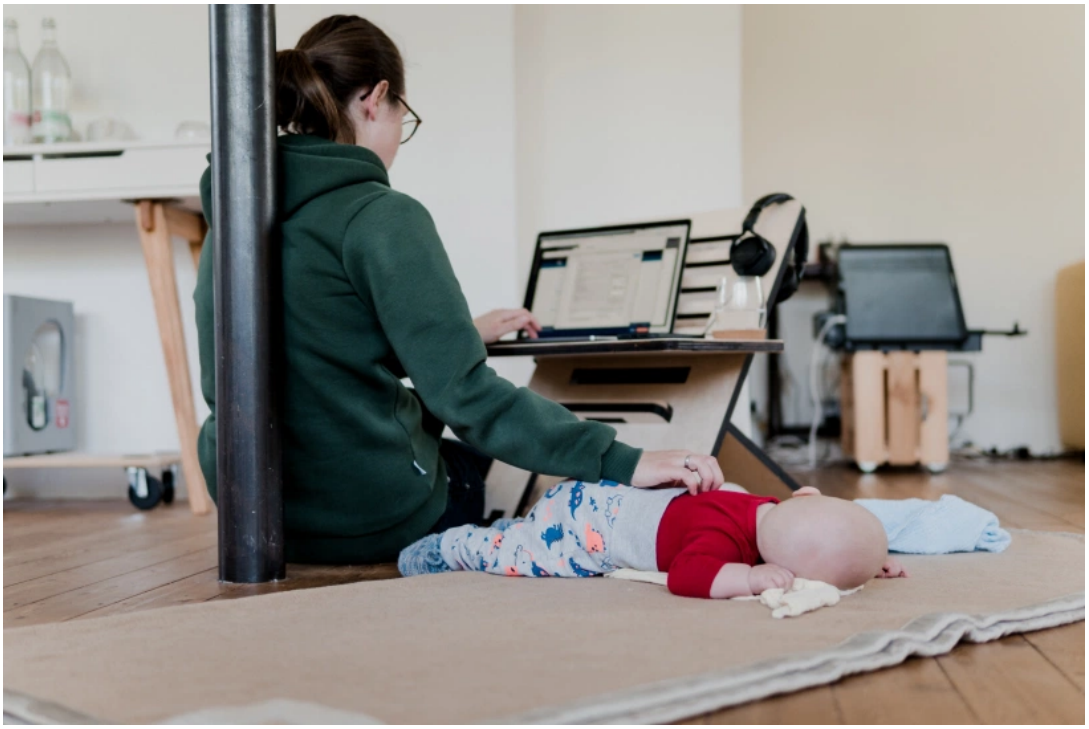
CORONAVIRUS, HUMAN RIGHTS, PRIVACY, WORKING FROM HOME

The right to privacy while working from home ('WFH'): why employee monitoring infringes Art 8 ECHR – by Eleni Frantziou



Date: October 5, 2020 Author: UK Labour Law Blog 0 Comments

Image by Standsome from Pixabay

Can employers monitor employees when they work from home (hereafter 'WFH')? Recent news coverage from the BBC and The New York Times has shed light on numerous employer practices intended to monitor employee productivity, which have been emboldened by the unprecedented wave of WFH during the Covid-19 pandemic. Monitoring can take various forms, depending on the app that the employer uses. It may include any of the following: opening emails; checking online behaviour such as time spent on work-related apps; tracking websites visited; taking screenshots of what

was typed on those websites; physical location tracking and, even, webcam surveillance and taking photos of employees whilst they are working. The legality of this monitoring is debatable: while it may be accepted under the DPA 2018, it is subject to several safeguards for the employee, such as prior notice, which are further highlighted in the Employment Practices Code. Yet, even if those safeguards are met, WFH is not specifically envisaged, so that a broader question of human rights law remains: is monitoring a justified limitation of the employees' reasonable expectation of privacy within their own homes? This post seeks to address this question by reference to the protection of the right to private and family life enshrined in Article 8 ECHR. It should be noted that while only the ECHR is considered in this post, EU law (which the UK's DPA 2018 implements) may protect privacy more extensively, under Articles 7 and 8 of the EU Charter – provisions which can be invoked directly against private employers before national courts and tribunals. As such, the discussion in this blog post relates only to the minimum threshold of human rights protection that employees may expect.

