Proportionate response to the COVID-19 threat? Use of apps and other technologies for monitoring employees under the European Union’s data protection framework

Seili SUDER* and Andra SIIBAK**

Abstract. This article explores the potential uses by employers of contact-tracing apps and other monitoring technologies to mitigate the spread of COVID-19, and the potential concerns that these raise in the context of the European Union’s General Data Protection Regulation. Given the imbalance of power in the employment relationship, the authors call for national laws to strengthen employees’ ability to refuse the use of such apps and technologies after the end of the COVID-19 pandemic. When such tools are no longer needed to keep employees safe, additional regulations and guidance will be necessary to prevent future problems, such as function creep and other misuse by employers.

Keywords: digital contact tracing, contact-tracing apps, employee monitoring, data protection, GDPR, COVID-19.

1. Introduction

The world of work has been profoundly affected by workplace lockdowns enforced as a result of the COVID-19 pandemic. In 2020, 94 per cent of the world’s workers lived in countries that had some such measure in place for health and safety reasons (ILO 2020). Governments and organizations are still trying to find ways to enable workers to return to work safely.

International human rights law considers health to be a human right.¹ Hence, as van Kolfschooten and de Ruijter (2020) argue, governments have a

---

* School of Law, University of Tartu, email: seili.suder@sm.ee (corresponding author).
** Institute of Social Studies, University of Tartu, email: andra.siibak@ut.ee.

¹ See United Nations, International Covenant on Economic, Social and Cultural Rights, adopted in New York, NY, 16 December 1966, Treaty Series, Vol. 993: 3, Article 12(1).

Responsibility for opinions expressed in signed articles rests solely with their authors, and publication does not constitute an endorsement by the ILO.

This article is also available in French, in Revue internationale du Travail 161 (2), and Spanish, in Revista Internacional del Trabajo 141 (2).

Copyright © The authors 2022
Journal compilation © International Labour Organization 2022
legal obligation to take steps to protect the health of the public, including the need to control epidemic diseases. As COVID-19 is a contagious disease that spreads through close social interaction between human beings, contact tracing – the process of identifying, assessing and managing people who have been exposed to a disease – has become one of the most important mechanisms for containing the spread of the virus (WHO 2020). Manual contact tracing through interviews with infected individuals has been a typical public health response to contagious disease since its use during an outbreak of syphilis in the 1930s (McLachlan et al. 2020). However, this practice is slow and burdensome, requiring an immense workforce of health officials with the appropriate training. The method has several additional limitations, including low responsiveness (the time lag ensuing from the manual tracing process), limited data-processing capacity, oversights or omissions by respondents, and respondents’ inability to identify individuals in a crowd (Alsdurf et al. 2020; Watts 2020). Thus, in addition to manual contact tracing, digital contact tracing, especially various smartphone contact-tracing apps that enable real-time tracing of a massive number of (potentially) infected individuals (Kretzschmar et al. 2020; Yasaka, Lehrich and Sahyouni 2020), has increasingly been used to try to slow the spread of the virus (Oswald and Grace 2021; Watts 2020) and to enable employees to return to work. Although no evidence has been found about the effectiveness of automated tracing apps in reducing the numbers of infected cases or about the numbers of infected contacts identified (Braithwaite et al. 2020), many different app providers (including various health protection agencies, non-health agencies within a federal government or local government, health insurers, employers, non-profit organizations, and universities) are actively developing new kinds of COVID-19 response technologies.

Recent analyses provide insights into potential problems relating to the adoption of digital contact tracing. Many authors (cf. Spears and Padyab, forthcoming; Watkins 2021; van Kolfschooten and de Ruijter 2020) have investigated various concerns relating to privacy, including security and risks associated with the use of data (Newlands et al. 2020; Bradford, Aboy and Liddell 2020) and the ethical challenges of using public health surveillance technologies (Klar and Lanzera 2020; Luciano 2020). Besides scholars’ voicing of concerns about governments offering surveillance solutions (van Kolfschooten and de Ruijter 2020), app users have initiated actions against app developers and health departments following the exposure of sensitive personal data by COVID-19 contact-tracing apps (Davis 2021). However, less attention has been paid to employer–employee power relationships and to ubiquitous surveillance in workplaces (Xia 2021; Scassa 2021).

This article aims to contribute to these discussions by exploring ways in which employers can use digital contact-tracing apps and other monitoring tools in the context of the General Data Protection Regulation (GDPR) of the European Union (EU). The second section gives an overview of the use of contact-tracing apps and similar technologies in the workplace to mitigate the spread of COVID-19. The third section points out various concerns relating to the EU data protection framework (the applicability of the GDPR, legal grounds for data processing, data protection principles and data protection impact assessment). The fourth section concludes.
2. Options for limiting the spread of COVID-19 in the workplace

Mitigating the spread of COVID-19 in a workplace is the responsibility of the employer. The fact that employers must maintain safe workplaces and prevent work-related injuries and illnesses means that employers are required to limit and, if necessary, track the cases of COVID-19 that arise in work settings. This responsibility is reflected, for instance, in guidance for reopening businesses issued by the White House and the Centers for Disease Control and Prevention (CDC) (2020), which includes a call for employers to “monitor workers”. In deciding how to manage COVID-19 detection and control in a workplace, employers have several options, including contact-tracing apps developed at the national level and various solutions generated at the organizational level.

2.1. Contact-tracing apps implemented at the national level

Given that the chances of becoming infected with COVID-19 increase through prolonged and close contact with an infected person, estimates of proximity and the duration of contact are important pieces of information to limit the spread of the disease. This information can be gathered using smartphones, since they keep track of location (via global positioning system (GPS) technology and Wi-Fi connections) and use built-in Bluetooth interfaces that allow communication with and the detection of proximity to other nearby smartphones (Ahmed et al. 2020). Widespread ownership and the above-mentioned features have made smartphones ideal for automated contact tracing. The prime function of contact-tracing apps is to exchange information when the phones of two people are in close proximity, and to inform individuals should it transpire that their counterparts were infected with COVID-19 at the time of contact (Azad et al. 2021). Although the first mobile health apps for public monitoring and surveillance, as well as for improving patient care and health worker safety, were created during the Ebola pandemic in 2014–16 (Chen et al. 2017; Perscheid et al. 2018), there has been a surge in smartphone contact-tracing app usage during the COVID-19 pandemic (Ahmed et al. 2020; Ravindranath 2020). For example, most countries in the EU have launched digital contact-tracing apps (European Commission 2020a).

Employers might think that it is reasonable to require their employees to download a government-launched contact-tracing app, since such apps are free and widely available in almost every country. Such a requirement, however, will also mean that employees will always need to carry their phones with them at work, with the app running. If an employer requires that employees use these apps, there are several practical issues to consider, such as determining on which device the app will be installed and, if the app is installed on a personal phone, checking that the app has indeed been installed. Employers may pre-install apps on employer-issued devices, but they cannot force their employees to install government apps on their personal devices and they have little power to force employees to actively review – much less use – any information that these apps provide.

