



**COVID-19  
WATCH  
ETUC BRIEFING  
NOTE  
ON NEW  
TECHNOLOGIES  
ALLOWING MORE  
SURVEILLANCE AT  
WORK  
30 SEPTEMBER 2020**

## **COVID-19 Watch ETUC briefing on new technologies allowing more surveillance at work**

COVID-19 is the biggest health, economic and social challenge in the history of the European Union. Numerous national measures have been implemented to fight the spread of COVID-19, also including those appertaining to workplaces and commuting to work.

Since the COVID-19 outbreak, workers in many sectors (most of them female workers) have continued being physically present at the workplace, at the frontline, fighting the virus, such as in healthcare, cleaning industry and retail. Europe is now entering a new phase of the fight against the pandemic, in which Governments are establishing gradual retake of work and the return to the workplace. The success of the EU exit strategy will largely depend on reaching agreements between the social partners on work organisation with a strong attention to occupational safety and health, for which the use of technology can be an effective tool if managed democratically.

The spread of the coronavirus pandemic has prompted countries to take extensive and far-reaching measures to tackle the consequences of the outbreak. Apart from curbing the spread of the disease, these measures have also posed legal challenges, significantly affecting workers' lives. Due to the nature of the virus, citizens' rights and freedoms have been curtailed, inter alia affecting their freedom of movement and assembly, as well as the right to conduct economic activities ([Bentzen 2020](#)). The dichotomy of privacy vs health, as much privacy vs the economy, is only going to get worse as tech presents solutions to (allegedly) help our return to normality: facial recognition could identify those who should be quarantined and sanction them if they recklessly put the lives of others at risk; smart technology could identify and report a worker who coughs which could reveal an infection of the virus. Body temperature could be automatically checked at the entrance of the working place ([Bartoletti 2020](#)).

Using contact-tracing apps to fight the spread of COVID-19 is intrusive and threaten EU citizens' right to privacy. To defend this right, key rules and principles of EU law, in particular those embedded in the General Data Protection Regulation (GDPR) and e-Privacy Directive, must be upheld. Claiming that defending privacy undermines the fight against the pandemic and the reopening of the economy is a mistake: for contact-tracing apps to be at all effective, they must be voluntarily and freely downloaded and used by a majority of citizens. This will only happen if citizens are confident that their privacy is not at stake. The two battles, for privacy and against COVID-19, are complementary, not opposed. Contact-tracing apps should only be used in the workplace if specific requirements are met [regarding, among other things,



**COVID-19  
WATCH  
ETUC BRIEFING  
NOTE  
ON NEW  
TECHNOLOGIES  
ALLOWING MORE  
SURVEILLANCE AT  
WORK  
30 SEPTEMBER 2020**

the purpose of the app, the type of data collected, how long the data is kept, whether workers give their consent, and whether trade unions are involved, ([Ponce Del Castillo 2020a](#)).

The COVID-19 pandemic, and the related switch to work-from-home practices, have also increased the demand for tools with capabilities for basic monitoring of employees' online activities and business intelligence reporting and data analytics to process employees' data ([Burdin 2020](#)).

Trade unions are worried that the current trends of surveillance and datafication could mean that COVID-19 data of today is at risk of being used for much more punitive and negative purposes by employers and that that the data will continue being used for such aims once the emergency is over.

Several public authorities have halted coronavirus tracking app on the grounds of violation of privacy. The Norwegian Institute of Public Health stopped gathering information and deleted all data from its mobile app after the Data Protection Authority warned that pairing Bluetooth for contact detection with location data for analysis went too far and questioned the usefulness of the app given its low usage ([Treloar 2020](#)). A proposal of the Croatian Government to track persons in self-isolation by their mobile phones was regarded as a serious threat to human rights by the opposition and civil society against this measure, and eventually the Government dropped the initiative ([Brändle 2020](#)).

Some of the developments reported by ETUC affiliates on surveillance at work in the light of the Covid-19 contagion are the following:

- **Belgium:** ACV-CSC conducted a survey among its members to explore the use of surveillance technology, especially in the light of the coronavirus. Despite most of the members reported no implementation of such technologies in their companies, some cases are worth mentioning, like the use of software like Veeva and Qlik Sense to measure the time spent in front of the computer in some companies and the case of a company in which telework was monitored through a surveillance software which registered each time the hand is placed on the computer mouse. In this latter case, social dialogue bodies were consulted and the extent of use of this practice could be better regulated in favour of workers. These technologies were reported to remain in place after the COVID crisis.

ACLVB reported about different companies have been running “tests” with smart wristbands using GPS and Bluetooth technology to enforce social distancing and perform contact tracking. Thermal imaging technology has been implemented in some workplaces. The national data protection authority and the labour inspection authority have spoken out against these practices. The union has also received several



# COVID-19 WATCH ETUC BRIEFING NOTE ON NEW TECHNOLOGIES ALLOWING MORE SURVEILLANCE AT WORK *30 SEPTEMBER 2020*

questions from its members regarding employers who ask teleworkers to access to their webcams to monitor their activity. In one case, this request was framed by the employer as a measure to monitor safe working conditions.

