

# Time to Wonder: Covid-19 and the Risks of Home Office

## Regulating for Globalization

21/04/2020

Miriam Kullmann (Visiting Scholar at Harvard University, Weatherhead Centre for International Affairs) and Elisabeth Greif (Johannes Kepler University Linz)

*Please refer to this post as: Miriam Kullmann and Elisabeth Greif, 'Time to Wonder: Covid-19 and the Risks of Home Office', Regulating for Globalization, 21/04/2020, <http://regulatingforglobalization.com/2020/04/21/time-to-wonder-covid-19-and-the-risks-of-home-office/>*

---

The worldwide and fast spread of the corona virus and the Covid-19 disease gave momentum to homework for workers having office jobs. While information and communications technology allows workers to be available for work 24/7 the – mostly – abrupt decision of employers to put their staff on teleworking from home creates legal and practical challenges with a view to working time and health and safety regulations as well as privacy and data protection rules, such as the General Data Protection Regulation (GDPR). With workers working from home, it becomes more difficult to keep track on whether they work, how long they work, and whether they work 'productively'. Moreover, home office means that workers often, but certainly not exclusively, use their own devices (BYOD) and the official software and other digital tools that their employer has provided for performing the work calling into question the separation between work and private life. The new Covid-19 related home office also provides enormous challenges for those having care duties, the latter also putting the gender perspective and the risk of discrimination (back) on the agenda.

## Tools for Surveilling Workers

Moving the designated workplace to the workers' home – even if only temporarily – proves challenging. Depending on the job and the inherent tasks work has shifted face-to-face interaction between workers to virtual meetings. Usually, the right of employers to give their workers work-related instructions and directions within the boundaries of the agreed and statutorily regulated working time also entails the possibility for employers to make sure that workers abide by the (contractually) agreed job description and the inherent tasks. Shifting work from the designated workplace to the workers' private homes leaves employers with merely two options: either doing nothing and trusting their workers that they will continue working as if they were at the office (not implying that this is always productive) or deploying means that replace the 'face-to-face-surveillance'. It very much depends on the applicable labour law regulations and institutions whether and to what extent technology can be used when workers are in their 'home office'. Apart from the legal particularities though, technology offers a broad palette of 'spyware', perpetuating modern-day Taylorism. (Hidden) software designed to monitor workers, such as keystroke monitoring, webcam and microphone, screen monitoring and timed screenshots, log for every activity on the company's notebook, to name just a few. Workers' activities produce information for employers which they may use to take disciplinary measures against 'not so productive' workers.

## Data Protection at Home?

While working from home under certain conditions can have benefits, 'home office' – as the term itself indicates – blurs the boundaries between work time and non-work time as work is being transferred and brought into the workers' home and family life. The 'surveillance' tools provided and used by the employer enter the employees' private spaces. Analytic tools pursue a double aim: On one hand, they monitor employees and encourage productivity while on the other hand, they help meeting compliance and security demands. More than ever worker monitoring is becoming increasingly intertwined with collecting for surveillance, performance evaluation, and management. Data is collected, processed, stored, and used for further analysis. The collection of data not strictly relevant to the work activity, especially when monitoring workers in the home office, raises data protection concerns. Article 9 GDPR seems clear in stating that the '[p]rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited'. An exemption can be made where the worker has given explicit consent (which in many cases can be doubted to exist) or when processing is necessary for carrying out obligations and exercising specific rights in the field of employment law, if authorized by EU or national law or collective agreements.

The observation of workers can be done by algorithms which – on a step-by-step-basis – are designed to solve 'problems' as – for example – distinguishing 'good' (productive) from 'bad' (unproductive) employees. With automated decision-making, however, the risk remains in the way certain previously defined data is collected, how different data is linked and which decision is taken on that basis can be biased: As variables for a distinction between 'good' and 'bad' employees, for example, employers may take into account how long someone has been using the employer's Virtual Private Network (VPN), or which email application has been used, whether and how long someone joined a virtual meeting, and how often and fast a worker answers email. These criteria can provide information on the productivity and availability of workers, but this is not always the case: If workers use their own devices, they may not have all software installed. Thus, the danger of using tracking systems is that the data collected and analyzed and the decisions that are based on that data may not reflect realistically what workers do. There is another and much more eminent danger associated with the use of automatically collected data to assess productivity: The use of surveillance software can lead to gender discrimination.

### **Gender-specific Impact of Covid-19**

The gender-specific effects of the virus do not only consist in the gender-specific differences in health. While men seem to show a higher mortality and vulnerability to the disease women seem more burdened by the social effects of the virus. For many women working as nurses, saleswomen in the supermarket or other indispensable tasks home office is not an option. Many of those who are at the frontline of the response (and at the lower end of the economic and salary scale) face a great risk of infection and a good part of them are female. Those women who can work from home, however, face on the one hand the risk of the coronavirus lockdown reinforcing gender stereotypes and the risk that the above-mentioned surveillance mechanisms may have a discriminatory effect. Even where both parents are in the home office, there is a tendency for household and childcare to be taken over predominantly by women. When programs measure the time employees are online continuously workers whose working day is interrupted by childcare or homeschooling might seem less 'productive' and less 'available'. A surveillance tool measuring continuous online time and labels it as productivity instead of focusing on the outcome of work processes thus runs the risk of undervaluing women's work.

### **The Lockdown as Magnifying Glass**

The effects of the lockdown and the resulting requirement of the home office for many employees are by no means a (completely) new phenomena but during the lockdown they become more visible, like under a magnifying glass. The temporal delimitation and spatial dislocation of work poses great challenges for the separation between work and private life. This challenge arises from the tension between the right of employees to privacy as laid down in Article 8 ECHR and Article 7 EUCFR (both guaranteeing the right to respect for private and family life, home and communications) and the interests of employers, which can fall under the protection of Article 16 EUCFR (freedom to conduct a business). As for the discrimination risk a number of EU directives (2000/43/EC, 2000/78/EC, 2006/54/EC) provide a robust framework to combat discrimination in the workplace. These directives also apply when the discrimination results from automatically collected data or automated decision-making. The surveillance of employers in home office runs the risk that variables measuring 'productivity' or 'availability' - if employed without considering their (unintended) effects - may lead to the reification of gender bias and gender discrimination. A human-rights based framework that takes into account the substantive aims of EU-antidiscrimination law and focuses on the outcome of decisions based on automatically collected data or automated decision-making may help to address and overcome those risks.

With special thanks to Marianne Hrdlicka for excellent research assistance and Birthe Dorn for her valuable comments.

***The Regulating for Globalization Blog is closely following the impact of COVID-19 on the labour, trade and European law communities, both practically and substantively. We wish our global readers continued health and success during this difficult time. All relevant coverage can be found here.***