The European Commission (2020a) has stated that the use of national-level contact-tracing apps should be voluntary in EU Member States. Therefore, users
have the option not to install the apps if they have concerns about privacy. Nevertheless, in many EU countries there are fears that contact-tracing apps may become mandatory if employers require their use as a condition for either returning to work or entering work premises (Scassa 2021). Given that it is unlikely that such apps would be voluntarily adopted extensively within a workplace, we argue that many employers may want to encourage more active adoption to increase the apps’ efficiency. It is likely that many organizations will promote such apps among their employees as part of their health and safety strategies and highlight the benefits of everyone using them (Chesler 2020; Reuters 2021). Beyond the EU, some countries allow employers to decide whether to make contact-tracing apps mandatory in the workplace. In the United States, for example, employers are permitted to require employees to use a contact-tracing app as a condition of employment (Brown et al. 2020; Bodie and McMahon 2021). In India, the contact-tracing app Aarogya Setu was made mandatory for government and private sector employees, some of whom need to download the app in order to access their workplace or get paid (Ghoshal 2020). However, not all countries are willing to allow employers this power. For instance, Australia has passed legislation that prevents private sector actors from making the use of contact-tracing apps mandatory.\footnote{Parliament of Australia, Privacy Amendment (Public Health Contact Information) Act 2020, No. 44, 2020, \textit{Bills Digest}, No. 98.} For their part, not all employers see the benefits of government contact-tracing apps. Employees from several organizations (including banks and transport companies) in the United Kingdom have voiced concerns that their employers are putting them at risk by instituting rules that require employees to leave their mobile phones in their lockers or to deactivate their apps while at work, thereby preventing them from using the National Health Service (NHS) COVID-19 contact-tracing app. In most cases, the employers justify this requirement by claiming that they already have strict protective measures against COVID-19 in place and thus see no need for an additional preventive tool (Clements 2020). Often these requirements have come as a result of “false alerts” that ask people to self-isolate and cause concern and stress among colleagues (Clements 2020). According to the National Association of Schoolmasters/Union of Women Teachers, teachers in the United Kingdom were advised either to switch off the app or to disregard any self-isolation alerts (Webber 2020). The National Police Chiefs’ Council in the United Kingdom also confirmed that police officers were being told not to install the NHS COVID-19 app on their work smartphones and that some were also being advised not to obey self-isolation alerts generated by the app when downloaded to their personal phones (Cellan-Jones 2020).

### 2.2. Employer-based technological solutions

Some potential problems concerning the effectiveness of contact-tracing apps (Klar and Lanzerath 2020) could be solved by means of custom-built solutions. In other words, employers have the option of building their own app, sourcing one from app developers or subscribing to workplace contact-tracing systems
offered by private companies. Some of these employer-based tracing apps (for example, Shield for Business by Onspota, and the Employee Contact Tracing Tool by Kronos) help employers track possible virus exposure in work premises by collecting data on workers’ locations, movements and proximity to others. Siemens has a contact-tracing tool that monitors where infected employees have been, whom they have come into contact with and on which floors of an office they may have spread the virus. In addition to identifying potential exposure to the virus, the system can be used to decide which rooms need deep cleaning and where to institute social-distancing rules (Chesler 2020). Several banks apply strategies in which rotating shifts of people pass through buildings on different days, without clustering in the same areas, in order to avoid contagion. At the time of writing, J.P. Morgan, HSBC and Deutsche Bank were planning to launch reservation apps and online systems that use algorithms and artificial intelligence to book office seats. Such apps can use card-swipes at security turnstiles to identify patterns and suggest when someone should book a desk. Furthermore, the data can tell companies when an office or entire floor is empty in order to determine when to turn off lights, cancel janitorial services or downsize office space (Reuters 2021). Apps can also be set up to activate and start contact tracing only within certain GPS coordinates, and then to deactivate once one is outside (Watkins 2021). For example, the app Blip generates a geofence – a virtual boundary – that detects when an employee enters and leaves an area. The app registers a signal from the worker’s phone so the employer can tell whether and for how long the employee is on site. It only registers employees’ locations when they enter and exit the geofence and it does not track their specific movements (Johnson 2021).

A diverse range of technologies (Ponce Del Castillo 2020), gathering varying amounts of different data, are being developed and marketed to employers (Scassa 2021). Some employer-focused COVID-19 technologies are based on questionnaires (for example, COVID-stop Manager by HeBA), whereas others focus on physical distancing (for example, COVID Radius by Rombit). Often these technologies utilize workers’ health data and enable employers to gather specific information about infected employees (as in the case of the Infectious Disease Tracking Tool by Vivid Learning Systems – since acquired by HSI). In these cases, employees are usually asked to self-report their health symptoms and status (Adams 2020) and the system generates a risk level for the workers based on their responses (KMWorld 2020). Organizations can use the QR-code-based check-in app hPass, which requires individuals to pass a symptoms quiz before entering a facility. Another app, SaferMe, as well as prompting daily self-reporting on health symptoms, uses the Bluetooth and GPS features of employees’ smartphones to automatically record close contacts between staff and lets them manually enter the contact details of other people, including clients (Haskins 2020). If any staff report COVID-19 symptoms the app will generate alerts identifying the colleagues they have directly or indirectly encountered. The app Oura can record body temperature, resting heart rate, respiratory rate and other health-related elements and will not only alert employees to changes in their biometric measurements but also predict potential infection with COVID-19, since this may be indicated by an increased respiratory rate (Eckel 2021).
Employers may also purchase different wearables that conduct contact tracing (for example, the wearables developed by Estimote). Some of these use location-tracking and proximity sensors and allow employees to change their health status in the dedicated system. This information is sometimes stored in a health dashboard that provides detailed logs of possible contacts that are shared with the employer (Etherington 2020). Employees may also wear a sensor that is designed to immediately inform them of a risk (by flashing, vibrating and escalating to auditory alerts) when people walk too close to one another. Some manufacturers, for example in Germany and the United States, are making use of sensors operating within bracelets or pocket clips that notify people when they get too close to another employee (Leswing 2020). If an employee tests positive for COVID-19, the employer can see who they have been in contact with by looking at sensor data (Towers-Clark 2020). Lanyards that track employees’ proximity to readers placed beside door thresholds, soap dispensers and sinks enable employers to record when workers enter and exit rooms and whether they have washed their hands (Bittle 2020). Employers also have the option of adopting already existing tracking or surveillance technology for contact tracing; they may repurpose technologies such as cameras and digital badges for health and safety purposes, monitoring where employees have been and with whom they have had contact. For example, badges that allow access to workplaces can be used to determine who might have been in a specific room at the same time as an infected person. Some employers are also integrating artificial intelligence software into existing security cameras to count bodies in a room, track employee compliance with social-distancing and mask-wearing regulations and send alerts when employees are not practising social distancing (Reuters 2021; Dave 2020). Employers may also combine different technologies used in a workplace to access multiple data sources and gain comprehensive insights across an entire company to reduce virus transmission. Given that the power imbalance in the employment relationship puts employers in a strong position to require that workers use apps or other technologies serving health and safety purposes, contact tracing is easier to implement in a workplace than elsewhere. The use of various technological solutions may help employers create effective contact-tracing programmes and reinforce social-distancing practices as part of a digitized work environment. However, this leads to an inevitable increase in surveillance in the workplace. Although such technological tools have been accepted during a time of crisis, they may be problematic in a post-pandemic work environment. It may be easier to implement mandatory COVID-19 surveillance technologies in the workplace than elsewhere, but the use of such technologies could lead to significant privacy, ethical and human rights issues (Luciano 2020; Scassa 2021). Furthermore, each of these technologies presents country- and region-specific challenges from a data protection and employment law perspective.

