy, which includes the use of apps, requires a thorough impact assessment, taking into account all societal impacts. It must also be accompanied by a plan to evaluate the effectiveness of the strategy. Such an evaluation strategy may include the following points:

- Are the architecture and programming still in line with the latest epidemiological knowledge (e.g. concerning infection routes)?
- How does a changing proportion of people using the apps affect infection rates (region-specific evaluation using postcodes etc.)? If a higher app usage density coincides with a stagnating or growing infection rate, what are the reasons for that?
- How does a growing number of people using such apps affect the public's trust in the health care system and the federal government?
- What concerns about data protection, privacy, autonomy, experience in use etc. do the users of the apps report?

Overall, digitally supported contact tracing must constantly adapt to new epidemiological findings and should provide solutions tailored to different situations without confronting the individual users with the complexity behind these solutions. The "super-spreader" phenomenon, for example, should also be appropriately addressed, e.g. by developing special technical solutions for certain types of events, locations and facilities where the currently common Bluetooth-supported proximity tracing fails to work or does not work well.

---

7 GitHub, Decentralized Privacy-Preserving Proximity Tracing, https://github.com/DP-3T; Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), https://www.pepp-pt.org/.

8 Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States (April 15, 2020), https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf; Interoperability guidelines for approved contact tracing mobile applications in the EU (May 13, 2020), https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

3.5 Trust through transparency

Since the effectiveness of automated contact tracing depends strongly on the distribution of the app, and its distribution strongly depends on the trust of the people, absolute transparency about the functioning and performance of an app is essential. Assurances must not only come from the persons or organizations that have developed a specific app. Rather, the source code must be verified and published by independent institutions (data protection authorities, NGOs, etc.). The establishment of a user committee and the accompanying support from a multi-disciplinary expert committee would also be an advantage (see also 3.8).

3.6 Data protection and data security

In the evaluation of "corona apps" and in the public discussion, data protection considerations are regularly in the foreground. Two types of data processing are to be distinguished: on the one hand, the processing of health data of a COVID-19 positive tested person in case of a notification of illness and possibly the health-relevant data of that person's contact persons in contact tracing, and on the other hand, the general data arising in the context of precautionary storage of data for a possible later reconstruction of the chain of infection.

This data is processed differently depending on whether the app follows a decentralized or a centralized approach. From the perspective of data protection, and here in particular the principle of data minimization, systems with a decentralized architecture must be given preference. In the currently most widespread models of decentralized architectures, only pseudonymized[9] data is exchanged and stored locally on the respective smartphones. For this purpose, each smartphone on which an app is installed sends a periodically (about every 15 minutes) changing code, which is recorded by other smartphones with apps in close proximity and stored locally. The code alone does not allow conclusions to be drawn about the sender. If a person receives the information that he or she has tested positive for COVID-19 or has been in contact with a person who has tested positive, he or she can or must (depending on the legal situation) upload the codes sent by his or her smartphone within a certain period of time to a central server (S1). For this purpose, the person usually needs his own unlock code, which is generated once by another, state-operated server (S2) when a corresponding entry is made in the (non-public) register of notifiable diseases according to Section 4 of the Austrian Epidemics Act in order to prevent false warnings from

9 Pseudonymized data is data that cannot be traced back to a specific person on its own, but which is linked by a key to the names and/or contact details of specific persons. Even if the key is only accessible to a single person, in this case pseudonymized data is still referred to as personal data, and the data protection provisions of the GDPR continues to apply. Only when the key that connects the two data sets with each other is irretrievably destroyed, and when it has become impossible to trace back the person from whom the data originated, is it referred to as anonymized data. Anonymized data are also not within the material scope of the GDPR.

non-COVID-19 positive persons. However, data from smartphones are not transmitted to the S2 for this purpose. Only pseudonymized data are stored on the S1, no contact data. All smartphones with an app synchronize regularly with S1 and thus receive all codes that the smartphone has sent from a positively tested person. This enables a comparison with the codes stored on the smartphone locally on the smartphone. If a code retrieved from S1 matches a locally stored code, the user on the smartphone had contact with a person who tested positive in the relevant period of time and who therefore uploaded the codes stored on his/her smartphone to S1, and receives a corresponding warning message. Conclusions about the other person or other persons who had contact with this person are, however, not technically possible. It is not possible to identify the person who has tested positive on the basis of either the codes stored on S1 or the pseudonymized contact data stored on the other smartphones. The data on positive tests stored in the register in accordance with Section 4 of the Austrian Epidemics Act are only required to generate the activation code and are not connected to the app's system. The sick person is not "revealed.".