In an excellent post of 3 September 2020 on this blog, Philippa Collins persuasively showed that domestic case law leaves much to be desired in respect of its accommodation of privacy under Article 8 ECHR, with employment tribunals having previously taken an employer-friendly view of the fairness of dismissals ensuing from monitoring. This is supported by the Strasbourg Court's rulings on workplace monitoring in *Bărbulescu* and *López Ribalda,* which in principle accepted the justifiability of monitoring under Article 8, subject to various proportionality requirements. This post will put forward an alternative view. It will argue that the ECtHR's broader case law casts serious doubt over the compatibility of monitoring with Article 8 of the Convention in a WFH environment, where the potential psychological harm of monitoring is such that any test of proportionality has to be very strictly applied. More specifically, whereas the Grand Chamber rulings in *Bărbulescu* and *López Ribalda* cannot be considered as mere aberrations, they are distinguishable from the WFH scenario because they do not concern the heightened protection of privacy afforded within the home. This protection is affirmed in another long-standing line of cases of the Strasbourg Court (e.g. *Chappell* and *Niemietz*). In turn, under their s.2 HRA duty to take into account and in principle to comply with 'clear and constant' findings of the ECtHR (*Manchester City Council v Pinnock* [2010] UKSC 45, §48), national courts and tribunals must give an appropriate weight to both of these strands of Strasbourg case law in order to reach the right balance between the employer's interest in supervising employees and the employees' right to privacy. Following the principles stemming from this case law would, in my view, lead to findings of incompatibility with Article 8 for most of the monitoring practices described above, even if these were *prima facie* justified by concerns over employee productivity or supervision.

Nuancing the application of *Bărbulescu* and *López Ribalda* to WFH

While prying by employers is not what was initially envisaged during the drafting of Article 8, the monitoring of calls, emails, and other correspondence comes within the scope of its protection. In *Copland,* the ECtHR found a violation on account of the monitoring of a civil servant's

telephone calls, email and Internet use without an appropriate legal basis (§§48-49). Similarly, in *Halford,* the Court found a violation of Article 8 because of the absence of a legal basis for the interception of calls by a civil servant (§51). In *Bărbulescu* itself, the Court found that a private employer's monitoring of an employee's use of the Internet, including by accessing private messages sent via Yahoo Messenger, violated the employee's private life (§§74-81). Indeed, while a lengthy discussion can be had about the appropriate distinction between public and private employers in the Court's case law, in practice a similar test is employed for assessing the necessity of monitoring in the case of negative obligations of public authorities acting in their capacity as employers as for assessing whether national courts adequately balanced the employee's Article 8 rights with the employer's interests in the case of private employers (*Libert*, §47).

In *Bărbulescu*, the Court found that states are required not just to show that an adequate legislative framework was in place to ensure the protection of privacy in the workplace, but also to ensure that national courts had offered an appropriate balance between the interests of employer and employee (*Bărbulescu*, §121-122). Paragraph 121 of the ruling laid down a set of considerations that courts must take into account when balancing these interests which, in summary, are the following:

(i) whether there was notice of the monitoring, which should normally have been clear about the nature of the monitoring and given in advance;

(ii) what was the extent of the monitoring by the employer and degree of intrusion into the employee's privacy, with a distinction to be drawn between the flow and content of the communications monitored (this is a distinction between employer checks, e.g., on *which* websites the employee visits, on the one hand, and seeing *what* they type in them, on the other, such as reading their private messages). Attention should also be paid to whether the monitoring was limited in time and place;

(iii) whether there were legitimate reasons to justify the monitoring of the flow of communications in the first instance and further reasons to justify accessing their content, which requires weightier justification;

(iv) whether there were less restrictive alternatives from the perspective of the employee's privacy;

(v) what the consequences of the monitoring were for the employee (e.g. dismissal) and whether the monitoring was used for its originally specified purpose;

(vi) whether there were adequate safeguards for privacy, particularly where content monitoring was at stake.