As the EU has one of the newest and most substantial data protection frameworks in the world, the next section concentrates on the GDPR and how it provides for the protection of individuals whose data are collected for the purposes of limiting the spread of COVID-19.
3. Scope for employee contact tracing under the GDPR

Recent scholarship (for example, Guinchard 2021) has focused on the lack of adequate safeguards to deal with the huge data trove created by the use of contact-tracing apps. The primary concern among scholars (for example, Ahmed et al. 2020) is the extent to which the apps can be repurposed to track their users, and how the collected data may be used when the current pandemic ends. Vitak and Zimmer (2020) even argue that governments must look beyond the near-term privacy-preserving steps taken by some app developers (such as Google and Apple) and seriously reflect upon the possible future impacts that these technologies may have on broader moral and political values. These concerns are also the reasons why regulators, national data protection authorities, and scholars have started to issue guidelines and recommendations to app developers and content creators to help them improve the development of their products in terms of security and privacy (CDC 2020; European Commission 2020b; Azad et al. 2021). Meanwhile, the European Data Protection Board (EDPB) has adopted guidelines within the EU on the use of location data and contact-tracing tools in the context of the COVID-19 pandemic (EDPB 2020a).

Far less attention has been paid within the EU to workplace settings where employers are readily using contact-tracing technologies to mitigate the spread of COVID-19. Given the increased workplace surveillance through contact-tracing technologies, it is also necessary to consider whether the GDPR is fit for purpose in the employment context. Moreover, the advice given by the EDPB on contact tracing in the workplace has been quite general (European Data Protection Supervisor 2020). During the COVID-19 pandemic, the GDPR has been both praised and criticized in regard to contact-tracing apps. For example, the UK Labour MP and Chair of the Joint Committee on Human Rights, Harriet Harman, branded the GDPR as wholly inadequate for ensuring the security and privacy of data collected by the UK Government’s COVID-19 contact-tracing app (Scroxton 2020). Scholars, however, have stated that the EU data protection legal framework was designed to be sufficiently flexible to allow both an efficient response in limiting a pandemic and also the protection of fundamental human rights and freedoms (Kędzior 2021; Bradford, Aboy and Liddell 2020). In the following sections, we will analyse the data protection issues that are relevant to the use of different contact-tracing solutions at workplaces in the EU.

3.1. Applicability of the GDPR

If an employer processes employees’ personal data, collected through contact-tracing technologies within the EU or the European Economic Area, compliance with the GDPR needs to be considered. Tracing apps and other technologies

---

3 The GDPR does not apply in the United Kingdom following the end of the Brexit transition period on 31 December 2020. However, the UK Data Protection Act 2018 enacted the GDPR’s requirements into UK law and, with effect from 2021, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 amended the Data Protection Act 2018 and merged it with the requirements of the GDPR to form a new, UK-specific data protection regime (see https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr).
intended for use within this area need to follow the GDPR. For the GDPR to be applicable, an employer’s activities need to amount to the processing of employees’ personal data. Personal data are defined in the GDPR as “any information relating to an identified or identifiable natural person” (Article 4(1), GDPR). Therefore, in order for the GDPR to be applicable, apps have to provide information that is linked to an employee and can, on its own or combined with other information, lead to the identification of that employee. In the case of contact-tracing solutions, the question of personal identifiable data can be crucial, given that an employer may or may not have access to personal data, depending on the type of technology used. The applicability of the GDPR depends on what data are accessible to the employer and in what form the data are collected and stored.

Contact-tracing apps and other technologies employed to mitigate the spread of COVID-19 gather a variety of data. More conventional personal data may include identity data, such as the user’s name, address, gender and contact details. Contact-tracing apps and other technological solutions may also process health data (for example, whether or not the user has tested positive for the virus) and location data or social/proximity graphs that indicate interactions between users and the people with whom they have come into close contact (Ahmed et al. 2020). For instance, Onspota’s Shield for Business app allows organizations to decide what employee data are collected for the purposes of identification. Some companies ask that employees be identified by name and phone number, whereas other companies want their employees identified only by a number. Employees are notified on the app if they have met someone who has tested positive for COVID-19, but are only given the location and time of contact, not the contact person’s name. Only employees working within the organization are notified (Shemer 2021).

Employers may also receive general information, such as a risk analysis of a specific room or workplace (the locations of users who test positive for COVID-19 will show up as high-level hotspots for COVID-19 infection) and the overall health status of the workforce (indicating, for instance, the departments in which people are experiencing COVID-19 symptoms). A contact-tracing system may also record the presence of a person in a specific room. Thus, if traced employees perform their tasks in a specific workplace, tracing technologies that monitor location may be used to determine those employees’ identities. Therefore, we argue, various technological solutions can make personally identifiable information available to employers (especially if the app/wearable has been developed in collaboration with an employer or has been sourced specifically for contact tracing in a workplace) and trigger the applicability of the GDPR.

However, depending on the user or the architecture and the salient features of an app (see Azad et al. 2021), employers may not receive personal information about employees. For example, some contact-tracing apps using Bluetooth technology broadcast anonymous “chirps” or “keys” on a phone. These keys change frequently, possibly every few minutes. If two phones running an app come into close enough contact for long enough, the two phones exchange keys (Brown et al. 2020). Scholars have analysed whether these unique identifiers, although encrypted, could be linked to a particular person and thereby meet the GDPR definition of personal data (Bradford, Aboy and Liddell 2020). The
applicability of the GDPR will not be triggered unless the employers receive these unique identifiers. Therefore, a more privacy-friendly option is to use a COVID-19 tracing app in which a randomly generated identifier is assigned to the user that does not reveal any personal information. The app should send data only to its servers and not to any other destinations (Watkins 2021).