**Germany.** In Germany, the works council of the logistical company brought a lawsuit against the employer who did not respect co-determination rules about the use of an installation and use of cameras to record workers in order to guarantee the respect of social distancing without consulting the workers' representatives.

The works council won the trial and the court condemned the company to refrain from recording and processing picture or videos of employees, all the more when the recordings were non-anonymized camera and they were sent abroad (Ireland) for processing, which violated data privacy rights of workers. Regarding the protection of workers against the risk of contagion, the court stated that other measures already undertaken by the company (like the appointment of "social distancing ambassadors") were already proven to be effective.

**Italy:** In March 2020, the Italian Government and social partners signed the "Shared regulatory protocol of measures to fight and contain the spread of the Covid-19 Virus in the workplace" agreement, which regulated the installation and use of thermometers for temperature detection at the entrance of many private companies and public offices. The agreement observed GDPR, as real-time detection of body temperature constitutes a processing of personal data. Some of the provisions of the agreement are the following:

- The temperature of workers and any person accessing the workplace will be detected but not recorded.
  - A worker will be identified only if the temperature detected exceeds the threshold of 37.5 °, in which case the worker will be denied access to the building.
  - Workers are duly informed about the processing of personal data, which should be exclusively treated for the prevention of contagion from Covid-19 with the specification that the data will be kept until the end of the state of emergency (currently established in Italy until October 15).
  - The data should not be disclosed or communicated to third parties, with the exclusion of the Health Authority for the tracking of the contacts of a worker who tested positive for Covid-19.
- **Norway:** LO-N informed of the main results of a report of the Fafo Work Life Institute, showing negative tendency in the that attitudes to camera surveillance in specified workplaces in 2019 compared to 2010. The closer to employees' own lives and



# COVID-19 WATCH ETUC BRIEFING NOTE ON NEW TECHNOLOGIES ALLOWING MORE SURVEILLANCE AT WORK *30 SEPTEMBER 2020*

personal activities the camera surveillance is performed, the less positive. The survey looked into monitoring of telephone calls, use of telephone/other communication technologies, emails, web pages, computer/screen use, electronic registration of entry and exit, camera surveillance, field technologies when work is undertaken outside the employer's premises, biometric tools, electronic registration of time use/productivity and monitoring of internal chat rooms. 59 percent of the respondents reported the application of one or more of these systems in their workplaces. Digital monitoring and surveillance were generally perceived as more uncomfortable than traditional systems for monitoring of entry and exit, time use and productivity. The research found that although the system often has been discussed with employee representatives and or safety delegates, breaches of the requirements still occur. The lack of information and consultation of workers and their representatives is related with problems for employees to accept the use of different monitoring technologies.

- **Spain:** In 2018, Spain approved the Organic Law on Data Protection and the Guarantee of Digital Rights, which includes the right to privacy and the use of digital devices in the workplace; the right to digital disconnection in the workplace; the right to privacy in the use of video surveillance and sound recording devices in the workplace; the right to privacy in the use of geolocation systems in the workplace; and digital rights in collective bargaining. With the exception of this latter reference to collective bargaining, the law makes the effectiveness of the right to privacy, private life and protection of the images and sounds of workers depending on the design that the employer makes on the direction and control of business activity, especially in the companies and sectors which are not covered by collective agreements. These shortcomings have been amplified in light of the measures taken to contain the Covid-19 contagion.

At the beginning of the pandemic, most companies in the industrial sectors (automotive, energy, chemicals...) tried to adopt measures such as temperature taking and mandatory testing, which involved increasing control over workers by undermining the right to privacy protection. They were also asked for responsible statements in which the worker assumed the possibility of being sanctioned and of carrying out serological tests or taking temperatures without health justification and by non-health care personnel.

Some companies wanted workers to inform them of the places visited during holidays in order to know if they had been in areas of high incidence of the disease. Trade unions took action to guarantee the confidentiality of this information, in some cases by negotiating the measures and in others by reporting complaints to the Labour Inspectorate.



# COVID-19 WATCH ETUC BRIEFING NOTE ON NEW TECHNOLOGIES ALLOWING MORE SURVEILLANCE AT WORK 30 SEPTEMBER 2020

In sectors such as health care, and elderly homes, sometimes workers are obliged to pay for their serological tests. The company “*Empresa Mixta de Servicios Funerarios*” request workers to sign statements in which they commit not to keep contact with anyone outside the family environment.