The case confirms that monitoring in the work environment in principle engages the employee's Article 8 right to privacy and that the expectation of privacy at work cannot be reduced to zero (§80). Yet, it also makes clear that the employee's reasonable expectation of privacy in the workplace is not in itself conclusive for coming to the determination of a violation (§74). Where, as in *Libert*, the safeguards listed above are met, the Court accepts the compatibility of the monitoring with Article 8.

The main question that arises, then, is how strictly the above criteria should be applied. A loose interpretation of these criteria led to a troubling ruling last year, in *López Ribalda*. In that case, the state was not found to be in breach of Article 8 for failing to protect against CCTV video-recording by a private employer, and this was so despite the fact that notice of the measures, as listed in *Bărbulescu*, had not been given in full. Two key aspects of *López Ribalda* must, nevertheless, be emphasised so that its distinctness from other potential violations of Article 8 can be appreciated: first, the Court found that there was a limited expectation of privacy on the facts (§93, §125), because the employees were working in a quasi-public space (a supermarket) in which they had contact with members of the public and knew CCTV was in operation in general within the store (although they did not know that it was filming them directly). Second, again due to the particularities of the facts (the purpose of the monitoring was to ascertain whether employees were stealing from the store, which the CCTV camera confirmed), this case depended on a need to balance the employees' right to privacy and the employer's right to protect their property, in line with Article 1 of Protocol 1 (§118), rather than with a broader interest in ensuring employee productivity, as in *Bărbulescu*. It follows that, while *López Ribalda* might be a problematic case for various reasons articulated in more detail elsewhere, it would be difficult to transpose it to a scenario like WFH, where there is a strong expectation of privacy, on the one hand, and a less tangible proprietary interest, on the other.

López Ribalda can, indeed, be read as confirming *Bărbulescu* and clarifying that some of the conditions listed therein can vary depending on the circumstances of the case. Two overarching principles drive the Court's analysis in respect of employer-imposed monitoring in both cases: first, the existence and degree of *privacy that an individual can reasonably expect* in a particular setting remains key to assessing whether Article 8 has been violated. The rigour of the balancing exercise conducted by the authorities is always determined by that expectation. Second, whereas the Court recognises case-by-case variations to the procedural guarantees listed in *Bărbulescu* §121, such as prior notice, its approach to balancing emphasises the *quality, appropriateness, and proportionality of the reasons offered for limiting privacy to the monitoring practice* in question, rather than accepting a mere appeal to abstract or unsubstantiated reasons. Combined with the case law on the protection of the home that I explore below, these two principles confirm that only weighty reasons accepted after strict proportionality scrutiny could allow monitoring in a WFH setting, where a very high expectation of privacy applies.

Assessing the justifiability of productivity monitoring based on the strong expectation of privacy generated by the protection of the home

The Strasbourg Court's case law on the home centres on function and is already broader than the residential dwelling. As the Court put it in *Moreno Gómez*, 'a home will usually be the place, the physically defined area, where private and family life develops.'(§53) In principle, this can include a single room, a caravan or any other space (see, e.g., *Buckley* and *Chapman*). Crucially, the high level of protection of privacy afforded to the home has extended not just to home offices, but also to private offices outside the

home (see, e.g., *Buck; Niemietz; Steeg*), as well as to commercial premises where the owner kept lodgings (*Chappell*). It is therefore possible to conclude with conviction that the protection of the 'home' as defined in a constant line of Strasbourg case law already captures the WFH scenario.