In the opinion of the Bioethics Commission, the consistent use of pseudonymization and the minimization of processed data in decentralized systems can considerably reduce data protection risks.[10] Nevertheless, the principles of data protection law must also be applied and observed in such systems.

As far as the legal basis for data processing is concerned, this is to be found in Article 9 GDPR for health data, and in Article 6 GDPR for general data (non-health-related mobility data, etc.). In addition, telecommunications law may be applicable in implementing the ePrivacy Directive when accessing data already stored in the end device.

The processing of data on the person identified as infected and his or her contact persons is relatively unproblematic and is based on Article 9 para. 2 (i) or (h) GDPR in conjunction with the Austrian Epidemics Act, Article 10 para. 2 Austrian Data Protection Law, and other national legislation.[11] As far as the precautionary storage of contact data is concerned, however, a distinction must be made according to upon whose initiative the app is used and thus the collection and further processing of the data occurs. If the initiative is taken by the data subject him- or herself by voluntarily using the app in order to help contain the pandemic, the processing can regularly be based on the data subject's free and informed consent (Article 6 para. 1 (a), Article 9

---

10 See also General Data Protection Regulation (GDPR) Recital 28 as well as European Data Protection Board (EDPB) Guidelines (footnote 11), Annex: Contact tracing applications analysis guide; Chaos Computer Club, 10 requirements for the evaluation of "Contact Tracing" apps, April 6, 2020, https://www.ccc.de/en/updates/2020/contact-tracing-requirements.

11 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, April 21, 2020, n. 33, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; implicitly critical of the "exposure" of COVID patients without their consent *Forgó*, Einige Bemerkungen zu datenschutzrechtlichen Rahmenbedingungen des Einsatzes von Tracing Apps zur Bekämpfung der COVID-19-Krise, Version 1.0 (April 13, 2020) 10, available at https://id.univie.ac.at/fileadmin/user_upload/i_id/Website_Header_IDLaw/Gutachten13.pdf.

para. 2 (a) of the GDPR). If, on the other hand, the app is used primarily on the initiative of the state or of the operator of a facility, it is difficult to establish that consent is given "freely" (in particular, Article 7 para. 4 of the GDPR would make it impermissible to make performance of a service dependent on consent). Depending on the concrete form of the system, it will then need a specific legal basis within the meaning of Article 6 para. 1 (c) or (e) in conjunction with Article 6 para. 3 of the GDPR or, at best, also Article 9 para. 2 (g) of the GDPR.

Such an approach cannot be inferred from the current version of the Austrian Epidemics Act when read in conformity with fundamental rights, and in particular not from Section 5 (3) of the Epidemics Act, which means that in the case of contact tracing in connection with a visit to the theatre and the like, either the Epidemics Act needs to be adapted or a basis in special COVID-19 legislation is required. This special legal basis must contain, among other things, suitable guarantees for data subjects, clear limitations on the purposes for which data may be processed, as well as unambiguous determination of the bodies to which data may be disclosed and the conditions under which this may be done.[12] This law should also regulate further details, in particular with regard to storage periods, the conditions of further use for research purposes and the like.

In all cases, data processing must comply with the general principles of data processing expressed in Article 5 of the GDPR, including the requirement of data minimization, purpose limitation, storage limitation and the guarantee of the best possible data security. The purpose limitation includes, among other things, that any secondary use that is incompatible with the purpose of the data collection – in particular in judicial or other proceedings against the user concerned – is excluded. These principles can also be realized by the technical design itself (privacy by design, see Article 25 of the GDPR).

3.7 Justice and prevention of discrimination

The use of apps to support contact tracing can only be recommended if it is ensured that those people who cannot use these apps or do not want to use them for reasons that must be respected (or those for whom this is only possible with difficulty) do not suffer any disadvantages in terms of their freedom of movement and autonomy. If contact tracing apps are introduced on a large scale, it will in some cases be unavoidable that the identification of people who do not participate will take a little longer and that this may result in the infection of other people. The non-use of apps must not be at the expense of the people who do not use them, nor must the privacy of these people be encroached upon more strongly than is the case with app users by means of substitute measures (e.g. monitoring electronic payment flows in order to trace where they have been and when).