3.2. Controllers of data

In the context of the GDPR, the concepts of controller, joint controller and processor are crucial, since they determine who is responsible for compliance with different data protection rules, and how data subjects can exercise their rights (Bradford, Aboy and Liddell 2020). To ensure accountability, the controller of any contact-tracing application should be clearly defined. If employers opt to use their own technology, as opposed to government apps, they will likely be the controllers of the app and have greater data protection responsibilities with respect to any data generated by the app. For example, a spokesperson for contact-tracing app maker BrightHR, which is based in the United Kingdom, indicated that, although the app collects data, those data belong to “the customer organization” – in other words, to the company using the app – and are thus subject to the company’s own policies (Johnson 2021). As a controller, the employer has to follow the rules of the GDPR (for example, by providing a legal justification for data collection and following the principles of data processing). The controller has to choose processors (app developers) who can demonstrate compliance with data protection by design. Thus, employers should have data processing agreements in place with the providers of contact-tracing apps if they hold or have access to data collected via the app on their behalf, including an obligation to ensure that data are kept safe and secure by the app providers. Hence, collaborations between app developers and employers need to respect the rules set out in the GDPR (such as those found in its Article 28).

Unfortunately, the roles of controller and joint controller are not always clear-cut if an employer uses contact-tracing technologies that are developed by the government or by large corporations and are meant for wider use. In the case of government apps, national health authorities should be the controllers of personal data, since they determine the purposes and means of data processing. However, the role of controller may be carried out by others. If the deployment of contact-tracing apps involves different actors, their roles and responsibilities must be clearly established from the outset and explained to the users (EDPB 2020b). For example, employers may wish to make use of government contact-tracing apps to protect the health and safety of their workers and clients. One way of doing this is to ask employees whether they have the app installed on their smartphones and, if so, what their status is (that is, whether they have received an exposure alert). We argue that the extent of an employer’s responsibility for privacy in relation to such apps depends on what role the employer plays. Where employers rely on their employees to voluntarily pass on relevant information generated by government contact-tracing apps, they are probably not the controllers of the data under the definition of the GDPR, given that they do not determine the purposes and means of the processing. However, the role of employers inevitably becomes more complicated if they insist on workers
downloading and using government apps for workplace safety. In this case, the employers take on a more active role by determining the purpose and means of the data processing and therefore become controllers within the definition of the GDPR. The EDPB guidance on the concepts of controllers, processors and joint controllers (EDPB 2020b) should, therefore, provide greater clarity on this question; if employers start to require the use of government contact-tracing apps in a workplace, they may fall into the role of joint controllers.

3.3. Justifications for processing

Most data protection authorities in the EU stress that under employment law employees are obliged to inform the employer if they suspect they have been exposed to COVID-19 or if they have been diagnosed with it and are a threat to others in the workplace (Suder 2021). Some data protection agencies also suggest that employers should raise awareness and invite employees to provide information to the employer regarding possible exposure (Suder 2021). Therefore, in most EU Member States an employer should be able to ask employees to disclose whether they have received an exposure alert from a contact-tracing app. In this case, the employer must rely on employees’ self-declaration of exposure to infection. We argue that, although experts in the EU (EDPB 2020a) generally state that it is advisable to use contact-tracing technology on a voluntary basis, nothing in the GDPR prohibits employers from using this technology if they have legal grounds for data processing and follow the principles of data protection. In our opinion, employers may therefore strongly encourage or require employees to download and use relevant apps to reduce the spread of the virus. This will likely require an occupational health and safety risk assessment indicating that a measure, such as the use of an app, would help safeguard the workforce and customers within the workplace. Contact-tracing apps should also complement other measures taken to help reduce the spread of the virus.

3.3.1. Legal grounds for data processing

The EDPB (2020a) declares that location data collected from electronic communication providers, such as app developers, may only be processed in accordance with the ePrivacy Directive (Articles 6 and 9). This means that such data can only be transmitted to authorities or other parties (such as employers) if the provider has anonymized the data or, in the case of data (that are not traffic data) indicating the geographic position of a user’s terminal equipment, with the user’s prior consent. For this reason, contact-tracing apps should not collect data without the end user’s consent. However, the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that consent is necessarily the legal basis for data processing at work (EDPB 2020a). Under the GDPR, employers need a lawful basis to justify data processing (whether they are processing location data or other personal data).

---

4 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), Official Journal of the European Union L201: 37–47, 31 July 2002.
Personal data processing is allowed only under the exhaustive list of legal conditions mentioned in the GDPR (Article 6). These conditions are relevant because they are a precondition for processing employees' personal data; failure to meet them renders the processing unlawful. Possible legal justifications that employers may use during the COVID-19 pandemic have been suggested by the EDPB, national data protection authorities, and researchers (Suder 2021; DSK 2020; Nemzeti Adatvédelmi és Információszabadság Hatóság 2020).

According to the EDPB, the GDPR provides several legal justifications for companies to process personal data during the COVID-19 pandemic without the consent of the data subjects (EDPB 2020c). Employers may process employees' personal data if such processing is necessary for the employers to comply with their “legal obligations” (obligations relating to health and safety at the workplace) or necessary for the “public interest” (in this case, the need to control a disease and limit threats to health). As these legal justifications need to be laid down by EU or national law, the EDPB also reminds employers that they are required to process personal data in accordance with national law (EDPB 2020d). For example, the United Kingdom required certain organizations to collect customer, visitor and staff contact details for contact-tracing purposes during the COVID-19 pandemic (UK Health Security Agency 2020).

Employers may also process employees’ data if it is “necessary for the purposes of the legitimate interests pursued by the controller” (Article 6(1)(f), GDPR). In this case, organizations need to perform legitimate interests assessment to verify whether the interests linked to the purposes pursued through data processing override the rights, freedoms or legitimate interests of the employee. Research suggests that it is reasonable to assume that the collection of employee data during the COVID-19 pandemic is aligned with employees' individual interests in terms of their well-being, so it is unlikely that there will be any overriding compelling individual rights that invalidate the processing of those data (Suder 2021).

In addition, “the vital interests of the data subject or of another natural person” (Article 6(1)(d), GDPR) are another possible legal basis mentioned by the EDPB and EU data protection agencies (EDPB 2020c; DSK 2020). Recital 46 of the GDPR recognizes that in exceptional situations, such as an epidemic, the legal basis for processing activities can be of “vital interest”. It can be argued that this basis should be interpreted in the broadest possible way to justify the “processing of personal data aimed at protecting all those persons susceptible to being infected in the spread of an epidemic”, such as employees and clients at a workplace (Agencia Española de Protección de Datos 2020). However, others have been hesitant to use “vital interest” as a legal basis for data processing during the COVID-19 pandemic, since its use should take into consideration the real circumstances in a country or a region and, among other factors, look at infection rates among the population (Autorité de protection des données 2020).