This case law provides strong support for the idea that the home cannot easily lose its protected status under Article 8(1) merely because it also serves other functions, and that it cannot simply be transformed into a quasi-public workspace during working hours. Rather, the Court tends to allow the strong privacy protection of the home insofar as the physical space in which the violation has occurred continues to serve as a principal or significant residence or 'domicile' (including of a professional nature) at the time when the potential interference occurs (discussed by Buyse here). It follows that the determinative question at stake in cases like *López Ribalda* and *Bărbulescu*, i.e. whether there was an expectation of privacy at all, does not arise in the WFH context. Being in a private space and, especially, in a private residence, is not only distinguishable from working in a quasi-public place, such as a supermarket, but it is indeed distinguishable from any other type of work environment. Whilst in their own homes, individuals enjoy an expectation of privacy of the highest degree (Buyse, as above).

What does the protection of the home mean? While the above-cited case law has been primarily about searches and evictions, rather than about monitoring, it confirms that the home is not endangered only by 'concrete or physical breaches, such as unauthorised entry into a person's home, but also includes those that are not concrete or physical, such as noise, emissions, smells or other forms of interference' that prevent quiet enjoyment of the home or of its amenities (*Moreno Gómez*, §53). The Court has repeatedly found that attacks on privacy within the home, such as covert filming, constitute particularly grave violations of Article 8. In *Khadija Ismayilova*, it recently characterised covert filming as a 'serious, flagrant and extraordinarily intense invasion' of private life (§116). In *Söderman*, the Grand Chamber found that it amounts to a breach of 'personal integrity' (§§81-86). It further noted that the psychological vulnerability created by having been filmed covertly was sufficient to violate the Article 8 rights of any person (§85), and that it was of particular seriousness when concerning children (§81).

Of course, the high expectation of privacy afforded within the home does not give rise to an *absolute* protection from outside incursions. Yet these cases highlight the potential severity that some forms of employer monitoring could acquire, when practised within individuals' homes. This underlines the difficulty of applying the second main principle stemming from *López Ribalda/Bărbulescu*, i.e. the existence of sufficiently good reasons for the monitoring, which are proportionate to the significant invasion of privacy sustained in this context. While an employer's fear of employee unproductivity during WFH might be a natural response to the rapid change of working patterns that followed the outbreak of Covid-19, it does not fundamentally alter the nature of their legitimate interest, which is that of knowing that salaries are being paid to good effect both during WFH and in a regular working environment. In fact, so far, there is no compelling evidence that WFH reduces employee productivity, while research

conducted during the lockdown period has suggested that the opposite is true. By contrast, monitoring during WFH would significantly reduce the potential of the individual's home to serve as a space of shielding from the public eye and could easily blur into the individual's family life, such as by tracking or capturing sensitive information about other members of their household, including their children.

A series of proprietary considerations could also have the effect of tipping the scales in favour of the employee. These include ownership or occupation of the Internet connection, all or some of the equipment used to perform work (e.g. the computer, the desk etc) and, ultimately, the physical space where work takes place. Whereas in a regular work environment these would normally constitute employer resources, monitoring at home engages the employee's right to respect for the use of such assets, in line with Article 1 of Protocol 1, as well as the right to enjoy their home's amenities as part of Article 8, as highlighted by *Moreno Gómez*. While the Article 8 claim is certainly stronger on the whole, the question of whose resources are at stake could be important for the balancing exercise in WFH cases. This is not only evident from *López Ribalda*, which concerned theft, but even from *Bărbulescu*, which was a typical productivity-driven case of employee monitoring, with the employer emphasising that time spent at work must be spent working and not on other activities (§15). The ruling, however, was silent on the question of working time and acknowledged the justifiability of monitoring by reference to the employer's need to protect company resources from use for personal purposes (§109). In turn, if monitoring is about productivity during working hours (which is even more clearly the case in a WFH setting), it is possible to imagine alternatives less restrictive to privacy, such as the submission of a breakdown of how working time is spent by the employee or the employer's use of disciplinary action where there is evidence of a failure to complete work tasks. Taken together, the above-linked studies that challenge heightened fears over unproductivity during WFH, the shift of the proprietary interests in favour of the employee, and the existence of less restrictive alternatives, would be likely to render productivity monitoring less persuasive in the WFH scenario.