- **UK:** Testing and tracing is poised to become a central part of the government’s exist strategy. the UK government has piloted the use of an app called NHSX to track people reporting Covid-19 symptoms and to alert those that they have been in contact with. TUC has delivered guidance on the proper performance of this tracking, for which employers should be prevented from having access to data gleaned from any state-run app that is rolled out. The tracking system should respect for existing privacy rules including those embedded in the General Data Protection Regulation (GDPR). There should be a commitment that contact-tracing apps should only be used in the workplace if specific requirements are met including setting out the purpose of the app, the type of data collected, how long the data is kept, ensuring workers give their consent and involvement of recognised trade unions in discussions about the use of the app.

The current trends in surveillance worry the public in general, and workers are in a more risky position. There is a growing discussion about the protection of workers’ personal data and privacy, including the boundaries between private life and work-related life. Some effects of the Covid-19 pandemic are becoming visible, such as (1) growing anxiety in the workforce about the threat of data misuse and poor working conditions (Kari 2020); (2) impacts on the right to disconnect, as well on the (3) productivity of workers working from home (Burdin 2020) and (4) the expansion of a general state of surveillance. There are risks of data being used for punitive, negative or other purposes once the emergency is over ([Bartoletti 2020](#))

Additional contact tracing apps to limit the transmission of the virus are introduced not only in the public sphere in many European countries but equally in workplaces. There is no single approach to develop these apps: technology and privacy parameters differ. Their use at the workplace is questionable as they can (1) track individual workers and (2) collect data, which raises 3 questions: what data is collected, what data protection is in place for workers and what employers should do or do not do with it?

As shown above, trade unions have started raising questions and outlining privacy guidelines for workers to return safely and protected to work ([TUC 2020](#)). Contact tracing apps can be useful to guarantee safety and prevent infection, but they mustn’t be turned into a tool for worker surveillance ([Ponce Del Castillo 2020b](#)). They can potentially be introduced if (1) the purpose of the app is well funded and respects the legal and regulatory frameworks, (2) the type of data collected is strictly used for contact-tracing, (3) the data is deleted after a defined period of time. Also, workers should give their clear informed consent and trade unions should



**COVID-19  
WATCH  
ETUC BRIEFING  
NOTE  
ON NEW  
TECHNOLOGIES  
ALLOWING MORE  
SURVEILLANCE AT  
WORK  
30 SEPTEMBER 2020**

be involved in all the steps of the process, including the development of confidentiality and security policies ([Ponce Del Castillo 2020a](#)).

‘Dressing up’ surveillance with the excuse of safeguarding public and occupational health is misleading. Surveillance can lead to anti-democratic, discriminatory and illegal practices at a global scale. The basis for workers’ guaranteed safety and privacy is high trust employment relationships ([TUC 2020](#)), as well as restrictions on the collection of data and maintenance of biometric surveillance bans.

Bartoletti I (2020) Protecting health and data privacy. The Progressive Post <https://progressivepost.eu/progressive-page/protecting-health-and-data-privacy>

Bentzen et al (2020) States of emergency in response to the coronavirus crisis: Situation in certain Member States III EPRS | European Parliamentary Research Service. [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI\(2020\)651972](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651972)

Brändle M et al (2020) Democracy and the state of emergency : Easing measures and rising tensions in the struggle with the Corona crisis in the Western Balkans, Croatia and Slovenia ; Report three. Friedrich-Ebert-Stiftung, <http://library.fes.de/pdf-files/bueros/belgrad/16119.pdf>

Burdin G HS, and Landini F. (2020) Why using technology to spy on home-working employees may be a bad idea. London School of Economics and Political Science, <https://blogs.lse.ac.uk/businessreview/2020/06/17/why-using-technology-to-spy-on-home-working-employees-may-be-a-bad-idea/>

Kari P (2020) Tracking tool allows Amazon workers to report Covid-19 cases. <https://www.theguardian.com/world/2020/may/06/tracking-tool-allows-amazon-workers-to-report-covid-19-cases>

Ponce Del Castillo A (2020a) Covid-19 contact-tracing apps: how to prevent privacy from becoming the next victim Policy Brief <https://www.etui.org/publications/policy-briefs/european-economic-employment-and-social-policy/covid-19-contact-tracing-apps-how-to-prevent-privacy-from-becoming-the-next-victim>

Ponce Del Castillo A (2020b) COVID-19 verschärft die Überwachung am Arbeitsplatz. May 8. <https://netzpolitik.org/2020/covid-19-verschaerft-die-ueberwachung-am-arbeitsplatz/>

Treloar S (2020) Norway halts coronavirus tracking App over privacy concerns. Bloomberg News, <https://www.bloomberg.com/news/articles/2020-06-15/norway-halts-coronavirus-tracking-app-over-privacy-concerns>

TUC (2020) Testing & tracing for Covid-19. How to ensure fair access and manage monitoring in the workplace. TUC, <https://www.tuc.org.uk/research-analysis/reports/testing-tracing-covid-19>