3.3.2. Legal grounds for processing health data

If personal data fall within the category of health data (relating to COVID-19 symptoms or notification of a possible exposure to the disease, among other things), a further condition under the GDPR must be satisfied (Article 9). Employers may
process an employee’s health data only in exceptional cases, given that health data fall into special categories of personal data and require specific protection. However, guidance provided by the EDPB and national data protection agencies indicates that, even if only restricted processing of health data is possible, such data can still be processed to protect one’s employees. Employers are granted such a right in the case of substantial “public interest in the area of public health” (Article 9(2)(i), GDPR), on the basis of EU or national law (EDPB 2020a). Employers may rely on this condition to justify the processing of health data relating to COVID-19 if they are executing explicit instructions and acting on the advice of competent authorities (Autorité de protection des données 2020; DSK 2020; Agencia Española de Protección de Datos 2020). However, most data protection agencies in the EU (see Suder 2021; DSB 2022) suggest that employers may process health data if the processing is necessary for the purposes of carrying out their obligations and exercising specific rights in the field of employment, in so far as this is authorized by EU or Member State law. In this case, the authorization arises from the employer’s obligation to protect employees against occupational hazards and to take necessary measures to maintain a safe working environment.

Furthermore, the processing of health data is also lawful when the employee makes the data public. For instance, when an employee voluntarily publishes that they have COVID-19, their employer may lawfully process such data. However, we believe it should be stressed that telling a few colleagues about one’s illness is not the same as making the information public, and employers need to take this into consideration.

As will be evident, employers have several possible legal justifications for processing employees’ personal data through the use of various technologies implemented in the workplace. However, in our opinion, the wide range of possibilities causes confusion. It seems that employers in different EU Member States have several ways of processing employees’ data, but that national data protection authorities and the EDPB have only provided general guidance on the topic. Despite the different legal bases suggested by these authorities, employers still seem to prefer the “easiest option”: obtaining the employee’s consent. However, this legal basis is fraught with potential hurdles, as we discuss below.

3.3.3. Consent

One way of introducing contact-tracing apps in the workplace is to obtain freely expressed consent from employees. However, scholars have argued that consent is meaningless in circumstances where a data subject requires a certain benefit (Belli, Schwartz and Louzada 2017). Owing to the imbalance of power that exists in the employment relationship, consent is likely to turn into an empty and ritual process (Padi 2018). In accordance with the GDPR, consent “should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment” (Recital 42, GDPR). Therefore, employers should not be granted the opportunity to use their position to pressure employees into agreeing to download contact-tracing apps. The GDPR does not prohibit the use of consent in the employment relationship (Article 29 Data Protection Working Party 2017a), but it is up to the employer to demonstrate that consent to such monitoring is freely given.
If consent is used as a legal basis for downloading contact-tracing apps, this should be restricted to situations where the employee is genuinely able to exercise free choice without any negative consequences (Article 29 Data Protection Working Party 2017a). Under the GDPR, when assessing whether consent is freely given, it is necessary to consider, inter alia, whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (Article 7(4)). This provision anticipates an employment situation in which an offer is made on a “take it or leave it” basis (Mangan 2018). Employment should never be made contingent on consenting to download a contact-tracing app. If the employee refuses to download an app, dismissal upon these grounds could be judged unlawful. However, we have to take into consideration that refusing consent is often complicated in an employment relationship. For example, refusing to use a key card that is used for contact-tracing can be difficult if the same card also gives access to the premises. Therefore, employers should offer employees different options to mitigate the risk of COVID-19. For instance, Onspota, which developed the Shield for Business app, also offers employees who do not consent to using the app an alternative solution, involving scanning various QR codes across the factory floor (Shemer 2021).

Sometimes, it is also difficult to refuse consent because to do so is seen as somehow “abnormal” (Poullet 2009). Colleagues who have downloaded the app can set a trend for others, thus reducing scepticism towards the technology (Gauttier 2019) and generating a culture where employees are expected to endorse this solution. We argue that the widespread use of apps, peer pressure and the different affordances provided by an app and by the infrastructure in a workplace act as triggers for the adoption of contact tracing and thus can have an impact on the quality of the consent given by the employee. In consequence, employees may not be able to make a calculated and rational decision about contact tracing and may be pressured into agreeing to solutions offered by the employer.

Voluntary contact tracing requires informed consent, and consent requires a clearly defined scope of action; in other words, consenting employees need to have relevant information so that they know to what they are consenting (Mitrou 2018). In the case of contact tracing, an informed decision is hard to make. Informed consent should include proper knowledge of the use that will be made of the data from the app, the placement of any sensors to trace employees’ movements, and whether the data received from the app are combined with other data. Furthermore, attempts to meaningfully inform employees may be inadequate. Research suggests that highly technical, long and complex privacy notices or policies often fail to inform data subjects about the true nature of data-processing practices (European Commission 2011). Even in the case of organizational guidelines and policies, employees may still not be sufficiently informed to give informed consent (Suder and Siibak 2017). Often, such policies do not provide clear information about what and for what purposes data are collected, how the data are analysed and what decisions result from analyses of those data (Solove 2013). Moreover, in an effort to avoid liability and to consider the future use of the data, employers may draft vague privacy policies to cover
any unforeseen eventualities of processing (Padi 2018). We argue that consent gathered by such privacy notices and policies is meaningless, since broad and vague information fails to genuinely inform the employee about all aspects and consequences of the contact-tracing technology. As employers do not usually develop apps themselves, they often do not know much about how the data are collected, stored, shared or used (Johnson 2021), and hence are not able to communicate this information to their employees.

3.4. Principles of data protection

The deployment of new applications and the intensified use of existing technologies to tackle the COVID-19 pandemic exacerbate the need to revisit the data protection principles of the GDPR (Article 5, GDPR). Researchers have indicated that these principles are key to the successful deployment and adoption of these technologies (Newlands et al. 2020). Furthermore, most EU data protection agencies (see Nemzeti Adatvédelmi és Információszabadság Hatóság 2020) emphasize the importance of abiding by general principles of data processing in the context of COVID-19. This section looks at a few of these principles in the light of their vital importance in relation to contact-tracing apps.