While monitoring for reasons other than productivity is not the main focus of this post, it is important to highlight that stronger reasons could improve the employer's case for monitoring. This is clear from both *López Ribalda* and from *National Federation of Sportspersons' Associations and Unions (FNASS) and Others*(a case I explore in more detail below). Justifications such as the protection of health or the prevention of fraud could be an important distinguishing factor for some professions, such as sport, banking, or the provision of social services, where private employers have a statutory obligation to act in the public interest and may need to engage in some monitoring to do so. However, even where there are good reasons for the monitoring, it is essential to still draw attention to the proportionality requirements highlighted in *López Ribalda* and *Bărbulescu* and already discussed above, such as the existence of less restrictive alternatives, as well as the assessment of the purposes for which the data is used. While monitoring may be deemed more easily justifiable in such cases, the

material collected during monitoring for one purpose cannot subsequently be used for a different purpose, such as to dismiss an employee for reduced performance.

Overall, it is difficult to see where the Court could accept productivity justifications in a WFH setting. It would be likely to be especially mindful of accepting image-based monitoring or active surveillance, e.g. physical tracking, as suitable and proportionate to the employer's interest in checking that employees' time is spent on work tasks. The threshold might not be set as high in respect of data monitoring, which has not (so far) been considered an attack on personal integrity in the same way as image-based/physical monitoring. However, as the invasiveness of any type of monitoring would still be much greater within the intimacy of a person's home than it is in the workplace, it can be expected that stricter proportionality scrutiny would apply to these interferences, too, including interferences that concern monitoring the flow of communications listed as a lesser harm in *Bărbulescu*, §121-ii. The following observations can be made in respect of video-surveillance/physical tracking and data-based monitoring, more specifically.

- **Video-surveillance and physical tracking**

The case law discussed above provides a good illustration of the clarity with which covert monitoring could violate Article 8. But any form of image-based or other physical surveillance or tracking in private homes could safely be considered incompatible with Article 8, when used for private interest reasons, such as time/productivity-checking. This is because the gravity of the harm to privacy is unlikely to be sufficiently counterbalanced in such cases, particularly where the monitoring extends beyond the purposes of work (as is often the case, for instance, with location tracking), thus capturing or having the possibility to capture the employee's activities during leisure time or the activities of other members of their household, such as their partner or children. The breadth of this type of violations would also be likely to render the question of notice insignificant. Knowledge that a picture-taking app or webcam surveillance were in use would not alleviate the severity of the attack on the employee's own personal integrity or the potential harm to the rights of others, such as family members. Indeed, the Court has long recognised as part of Article 8 'the right to live privately, away from unwanted attention' and the need to secure for the individual 'a sphere within which he or she can freely pursue the development and fulfilment of his personality' (*Smirnova*, §95; reiterated *inter alia* in: *Sidabras and Džiautas*, §43; *Couderc and Hachette Filipacchi Associés*, §83; *Satakunnan Markkinapörssi Oy and Satamedia Oy*, §130; and *Bărbulescu*, §70). This is further reinforced by the right to ownership of one's image, which the Court considers a core part of one's identity, applicable in certain cases even in a public place for a public figure (*Von Hannover*, §§95-97). Further, unlike *López Ribalda*, where the Court was influenced by a high degree of 'publicness' of the setting in question, the Court has in other cases found video-surveillance in the workplace to violate Article 8. *Antović and Mirković* is a case in point.

In *Antović and Mirković*, the Court found that the non-covert use of video-surveillance in a university auditorium was a significant intrusion into the lecturers' private life (§44). Noting that social activities and exchanges between defined individuals took place in that space, the Court found that the university auditorium should be distinguished from public entryways, the street or, one might add, a supermarket, as only a defined group (students and lecturers) would have cause to enter it (§59). The fact that the video-surveillance had been communicated to the employees, in line with *Bărbulescu*, was immaterial for the Court in this case. The invasive character of the collection of someone's image and the inability on the part of the employer to adduce reasons why the justification they had otherwise given for the surveillance – public safety – should apply within the classroom, were key to the Court's ruling. These findings acquire even greater force when applied to one's own home, where the reasoning of the Court in *Antović and Mirković* would arguably have been unanimous. The joint dissenting opinion of judges Spano, Bianku and Kjølbro in that case is particularly useful for appreciating the minimum threshold the Court would be likely to set.

