Journal of Law and the Biosciences, 1–5
doi:10.1093/jlb/lsaa008
Advance Access Publication 22 April 2020
Peer Commentary

Reporting, recording, and communication of COVID-19 cases in workplace: data protection as a moving target

Mahsa Shabani[1,*,†], Tom Goffin[2] and Heidi Mertes[3]

[1]Metamedica, Faculty of Law and Criminology, Ghent University, Ghent 9000-B, Belgium
[2]Metamedica, Department of Public Health and Primary Care, Ghent University, Ghent 9000, Belgium
[3]Metamedica, Faculty of Arts and Philosophy, Ghent University, Ghent 9000-B, Belgium
*Corresponding author. E-mail: mahsa.shabani@ugent.be

ABSTRACT

In response to concerns related to privacy in the context of coronavirus disease 2019 (COVID-19), recently European and national Data Protection Authorities (DPAs) issued guidelines and recommendations addressing a variety of issues related to the processing of personal data for preventive purposes. One of the recurring questions in these guidelines is related to the rights and responsibilities of employers and employees in reporting, recording, and communicating COVID-19 cases in workplace. National DPAs in some cases adopted different approaches regarding duties in reporting and communicating the COVID-19 cases; however, they unanimously stressed the importance of adopting privacy-preserving approaches to avoid raising concerns about surveillance and stigmatization. We stress that in view of the increasing use of new data collection and sharing tools such as 'tracing and warning' apps, the associated privacy-related risks should be evaluated on an ongoing manner. In addition, the intricacies of different settings where

† Mahsa Shabani (LL.M, PhD) is Assistant Professor in Health Privacy Law at Ghent University. Tom Goffin (PhD) is Assistant Professor in Health Law at Ghent University. Heidi Mertes (PhD) is Assistant Professor in Medical Ethics at Ghent University. All co-authors are a member of Metamedica platform at Ghent University which is an interfaculty platform on Law, Ethics and Policy of Innovation in Healthcare.

such apps may be used should be taken into consideration when assessing the associated risks and benefits.

KEYWORDS: data protection, privacy, pandemics, employment, COVID-19, regulation

In the wake of COVID-19 outbreak, concerns related to the lawful processing of personal information from COVID-19 cases have led various European and national DPAs to develop guidelines regarding personal data protection in the context of the COVID-19 outbreak. Notably, under the EU General Data Protection Regulation (GDPR), processing personal health-related data is subject to a higher protection, since health data are considered as sensitive data.[1] According to Article 9 (2) of the GDPR, sensitive data, including personal health-related data, can only be processed inter alia when data subject gives her/his explicit consent or when processing is necessary 'for reasons of public interest in the area of public health' on the basis of Union or Member State law.

One of the recurring questions in these guidelines has been related to the duties and responsibilities of employers regarding recording the COVID-19 cases and disclosing the relevant information to the staff for preventive purposes. In this context, the COVID-19 cases may refer to both confirmed and potential cases including symptomatic but not tested individuals or those being at a higher risk due to being in close contact with positive cases. While processing information from COVID-19 cases by public health authorities is justified on the basis of their legal mandate in preventing infectious diseases, there is diversity regarding whether employers should/may communicate COVID-19 cases to co-workers and how far identifying information including name(s) of the positive cases should/may be disclosed.

The guidance provided by the European Data Protection Board on March 19, 2020, asserts that 'Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (eg in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected'.[2] In any event, the principles of proportionality and data minimization should be fully respected in processing personal information from employees.

The guidelines issued by the national DPAs adopt different approaches regarding the duty of communication of COVID-19 cases to staff. For instance, while the UK Information Commissioner's Office states that employers 'should' communicate the COVID-19 cases to staff,[3] according to the Ireland and Belgium's DPAs, employers

1 Article 9 (2), EU General Data Protection Regulation. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

2 European Data Protection Board. Statement on the processing of personal data in the context of the COVID-19 outbreak. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (accessed Mar. 30, 2020).

3 Information Commissioner's Office. Data Protection and Coronavirus: What you need to know. https://ico.org.uk/for-organisations/data-protection-and-coronavirus/ (accessed Mar. 30, 2020).