If an employer uses contact-tracing technologies, the collection of any personal data should meet a specific purpose that is duly communicated to employees. The precise purposes will depend on the functionalities of the app. Therefore, the purposes of data processing must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis, such as to monitor the behaviour and performance of employees. Examples of illegitimate further processing include repurposing cameras installed to prevent the spread of COVID-19 in the workplace to monitor how employees are performing, how much time they are spending at their workstations, and which colleagues are participating in meetings. In our opinion, the concern is that contact-tracing apps will increase the amount of data generated in the workplace environment. This may lead employers to use technologies for purposes other than those originally planned, in activities constituting illegitimate further processing of workers’ data. Hence the risk of “function creep” and the use of data for purposes unintended by the data subject. For example, data initially used for contact tracing could potentially be later used to check employees’ attendance and their use of work and break time (see Johnson 2021). Such concerns have led both EU data protection agencies (see DSK 2020) and researchers (Gasser et al. 2020) to emphasize that digital surveillance and measures to combat the COVID-19 pandemic need to cease at the end of the health crisis (or when the pandemic has been sufficiently contained). Any personal data collected as part of these measures must be deleted once they no longer serve their initial purpose. This means, for instance, that a contact-tracing app should be discontinued once the pandemic has been contained and any stored personal data should be destroyed. Some authorities managing tracing apps have indicated that the app data collected will be removed once the app system is deactivated at the end of the pandemic (Ahmed et al. 2020). However, “end of the pandemic” is a vague deadline. There is no clear picture of what will happen to workplace technologies after the virus has receded.
The European Commission has emphasized that contact-tracing apps should collect the minimum amount of data required (European Commission 2020a). According to the EDPB, a contact-tracing application should not collect unrelated unnecessary information, such as individual user locations when proximity data can be used instead (EDPB 2020a). Similarly, the amount of contact-tracing data processed by employers should be strictly limited. Azad et al. (2021) indicate that a number of contact-tracing apps request permissions that may not be required for the successful operation of the app’s function (for example, access to storage media, cameras and microphones). It is also worth noting that we live in a digital ecosystem where many of the innovative digital technologies that individuals use have been developed in direct opposition to the core legal principles of data protection. Instead of limiting data processing to the minimum needed to provide a service, a number of businesses collect as much data as possible. Many health apps violate the GDPR by collecting far too much data for too long, without transparency and without securing the data (Guinchard 2021). It is therefore essential that contact-tracing apps used in the workplace do not have similar tendencies.

As will be evident from the above, there has been a lot of discussion about different data protection principles. However, one principle in particular – the principle of fairness – seems to be forgotten in wider discussions. In order to ensure fair and transparent processing as regards employees, the employer should take into account the specific circumstances in which personal data are processed (Recital 60, GDPR). Vitak and Zimmer (2020) have indicated that the appropriateness of sharing data with third parties (namely, employers) to support public health in the context of COVID-19 depends on the context. They argue that if we ignore this contextual integrity we risk the long-term loss of autonomy and growing function creep across a wide range of technologies. Therefore, we believe, it is crucial that employers handle employees’ personal data from contact-tracing technologies only in ways that could be reasonably expected by the employees and that employers do not, without justification, use the information in a manner that has a negative effect on employees. The harm that may arise from employers seeking information through contact-tracing apps is that of “informational injustice” (van den Hoven and Weckert 2008), where information presented in one context is used in another. For example, employees may be comfortable with data from contact-tracing apps being shared with health authorities or their health providers, but they may feel that it is inappropriate to share that same data with employers. Similarly, although individuals may be comfortable sharing their location with an app developer to receive contact-tracing services, they may not want such data to end up with employers to serve the long-term monitoring of their movements. We argue that employers need to consider the context when monitoring employees and to refrain from any unjustified actions, such as dismissing employees if they refuse to download a tracing app.

3.5. Impact assessment

Researchers have emphasized that compliance with data protection laws is not a box-ticking exercise to be undertaken after a digital technology has been developed (Guinchard 2021). Data protection by design requires both controllers and
processors to ascertain potential privacy risks before, not after, an app is rolled out. In the case of high-risk processing, such as health data processing, data protection impact assessments (processes to identify and address data protection and privacy risks) have become mandatory. They seek to mitigate risks and, if mitigation is not possible, to decide whether the processing should be conducted at all (Article 35, GDPR; Maddocks 2020). Similarly, the EDPB has stated that a data protection impact assessment must be carried out before contact-tracing tools are implemented, since “the processing is likely to result in a high risk to the rights and freedoms of natural persons” (Article 29 Data Protection Working Party 2017b, quoting Article 35, GDPR).\(^5\) The EDPB also strongly recommends the publication of such assessments. However, not all contact-tracing apps are accompanied by impact assessments, nor are such assessments readily available (Ahmed et al. 2020). Furthermore, little can be known about whether employers who encourage or require employees to download these apps have read the assessment made by the app’s developer or have even determined whether the developer has undertaken an assessment. Ultimately, if the employer uses contact tracing in the workplace, an impact assessment is required. For example, systems that track interactions between individuals and locations within a workplace and make that information available to the human resources department, or to the person managing the system, require a detailed data protection impact assessment to identify potential privacy risks.

4. Conclusion

During the COVID-19 pandemic, there has been much discussion about government contact-tracing apps. The possible actions of employers should also be a matter of great concern. The use of contact-tracing technologies is one way to protect health and safety in the workplace and to minimize absences owing to illness. While a contagious and deadly disease is spreading, worker safety is paramount and the use of contact-tracing apps and similar technologies may be crucial to halting contagion – and is, on that basis, justified in dealing with COVID-19. However, employers should have legal justification for such data processing, avoid function creep, have strong data minimization and destruction policies and ensure coherence with other data protection principles, such as fairness and transparency. In regard to the period that will follow the pandemic, there are concerns about invasive surveillance and further use of these technologies that need to be addressed.

The GDPR is a broad piece of legislation that provides rules for processing personal data gathered to deal with the kinds of problems posed by the COVID-19 pandemic. Indeed, the GDPR gives employers the legal basis to process personal data during epidemics. However, owing to the complex and vague rules relating to consent in the GDPR, contact-tracing technologies are likely to expand without clear direction, which may further erode employee privacy protection in the future. After the COVID-19 crisis is over and workplaces start returning to

---

\(^5\) Data processing is considered to be high risk if the employer is carrying out large-scale data processing or systematic monitoring of employees or is using new technological solutions for data processing.
some kind of normality, employees and employers will benefit from a clear and stable approach to contact tracing in the workplace. Owing to the imbalance of power between employers and employees, national laws are needed to strengthen employees’ ability to refuse to download contact-tracing apps or similar technologies, and to provide specific rules if such technologies continue to be used after the health crisis subsides. When the technology is no longer needed to keep employees safe, regulations and guidance should prevent its misuse by employers.

References
Adams, Ben. 2020. “PRA Health Sciences Unveils COVID-19 Monitoring App to Track Symptoms”. Fierce Biotech, 25 March 2020. https://www.fiercebiotech.com/cro/pra-health-sciences-unveils-covid-19-monitoring-app-to-track-symptoms.

Agencia Española de Protección de Datos. 2020. “Report from the State Legal Service (Detached Department of the SLS at the Spanish DPA) on Processing Activities Relating to the Obligation for Controllers from Private Companies and Public Administrations to Report on Workers Suffering from COVID-19”. Ref. 0017/2020. Madrid.

Ahmed, Nadeem, Regio A. Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S. Kanhere, Aruna Seneviratne et al. 2020. “A Survey of COVID-19 Contact Tracing Apps”. IEEE Access 8: 134577–134601.

Alsdurf, Hannah, Edmond Belliveau, Yoshua Bengio, Tristan Deleu, Prateek Gupta, Daphne Ippolito, Richard Janda et al. 2020. “COVI White Paper”, Version 1.1, 27 July 2020. arXiv:2005.08502.