The dissenting judges highlighted that, whereas they disagreed with the majority's finding that video monitoring in itself constituted an interference with the applicants' privacy in this case, they would have felt differently if it had concerned private offices (not to mention private residences). More specifically, the dissenting judges found it conclusive that the applicants were 'university teachers who were giving lectures in a university amphitheatre, thus fully engaged in a professional activity in a quasi-public setting, and not, for example, in their offices. Having been notified of the video surveillance in the amphitheatres, their reasonable expectation of privacy in that particular context, if any, was very limited' (§12 of dissenting opinion, emphasis added). It is also remarkable that, while the dissenting judges (unlike the majority) did think that notice would matter in such a case, they still would have felt differently if the applicants 'irrespective of such notice had a reasonable expectation of privacy' (§8 of dissenting opinion, emphasis added). In other words, even for the dissenting minority that took a more conservative stance than the majority of the Court in this case, Article 8 would have been clearly violated in a WFH context. This is because the expectation of privacy is not in question, there is a potential of capturing a broader set of activities likely to accompany home-working (e.g. intermittently caring for children or for other family members, eating meals, or taking breaks from work in the same space as working) and the monitoring is made with the purpose of being processed to assess productivity and can be used, e.g., in support of a subsequent case for dismissal (whereas in that case, it was not used at all).

Other forms of physical tracking, such as keyboard movement tracking, can also be brought within the principles set out in this case law. Even if this type of monitoring does not concern image protection *per se* and has not yet been the subject of explicit condemnation in the case law, it raises precisely the same principle, namely that effective ownership of data pertaining to one's bodily integrity including (but not necessarily limited to) one's image, is a key feature of Article 8. Thus, even with notification, and most certainly in its absence, any indiscriminate or unclearly delimited form of video-

surveillance or physical tracking of employees for the purpose of monitoring their productivity whilst in their own homes is incompatible with the case law of the ECtHR, as it currently stands. Crucially, this case law can apply to more limited forms of physical tracking and surveillance, too. For instance, the daily tracking of one's whereabouts during working hours would still be likely to be found incompatible with Article 8. The *FNASS* case can be used to illustrate this point.

In *FNASS*, the Court decided that Article 8 was applicable where the French state required high-level athletes to provide, at three-monthly intervals, full information on their whereabouts, including at weekends and during their holidays, as part of the effort against doping (§§155-159). While the Court found that this constituted an interference with Article 8, it did not find a violation on the facts, due to the special nature of sport and the legitimate aim pursued by the interference. However, it follows from the Court's reasoning that regular tracking would normally fall short of the proportionality requirement. This would appear clearly to be the case where the matter concerns reasons of private interest for the employer, such as productivity monitoring, as opposed to the fulfilment of the legitimate public aim pursued in *FNASS*. Indeed, while the *FNASS* case provides some support for requirements to declare how working time (and, for certain professions, limited aspects of non-working time) has been spent, it is important that the case presupposed agency through individual submission of the relevant data by the employee, rather than mining this information through tracking or surveillance.

- **Monitoring of other forms of private data, such as online activity**

The main principles stemming from *López Ribalda/Bărbulescu* that I have summarised earlier in this post as the need for an analysis of both the employee's expectation of privacy and of the employer's reasons and regard for proportionality, are also crucial in cases of monitoring of online activity. Still, as checks on online activity are especially reminiscent of *Bărbulescu* in terms of the type of monitoring, it is worth highlighting in more precise terms what a greater expectation of privacy would mean in this context. On the one hand, it is true that the opening of company email or other employer-provided software would not differ fundamentally from *Bărbulescu* and *Libert*, insofar as it occurred through company servers and not through data collection. That is certainly not to suggest that private information of this type can be read and used for disciplinary action or dismissal at will, but, rather, that the high standards set out in respect of this form of content monitoring would not change drastically in the WFH setting, compared to earlier rulings. On the other hand, WFH would justify a strict proportionality standard with respect to *any* data monitoring accessed via the person's home network, including by tracking which websites the employee is visiting, which *Bărbulescu* had classified as a lesser intrusion than content monitoring (§121 – ii). Further, like image-based monitoring and surveillance, WFH reduces the mitigating effect of notice of the monitoring for the employer.