12 EDPB Guidelines (footnote 11) marginal 31; more detailed *Forgó* (footnote 11) p. 34.

3.8 Overall societal impact – towards a culture of surveillance?

In the literature "function creep" is described as the situation where data or technologies are used for ever more purposes "because they are already there." As we know from empirical studies,[13] this is one of the most important concerns people have. Even if these apps are so privacy-friendly that the risk of misuse is eliminated, just getting used to using apps can provide fertile ground for "function creep." In order to avoid this process, it would be important to ensure that users have a say in the decision making process through appropriate structures and to ensure the automatic deletion of data or their anonymization (for research purposes) and deactivation of the relevant applications and backend structures after the end of the pandemic.

In addition, a perspective on the effects on society as a whole must also take into account aspects of economic dominance and economic and political power. Even if companies such as Google, Apple, or Amazon do not directly enrich themselves with corona apps, the integration of their technology in contact tracing and data acquisition or archiving strategies is problematic in that it allows powerful large companies to further expand their market-dominating position – and also to gain more political weight.[14] The American legal scholar Frank Pasquale observed several years ago that such companies had already changed their position as market participants and had become regulatory bodies, due to their degree of economic and political influence.[15] Even though there is no ownership right by third parties in people's personal data, who has control over data sets of large parts of the population still plays an important role: is it a private, multinational company or an organization that is subject to democratic control and accountable to the public?

---

13 E.g. Ipsos, M.O.R.I., 2016. The one-way mirror: public attitudes to commercial access to health data. London: Wellcome Trust.

14 E.g. Sharon, T., 2016. The Googlization of health research: from disruptive innovation to disruptive ethics. Personalized Medicine, 13(6), pp. 563–574. Prainsack, B., 2020. The political economy of digital data: introduction to the special issue. Policy Studies [online first].

15 Pasquale F (2017) From territorial to functional sovereignty: The case of Amazon. Law and Political Economy (6 December). Available at: https://lpeproject.org/blog/from-territorial-to-functional-sovereignty-the-case-of-amazon/ (accessed June 1, 2020).

4 Voluntariness and obligation

Probably the most controversial question around the ethical evaluation of contact tracing apps is the extent to which their use must remain completely voluntary, or the state or private players can prescribe their use, or at least make it a condition for accessing certain premises and using certain services. Although this question is closely linked to that of the legal basis under data protection law, it is by no means identical:[16] even if data processing is based on a legal basis and not on the consent of the data subject, it may still be advisable to make the use of an app purely voluntary.

4.1 Admissibility of state-imposed requirements

Any obligation to use an app that is imposed by the state constitutes an encroachment on fundamental rights. This applies even if no personal data (yet) leave the user's end device at all, since the very activity of the app on the end device itself constitutes an encroachment (Bluetooth connection, battery consumption, storage space) and, in addition, not only the objectively processed data and other objective restrictions must be taken into account, but also the subjective feeling of many people that they are being monitored by the State or that society is developing in the direction of a surveillance society, and the associated unease. Thus, any such obligation must strictly comply with the principle of proportionality.

However, if the principle of proportionality is observed, it is conceivable – provided that the ethical and legal requirements outlined above in Section 3 are met – that a state could in principle introduce an obligation – limited in time from the outset – to use such apps in times of epidemics. This can be justified in particular if the alternative would only be the complete prohibition of many activities, i.e. a generally more drastic encroachment on fundamental rights (e.g. freedom of movement, freedom of assembly, freedom of employment, freedom of religious practice, freedom of art, etc.), so that the use of an app would ultimately be the less severe means. In this context, the concrete architecture of an app and the data protection implications associated with it as well as the alternative forms of tracking and tracing should be considered. In any case, such a measure would require a specific legal basis, if possible itself limited in time, i.e. either the inclusion of a new provision in the Austrian Epidemics Act or in special COVID-19 legislation.

A general obligation to use an app (e.g. in all public places) would arguably be disproportionate in any case, especially since even without an app there is no threat

16 EDPB Guidelines (footnote 11) n. 29.

of blocking all public places nor would it be possible in terms of basic rights. For those places and facilities for which universally accepted and practicable safety measures (social distancing, wearing masks, etc.) exist, the continued application of these safety measures would probably also be the more appropriate and proportionate measure.

A mandatory introduction of the app could, however, be considered for places and facilities that are currently still closed for epidemiological reasons or where compliance with regulations currently in force would impose such severe restrictions on all parties involved that, after weighing up all the circumstances, the use of the app would be the lesser encroachment on fundamental rights. In order to exclude possible effects of discrimination, alternatives (e.g. forms of conventional registration) would have to be found for persons who do not own a smartphone or whose operating system is not compatible with an app for any reason.