'may' communicate the cases, when justified.[4,5] It is also interesting to note that according to the Netherlands' DPA, communicating the positive cases to staff is not a duty of employers.[6] This heterogeneity may be due to differences in national regulations regarding epidemiological surveillance and protocols regarding safety and risk management at the workplace.

With regard to the permissibility of disclosing personal information about the positive cases when communicating to staff, disclosing names of the cases has been generally disfavored and perceived to be unnecessary in many cases. The Danish DPA states that a number of points should be taken into consideration when deciding to disclose information from COVID-19 cases, including whether the recording or disclosing of information is justified and whether it is necessary to specify the information. In addition, account should be taken whether the purpose can be achieved by 'telling less' and whether it is necessary to name names—eg the name of the person infected and/or in the home quarantine. Therefore, employers are instructed to evaluate on a case-by-case basis whether disclosing the identifying information from individuals is necessary or not.[7]

It seems this approach is better suited for the realities of different workplaces. Thus, employers can adopt communication strategies based on the setting of the workplaces (the number of the employees, likelihood of direct contact, etc.) and strive to communicate information in a manner that protects the privacy of employees as much as possible. As disclosing the names of individuals may have stigmatizing effects, it is essential to adopt communication strategies that respect the privacy of the persons involved.

Closely related to this topic is the duty of potential or confirmed COVID-19 patients to report their test results/symptoms to their employers. For instance, the Netherlands' DPA asserts that such reporting should be only on a voluntary basis, while France and Luxembourg's DPAs assert that the employees who contracted COVID-19 should report to their employers.[8,9] Notably, a potential duty of the employees to report is closely related to the responsibilities of the employers in recording such cases and eventually communicating to staff and health authorities.

In the guidelines provided by the DPAs, it has been presumed that the management of personal information from employees and consequently the scope of communication of the COVID-19 cases would be effectively controlled by employers. In parallel, rapidly emerging mobile apps that, among others, aim for tracing and preventing the

4 Ireland Data Protection Authority. Data Protection and COVID-19. https://dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19 (accessed Mar. 30, 2020).

5 Belgium Data Protection Authority. Covid-19 and processing of personal data in workplace. https://www.gegevensbeschermingsautoriteit.be/covid-19-en-de-verwerking-van-persoonsgegevens-op-de-werkvloer (accessed Mar. 30, 2020).

6 Netherlands Data Protection Authority. Corona in Workplace. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/corona-op-de-werkvloer (accessed Mar. 30, 2020).

7 Denmark Data Protection Authority. GDPR and Coronavirus. https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/ (accessed Mar. 30, 2020).

8 France Data Protection Authority. Coronavirus (COVID-19): Remarks from CNIL on collection of personal data. https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles (accessed Mar. 30, 2020).

9 Luxembourg Data Protection Authority. Coronavirus (COVID-19): CNPD Recommendations relating to the Collection of Personal Data in a Context of a Health Crisis. https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html (accessed Mar. 30, 2020).

spread of the virus by potentially warning the exposed people offer novel opportunities that may also be used by employers to facilitate reporting and communication of the COVID-19 cases in workplaces. The potential benefits of using tracing and tracking apps have been highlighted in recent scientific literatures[10] and policy recommendations such as a recent European Commission Recommendation C(2020) 2296, which states 'expert opinion suggests that applications aiming to inform and warn users seem to be the most promising to prevent the propagation of the virus, taking into account also their more limited impact on privacy, and several Member States are currently exploring their use'.[11]

Thus, duties of reporting and the scope of communications of the positive cases may be considerably expanded beyond what has been originally foreseen in the relevant data protection guidelines. Employers may favor using apps by staff as it will allow recording and (partly) automating communication of positive cases in the workplace by sending direct notifications to those who are considered to be at a higher risk of contracting the virus. These apps have been already used in countries such as Singapore, South Korea, and Israel, and recently plans for using them in Germany, Belgium, and the UK have been announced.[12]