Article 29 Data Protection Working Party. 2017a. Opinion 2/2017 on Data Processing at Work. WP 249. Brussels: European Commission.

———. 2017b. Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679. WP 248 rev.01. Brussels: European Commission.

Autorité de protection des données. 2020. “COVID-19 sur le lieu de travail”. September 2020. https://www.autoriteprotectiondonnees.be/professionnel/themes/covid-19/covid-19-sur-le-lieu-de-travail.

Azad, Muhammad Ajmal, Junaid Arshad, Syed Muhammad Ali Akmal, Farhan Riaz, Sidrah Abdullah, Muhammad Imran, and Farhan Ahmad. 2021. “A First Look at Privacy Analysis of COVID-19 Contact-Tracing Mobile Applications”. IEEE Internet of Things Journal 8 (21): 15796–15806.

Belli, Luca, Molly Schwartz, and Luiza Louzada. 2017. “Selling Your Soul while Negotiating the Conditions: From Notice and Consent to Data Control by Design”. Health and Technology 7 (4): 453–467.

Bittle, Jake. 2020. “Your Boss Wants to Know whether You Washed Your Hands”. Slate, 5 May 2020. https://slate.com/technology/2020/05/RFID-technology-handwashing-social-distancing-coronavirus-workplace.html.

Bodie, Matthew T., and Michael McMahon. 2021. “Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic”. Washington University Journal of Law & Policy 64 (1): 31–61.

Bradford, Laura, Mateo Aboy, and Kathleen Liddell. 2020. “COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes”. Journal of Law and the Biosciences 7 (1). https://doi.org/10.1093/jlb/lsa034.

Braithwaite, Jeffrey, Kristiana Ludlow, Luke Testa, Jessica Herkes, Hanna Augustsson, Gina Lamprell, Elise McPherson, and Yvonne Zurynski. 2020. “Built to Last? The Sustainability of Healthcare System Improvements, Programmes and Interventions: A Systematic Integrative Review”. BMJ Open 10 (6). http://dx.doi.org/10.1136/bmjopen-2019-036453.
Brown, Stephen R., Michael F. Linden, Emma J. Sullivan, and Joseph J. Torres. 2020. “May an Employer Require Its Employees to Use a Contact Tracing App?” Jenner&Block COVID-19 Coronavirus Resources, 24 April 2020. https://jenner.com/system/assets/publications/19870/original/May%20an%20Employer%20Require%20Its%20Employees%20to%20Use%20a%20Contact%20Tracing%20App.pdf?158801012.

CDC (Centers for Disease Control and Prevention). 2020. “Preliminary Criteria for the Evaluation of Digital Contact Tracing Tools for COVID-19”. 3 May 2020. https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/prelim-eval-criteria-digital-contact-tracing.pdf.

Cellan-Jones, Rory. 2020. “Police Told Not to Download NHS Covid-19 App”. BBC News, 28 September 2020. https://www.bbc.com/news/technology-54328644.

Chen, Yuanfang, Noel Crespi, Antonio M. Ortiz, and Lei Shu. 2017. “Reality Mining: A Prediction Algorithm for Disease Dynamics Based on Mobile Big Data”. Information Sciences 379 (February): 82–93.

Chesler, Caren. 2020. “Coronavirus Will Turn Your Office into a Surveillance State”. Wired, 4 May 2020. https://www.wired.co.uk/article/coronavirus-work-office-surveillance.

Clements, Laura. 2020. “Transport for Wales Is Telling Staff to Turn Off the NHS’ Contact Tracing App”. Wales Online, 15 December 2020. https://www.walesonline.co.uk/news/wales-news/transport-for-wales-coronavirus-staff-19453360.

Dave, Paresh. 2020. “Companies Bet on AI Cameras to Track Social Distancing, Limit Liability”. Reuters, 27 April 2020. https://uk.reuters.com/article/uk-health-coronavirus-surveillance-tech/companies-bet-on-ai-cameras-to-track-social-distancing-limit-liability-idUKKCN22916F.

Davis, Jessica. 2021. “PA Health Dept Sued; Investigation Looms, after Contact Tracing Breach”. HealthITSecurity, 10 May 2021. https://healthitsecurity.com/news/pa-health-dept-sued-investigation-loomsafter-contact-tracing-breach.

DSB (Datenschutzbehörde). 2022. “Information der Datenschutzbehörde zum Coronavirus (Covid-19)” [Information from the Data Protection Authority Concerning the Coronavirus (Covid-19)]. April 2022. https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html.

DSK (Datenschutzkonferenz). 2020. “Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie” [Press release – German Data Protection Supervisory Authorities Joint Information Paper on Data Protection in Connection with the Coronavirus Pandemic], 13 March 2020. https://www.datenschutzkonferenz-online.de/media/pm/20200325_Informations_zu_Corona_und_Arbeitgeber.pdf.

Eckel, Erik. 2021. “How the Oura Ring Health-Monitoring Wearable May Help Make Returning to the Office Safer”. TechRepublic, 9 April 2021. https://www.techrepublic.com/article/how-the-oura-ring-may-help-make-returning-to-the-office-safer/.

EDPB (European Data Protection Board). 2020a. Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak. Brussels.

———. 2020b. Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 1.0. Brussels.

———. 2020c. “Statement of the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak”. 16 March 2020. Brussels.

———. 2020d. “Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak”. 19 March 2020. Brussels.

Etherington, Darrell. 2020. “Estimote Launches Wearables for Workplace-Level Contact Tracing for COVID-19”. TechCrunch, 2 April 2020. https://techcrunch.com/2020/04/02/estimote-launches-wearables-for-workplace-level-contact-tracing-for-covid-19/?guccounter=1.

European Commission. 2011. “Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union”. Wave 74.3 (Report). Brussels: TNS Opinion & Social.
COVID-19 employee monitoring under the EU data protection framework