The distinction between communication flow monitoring and content monitoring is not given excessive weight in the Strasbourg Court's case law beyond the workplace and should not necessarily be considered applicable

when the employee works from home. The Court's Grand Chamber has often held that the protection of data should not be interpreted restrictively and relates to any data concerning an 'identified or identifiable' individual (*Amann*, §65). This not only covers data such as websites visited, but even extends to a broader 'informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated' (*Satakunnan Markkinapörssi Oy and Satamedia Oy*, §137). In *Benedik*, for example, the Court found that the collection of data associated with a dynamic IP address can violate Article 8. Dynamic IP addresses (i.e. the type of IP address most home networks have) are in principle visible to and can be captured by other Internet users. Even though these addresses change and are thus not strictly personal to an individual, they can reveal details about them, such as their location and patterns of online behaviour. In *Benedik*, the Court noted that the individual concerned cannot be expected to conceal the address to prevent interception of their data (§116) and further remarked that entire households can be exposed through data collection via IP addresses, as they will often share an Internet subscription (§112).

These cases show that even less individualised forms of tracking of online behaviour than tracking the flow of communications have been proscribed by the Strasbourg Court, when occurring through private servers. While these rulings might not *prima facie* concern monitoring of employees' work patterns, it would be erroneous for national courts to treat them as irrelevant, because they raise considerations pertinent to the WFH scenario, where workers have adapted their own Internet connections to fulfil work tasks, yet may be unaware of the exposure that this creates for themselves and their family members. For example, even where only website tracking is at stake, this could still reveal to the employer information that the employee is entitled to keep private, such as their personal preferences or those of other members of their household, including information about protected characteristics, such as religion or sexual orientation. Thus, whereas *Bărbulescu* had distinguished monitoring of content from the monitoring of data flows, this finding was made in a context where key concepts, such being 'at work' and using company resources, were clear.

Indeed, neither the distinction between website traffic and access to content nor notice that private information might be accessed and processed should be over-emphasised in the WFH environment. Notification would again be extremely difficult to treat as a determinative factor in a setting where a high expectation of privacy exists. This is the case particularly insofar as the collection of information from a home network could have the effect of exposing the person without time limitations and revealing sensitive information about non-employees with whom the individual interacts online or who use the same computer or Internet connection at home. And even in the unlikely event that notice were still considered a relevant factor, there should be evidence that the employee had a fully informed understanding of the types of information that the employer could access and for which purposes, as well as what steps had been taken to limit their exposure to working time. This is highlighted by *Libert*, where the Court only accepted the relevance of notice as part of a time-limited (albeit content-based) monitoring practice for a company-owned computer, which

was opened only when the computer was returned to the office. This threshold would be very difficult to meet for the pervasive tracking offered by employee monitoring apps, which remotely capture information in real time via the person's home network.

The psychological harm caused by monitoring during WFH and the heightened vulnerability of the employee

Before concluding, it is worth underlining a final – and, arguably, the strongest – countervailing factor in favour of the employee in the WFH environment: the psychological damage caused by monitoring within the home. While consent and clear employment charters may somewhat soften the blow of a limitation of Article 8 in cases where one knows they can return to a place of privacy at the end of the working day, this is precisely what would be lost through WFH monitoring. The importance of the psychological impact of interferences with privacy is already evident from the Court's position on the concept of the home. It would be likely to be considered a distinct feature of WFH monitoring, further hindering the potential of any such monitoring being accepted under Article 8, at least for productivity-related reasons.