Use of tracing–warning apps in workplaces raises a number of privacy concerns. While use of such apps is generally considered to be voluntary,[13] their mandatory use in some settings such as workplaces may be justified on the basis of already existing duties and responsibilities for reporting and recording the (potential) COVID-19 cases. Additionally, risks of identifiability and privacy breaches may be higher when using apps in small workplaces. Most tracing apps are claiming that they are operating on the basis of anonymized data; therefore, their activities fall outside the scope of data protection regulations, such as the EU GDPR that only applies to directly or indirectly identifiable data. However, what one needs to take into account is that removing obvious identifiers (eg names, national registration number, etc.) does not always sufficiently address the concerns about identifiability, especially when reporting and notification take place in a setting comprising a small group of people. Moreover, accounts should be taken of general privacy-related concerns in using health-related

10 Ferreti, Luca et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. DOI: 10.1126/science.abb6936. 2020.

11 European Commission. Commission Recommendation C(2020) 2296 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf (accessed Apr. 9, 2020).

12 Standard. 'You have been possibly come in contact with an infected patient'. https://www.standaard.be/cnt/dmf20200327_04904961?articlehash=B2AE5A1C8CAE0AF4190A2E60906E41D0238CF28D0CAAB8B8D9038AE2E90F0603F109D181A832B022DEBD08D4BC6E32E843C60224E3D757FE4395A104C476CC62 (accessed Mar. 30, 2020). EU Privacy watchdog calls for pan-European mobile app for virus tracking. https://www.reuters.com/article/us-health-coronavirus-tech-privacy/eu-privacy-watchdog-calls-for-pan-european-mobile-app-for-virus-tracking-idUSKBN21O1KJ (accessed Apr. 9, 2020). How will the NHS COVID-19 app contact-tracing app work and when will it go live? https://tech.newstatesman.com/security/nhs-covid-19-contact-tracing-app-rollout (accessed Apr. 9, 2020).

13 German minister says tracking apps to tackle coronavirus must be voluntary. https://www.reuters.com/article/us-health-coronavirus-germany-app/german-minister-says-tracking-apps-to-tackle-coronavirus-must-be-voluntary-idUSKBN21I0KM (accessed Apr. 09, 2020).

apps which have been previously discussed in scholarly literatures and normative documents.[14]

In view of new possibilities that ICT offers in processing personal sensitive data,[15] it is imperative to consider assessment of the data protection concerns and adequacy of the proposed safeguards and guidance in the context of COVID-19 as a dynamic endeavor. Thus, data protection oversight bodies should be involved in the development of such apps from the beginning and publish their consultations publicly when possible. This is crucial for improving transparency and eventually maintaining public trust related to using such apps for processing sensitive health-related data. Recently, the importance of an ongoing evaluation and consultation by the relevant oversight bodies has also been stressed in the European Data Protection Supervisor's response to the European Commission DG Connect regarding monitoring the spread of COVID-19 by using data from telecommunication providers and the European Commission's Recommendation C(2020) 2296 (see above).[16] Notably, risks associated with processing of personal data may considerably evolve when new data collection and communication tools are being used.

Finally, regardless of whether monitoring and communication of COVID-19 cases in the workplace rely on apps or not, disclosing the identity of those infected should only happen on a need-to-know basis, in order to prevent stigmatization and privacy breaches. While it is expected that the current public health emergency would justify limiting the privacy rights of individuals temporarily, it is crucial to ensure that adequate safeguards are in place to mitigate potential risks for the individuals when collecting, reporting, and communicating their health-related information for preventive measures. As it has been stressed in the recent joint civil society statement on States use of digital surveillance technologies to fight pandemic, 'These are extraordinary times, but it's important to remember that human rights law still applies'.[17]

14 European Commission. Draft Code of Conduct on privacy for mHealth apps. https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised (accessed Apr. 9, 2020).

15 Ienca, M and Vayena, E. *On the responsible use of digital data to tackle the COVID-19 pandemic.* Nat Med. https://doi.org/10.1038/s41591-020-0832-5. 2020.

16 European Data Protection Supervisor. Monitoring Spread of COVID-19. https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf (accessed Mar. 30, 2020).

17 Amnesty International. Joint Statement: states use of digital surveillance technologies to fight pandemic must respect human rights. https://www.amnesty.org/en/documents/pol30/2081/2020/en/ (accessed Apr. 9, 2020).