——. 2020a. “Mobile Applications to Support Contact Tracing in the EU’s Fight against COVID-19", progress report, June 2020. Brussels.
——. 2020b. “Communication from the Commission: Guidance on Apps Supporting the Fight against COVID 19 Pandemic in Relation to Data Protection – 2020/C 124 1/01”. Official Journal of the European Union C 124 I: 1–9.
European Data Protection Supervisor. 2020. “Orientations from the EDPS: Reactions of EU Institutions as Employers to the COVID-19 Crisis”. 15 July 2020. Brussels.
Gasser, Urs, Marcello Ienca, James Scheibner, Joanna Sleigh, and Effy Vayena. 2020. “Digital Tools against COVID-19: Framing the Ethical Challenges and How to Address Them”. Manuscript available online. https://arxiv.org/abs/2004.10236.
Gauttier, Stéphanie. 2019. “I’ve Got You under My Skin: The Role of Ethical Consideration in the (Non-)Acceptance of Insideables in the Workplace”. Technology in Society 56 (February): 93–108.
Ghoshal, Somak. 2020. “Open Book? In India, Where People Are Forced to Download a Tracking App to Get Paid, Journalists Are Worried about It Also Being Used to Access Their Contacts”. Index on Censorship 49 (2): 53–55.
Guinchard, Audrey. 2021. “Our Digital Footprint under Covid-19: Should We Fear the UK Digital Contact Tracing App?” International Review of Law, Computers & Technology 35 (1): 84–97.
Haskins, Caroline. 2020. “Workers Around the World Are Already Being Monitored by Digital Contact Tracing Apps”. BuzzFeed News, 30 May 2020. https://www.buzzfeednews.com/article/carolinehaskins1/coronavirus-private-contact-tracing.
ILO. 2020. “ILO Monitor: COVID-19 and the World of Work”, 6th ed., 23 September 2020. Geneva.
Johnson, Erica. 2021. “School Custodian Refuses to Download Phone App that Monitors Location, Says It Got Her Fired”. CBC News, 12 April 2021. https://www.cbc.ca/news/gopublic/tattleware-privacy-employment-1.5978337.
Kędzior, Magdalena. 2021. “The Right to Data Protection and the COVID-19 Pandemic: The European Approach”. ERA Forum 21 (4): 533–543.
Klar, Renate, and Dirk Lanzerath. 2020. “The Ethics of COVID-19 Tracking Apps: Challenges and Voluntariness”. Research Ethics 16 (3–4). https://doi.org/10.1177/1747016120943622.
KMWorld. 2020. “Pegasystems Creates Free App to Track COVID-19 Employee Exposure”, 24 March 2020. https://www.kmworld.com/Articles/ReadArticle.aspx?ArticleID=139909.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Janneke H. H. M. van de Wijgert, and Marc J. M. Bonten. 2020. “Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study”. The Lancet Public Health 5 (8): E452–E459.
Mitrou, Lilian. 2018. “Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof’?” Manuscript available online. http://dx.doi.org/10.2139/ssrn.3386914.

Nemzeti Adatvédelmi és Információszabadság Hatóság. 2020. “Information on Processing Data Related to the Coronavirus Epidemic”. NAIH/2020/2586. Budapest.

Newlands, Gemma, Christoph Lutz, Aurelia Tamò-Larrieux, Eduard Fosch Villaronga, Rehana Harasgama, and Gil Scheitlin. 2020. “Innovation under Pressure: Implications for Data Privacy during the Covid-19 Pandemic”. Big Data & Society 7 (2). https://doi.org/10.1177/2053951720976680.

Oswald, Marion, and Jamie Grace. 2021. “The COVID-19 Contact Tracing App in England and ‘Experimental Proportionality’”. Public Law, No. 1, 27–37.

Padi, Joel. 2018. “Big Data Analytics, Consent and the European Union (EU) General Data Protection Regulation 2016 (GDPR): The Fallacy of Consent and Control”. LLB dissertation, Keele University.

Perscheid, Cindy, Justus Benzler, Claus Hermann, Michael Janke, David Moyer, Todd Laedtke, Olawunmi Adeoye et al. 2018. “Ebola Outbreak Containment: Real-Time Task and Resource Coordination with SORMAS”. Frontiers in ICT 5 (7). https://doi.org/10.3389/fict.2018.00007.

Ponce Del Castillo, Aída. 2020. “COVID-19 Contact-Tracing Apps: How to Prevent Privacy from Becoming the Next Victim”, ETUI Policy Brief No. 5/2020. Brussels: European Trade Union Institute.

Poulet, Yves. 2009. “Data Protection Legislation: What Is at Stake for Our Society and Democracy?” Computer Law & Security Review 25 (3): 211–226.

Ravindranath, Mohana. 2020. “Coronavirus Opens Door to Company Surveillance of Workers”. Político, 26 June 2020. https://www.politico.com/news/2020/06/26/workplace-apps-tracking-coronavirus-could-test-privacy-boundaries-340525.

Reuters. 2021. “As Employees Return to the Office, Banks Explore Surveillance Tech”. VentureBeat, 21 May 2021. https://venturebeat.com/2021/05/21/banks-explore-sensors-cameras-monitoring-tech-as-workers-return-to-office/.

Scassa, Teresa. 2021. “COVID-19 Contact Tracing: From Local to Global and Back Again”. International Journal of E-Planning Research 10 (2): 45–58.

Sudor, Seili. 2017. “Employers as Nightmare Readers: An Analysis of Ethical and Legal Concerns Regarding Employer–Employee Practices on SNS”. Baltic Journal of Law & Politics 10 (2): 76–106.

Towers-Clark, Charles. 2020. “Is Contact Tracing a Public or Private Concern?” Forbes, 17 June 2020. https://www.forbes.com/sites/charlestowersclark/2020/06/17/is-contact-tracing-a-public-or-private-concern/.

UK Health Security Agency. 2020. “Guidance: Maintaining Records of Staff, Customers and Visitors to Support NHS Test and Trace” [Guidance was withdrawn on 24 February 2022]. https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace.
van den Hoven, Jeroen, and John Weckert, eds. 2008. Information Technology and Moral Philosophy. New York, NY: Cambridge University Press.

van Kolfschooten, Hannah, and Anniek de Ruijter. 2020. “COVID-19 and Privacy in the European Union: A Legal Perspective on Contact Tracing”. Contemporary Security Policy 41 (3): 478–491.

Vitak, Jessica, and Michael Zimmer. 2020. “More than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies”. Social Media + Society 6 (3). https://doi.org/10.1177/2056305120948250.

Watkins, Kevin. 2021. “Security and Privacy of COVID-19 Contact-Tracing Apps”. Symantec Enterprise Blogs/Threat Intelligence, 12 March 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/security-privacy-covid-tracing-apps.

Watts, David. 2020. “COVIDSafe, Australia’s Digital Contact Tracing App: The Legal Issues”. Manuscript available online. http://dx.doi.org/10.2139/ssrn.3591622.

Webber, Ashleigh. 2020. “Teachers Told to Disable NHS Contact-Tracing App, Claims Union”. Personnel Today, 17 November 2020. https://www.personneltoday.com/hr/teachers-told-to-disable-nhs-contact-tracing-app-claims-union/.

White House and CDC. 2020. Guidelines: Opening Up America Again. Washington, DC. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/04/Guidelines-for-Opening-Up-America-Again.pdf.

WHO (World Health Organization). 2020. “Contact Tracing in the Context of COVID-19: Interim Guidance”. 10 May 2020. Geneva.

Xia, Yang. 2021. “Workforce Survival: Tracking Potential COVID-19 Exposure amid Socioeconomic Activities Using Automatic Log-Keeping Apps”. Population Health Management 24 (2): 156–157.

Yasaka, Tyler M., Brandon M. Lehrich, and Ronald Sahyouni. 2020. “Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App”. JMIR mHealth and uHealth 8 (4). https://doi.org/10.2196/18936.