Therefore, the obligation to use digital contact tracing as a condition for the use of a facility may be a proportionate measure, provided that, in addition to the ethical and legal requirements described in Section 3 the following conditions are cumulatively met:

- The facility is not required for basic supplies (i.e. this excludes supermarkets, pharmacies, hospitals, public transport or similar)
- From an epidemiological point of view, the alternative would be that the facility cannot be operated at all (in particular because other protective measures are not feasible for technical or economic reasons) or that unacceptable restrictions are imposed on other persons (e.g. as a result of shortages and waiting times), i.e. that the overall impact on fundamental rights would be even greater than the app.
- Solutions (e.g. rental devices with registration) are found for people who cannot be expected to use a smartphone or the app (due to age, health, income, etc.) and thus discrimination is reliably avoided.

In addition, as part of a broader safety policy for facilities, it could be considered, while respecting the principle of proportionality, certain professionals should be obliged to use such apps who are in close physical contact with a particularly large number of different people and might therefore function as infection multipliers (e.g. health care professionals, kindergarten teachers). In addition, however, people who are exposed to a particularly high risk of infection must receive testing and manual tracing.

4.2 Admissibility of requirements imposed by private stakeholders

If private stakeholders (e.g. supermarkets, restaurants) make the conclusion of a contract dependent on the fulfilment of certain conditions, the provisions of Part III of the Austrian Equal Treatment Act (GlBG) must first be taken into account in the case of mass transactions. However, indirect discrimination on the basis of one of the features mentioned there is unlikely to occur (this is different in Germany on account of the different legal situation there). More extensive protection against discrimination (e.g. on grounds of age – possibly relevant here) exists under Part II in employment contexts. Unless other special regulations (e.g. the Austrian Local Supply Act – NahversorgungsG) apply, the general principles concerning obligations to contract must be taken into account. This means that a trader offering certain goods or services to the public may not, without objectively justified reasons, reject a customer who belongs to the addressed public and who is in need of the relevant goods or services and cannot easily get them elsewhere, if the goods and services fall within the "normal needs" or "basic needs" and if the customer is prepared and able to pay for the goods or services under the usual conditions. In principle, this does not change even the domiciliary rights, i.e. the domiciliary rights are limited in this respect. Even outside of an obligation to enter into a contract, any discriminatory exclusion from the use of a service must be avoided with a view to avoid infringement of personality rights if there is no sufficient objective justification; the decisive factor is that, in balancing the freedom of contract of the supplier and the interests of others not to be treated unequally in a discriminatory manner, the limits set by public policy are not exceeded.[17] Thus, everything focuses on the question of whether the refusal to conclude a contract with a customer without an app would be "objectively justified."

4.3 Enshrining voluntariness in the law?

There have been repeated calls not to regulate the obligation to participate in digital contact tracing, but rather to stipulate the absolute voluntariness of the measure by law.[18] This may seem surprising at first glance, given that freedom is normally the rule and coercion the exception, and as it is normally coercion that must be laid down and justified by law. But a closer look reveals that there is a smooth transition between voluntariness and state coercion, because the intervention of the operators of facilities can lead to a situation in which the use of the app becomes *de facto* mandatory even without any (direct) state coercion. Thus, for example, every operator of a facility, every host of an

17 For example, OGH 3 Ob 548/91.

18 *Forgó* (footnote 11), p. 34; indicated in the EDPB Guidelines (footnote 11), marginal 31.

event, etc. is obliged or at least expected to develop a COVID-19 protective policy for the facility or event in order to guard against possible claims for damages or to avoid a loss of reputation. One of the most obvious components of such a COVID-19 policy is to prescribe digital contact tracing, because it is particularly easy and inexpensive for the operator or host to implement. Data protection aspects can also argue in favor of operators prescribing the use of an app with a decentralized architecture rather than using much more intrusive, "manual" methods (e.g. recording customer contact data for forwarding to health authorities if necessary). It is therefore not far-fetched to expect that even without any governmental coercion, the more or less nationwide prescription of digital contact tracings by private stakeholders could arise.

For these reasons – and also in order to create legal certainty for all parties involved – it may indeed be advisable to lay down in law also the conditions under which private stakeholders can make the use of digital contact tracings a precondition for the use of a facility or participation in an event. In this respect, the considerations that have been elaborated to justify a state obligation (cf. 4.1 above) will ultimately also be decisive.

5 Conclusions and recommendations

1. There is no alternative to contact tracing in a pandemic. This is especially true in a phase in which the spread of the infection is still (or once again) at a stage where the targeted isolation of infection clusters makes area-wide restrictions for the entire population unnecessary. It can therefore only be a question of how, and not of whether, contact tracing is to be carried out. In this respect, in addition to classic ("manual") tracing, various forms of digitally supported contact tracking and tracing are increasingly being discussed, especially using digital applications on mobile phones ("corona apps").
2. Minimum requirements for such applications are their epidemiological appropriateness, their integration into an overall strategy, suitability in a cross-border context, impact assessment and regular evaluation and, if necessary, adaptation, transparency, comprehensive guarantees of data protection and data security including a time limit on the measure, reliable prevention of discrimination and careful consideration and control of the effects on society as a whole. The latter also and especially concerns effective measures against "function creep," i.e. the creeping establishment of surveillance technologies beyond the concrete cause of the COVID-19 pandemic.
3. A detailed regulation in the Austrian Epidemics Act or in special COVID-19 legislation which, in addition to the conditions for the application of the measure, also explicitly clarifies its limited duration, the prohibition of data processing for purposes other than the containment of COVID-19, and other issues, is to be demanded in the interest of legal certainty for all parties involved. It would be preferable if the actions were monitored by a multidisciplinary panel of experts. In addition, control by civil society could be enhanced by the establishment of a user committee which has a say in decisions on changing functionalities of the app.
4. The use of such applications must in principle be voluntary, although there is often no real voluntariness, even below the threshold of legal obligation, and in particular with the involvement of private stakeholders (e.g. operators of facilities or event organizers). Therefore, similar conditions should be formulated for both public and private stakeholders, under which the use of a certain application can be made a condition for the use of a facility or the receipt of a service. People who do not want to or cannot use such applications should not be disadvantaged in terms of their freedom of movement or autonomy.

5. An obligation for digital contact tracing may be justified for the use of facilities which are not required for basic supplies (e.g. concert halls or restaurants, but not supermarkets, hospitals or public transport). However, this only applies if the measure is strictly proportionate. In principle, this is only given if the facility in question (e.g. concert hall) would otherwise remain closed or could only be operated under unacceptable restrictions and therefore an even more severe encroachment on fundamental rights would occur, i.e. digital tracing would be the less severe means from the point of view of fundamental rights. For persons who do not own a smartphone or who are not able to use corresponding end devices, reasonable alternatives must be created to avoid discrimination.
6. Digitally-supported contact tracing – including the use of apps – must constantly adapt to new epidemiological findings and should provide tailor-made solutions for different situations without confronting the individual users with the complexity behind these solutions. The "super-spreader" phenomenon, for example, should also be appropriately addressed. Digital tracing solutions should therefore be developed for certain professionals who are in positions where they might function as particularly powerful multipliers of the virus (e.g. kindergarten teachers, health care personnel). Special technical solutions would also have to be developed for certain types of events, places and facilities where the currently common Bluetooth-supported proximity tracing fails to work or does not work well.

Members of the Austrian Bioethics Commission for the 2017–2020 term

Chair
Dr. Christiane Druml

First Vice Chair
Univ.-Prof. Mag. Dr. Markus Hengstschläger

Second Vice Chair
Univ.-Prof. Dr. h.c. Dr. Peter Kampits

Univ.-Prof. DDr. Matthias Beck
Univ.-Prof. Dr. Alois Birklbauer
Dr. Andrea Bronner
Univ.-Prof. Dr. Christian Egarter
Dr. Thomas Frühwald
Dr. Ludwig Kaspar
Univ.-Prof. Dr. Lukas Kenner
Dr. Maria Kletecka-Pulker
Univ.-Prof. Dr. Ursula Köller MPH
Univ.-Prof. Mag. Dr. Michael Mayrhofer
Univ.-Prof. Dr. Johannes Gobertus Meran MA
Dr. Stephanie Merckens
Univ.-Prof. Dr. Siegfried Meryn
Univ.-Prof. Dr. Christina Peters
Univ.-Prof. Mag. Dr. Barbara Prainsack
Univ.-Prof. DDr. Walter Schaupp
Univ.-Prof. Dr. Andreas Valentin MBA
Dr. Klaus Voget
Univ.-Prof. Dr. Ina Wagner
Priv.-Doz. Dr. Jürgen Wallner MBA
Univ.-Prof. Dr. Christiane Wendehorst LL.M
Univ.-Prof. Dr. Gabriele Werner-Felmayer