Employees have reported that monitoring during WFH has been 'demoralising' and has made them feel constantly under scrutiny and 'incredibly stressed out.' Indeed, the vulnerability created by feeling 'watched' or in any other way monitored in one's own home and through one's own possessions is not relevant only when being filmed or physically tracked, but also extends to the knowledge, suspicion, or fear of being monitored through private communications as well as other online activities, such as browsing history and website traffic. This is highlighted by Elizabeth Anderson in her aptly titled book 'Private Government: How Employers Rule our Lives (and Why We Don't Talk about It)' at 39-41, and has been compellingly discussed in the ECHR context by Virginia Mantouvalou. As Mantouvalou has noted, beyond the clear impact that monitoring of online activity can have on Article 8, it can also have a chilling effect on the exercise of other rights, such as Articles 9 and 10, due to the fear of dismissal over expressing one's thoughts or beliefs in private or revealing them through websites that the employee visits in their free time.

These considerations are likely to be profoundly significant for the Strasbourg Court. The psychological harm caused by monitoring has already been a factor in its analysis in *Antovic and Mirkovic*, *Copland*, *Halford* and *Bărbulescu*. The human need to build and maintain social relations was the very reason why, in *Bărbulescu*, the Court emphasised that 'employers cannot reduce private social life in the workplace to zero.' (§80). Further, the Court's position with regard to psychological harm has been shown acutely in cases concerning the home. As already indicated in earlier sections, the Court has explicitly recognised that the psychological injury suffered by a person monitored in the intimacy of their home is especially severe (*Söderman*, §80). The Court has also already accepted that monitoring within the home places the individual in a state of fear of repercussions, which

could restrain their exercise of other rights and, most notably, the freedom of expression (*Khadija Ismailova*, §164). All of this invites serious questioning of the acceptability of any of the types of monitoring analysed above.

Additional considerations can be raised here which, albeit not yet featuring centrally in the Court's case law, could be much more succinctly carved out if the Court had the opportunity to assess the particular vulnerability of an employee in this context. For example, the inherently imbalanced structure of the employment relationship in itself challenges the possibility of consenting to employer-mandated monitoring. This is an even deeper concern when it relates to a person's home, at a time when a global public health emergency is placing a significant part of the workforce at risk of redundancy. Feelings of anxiety and helplessness, as well as the potential difficulty of accessing workplace representation whilst isolated from co-workers, further weaken the position of the employee during WFH. It would thus be welcome if the Court drew a sharp line at the justifiability of monitoring in a WFH environment, other than for public interest reasons.

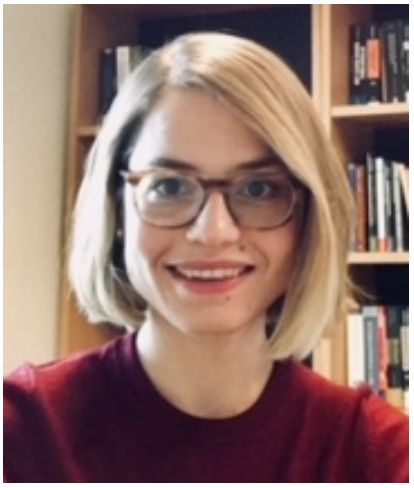
To do so, the Court might in future be prepared to recognise a positive obligation to protect the basis of mutual trust and confidence upon which the employment relationship functions. Indeed, rather than seeking to increase trust (as suggested, e.g., by pp. 5, 58-59 of the Employment Practices Code), the monitoring practices mentioned in the beginning of this post clearly point to a deterioration of the employer/employee relationship and support a culture of employee denigration. This is exemplified by the app providers' websites, which vividly paint a picture of employees as time-wasters routinely engaged in 'wage and time theft'. This culture can force human beings into a dystopian, all-encompassing world of work, where taking an 'extra 10-minute break here or there' – to use one BBC interviewee's words – must be urgently exposed and punished. Unless a requirement for state authorities to curtail such tendencies were built into the case law, it might not be long before the Court's conception of a private life 'not susceptible to exhaustive definition', in which work has traditionally played a valuable role (see, e.g., *Sidabras and Džiautas,* §43), starts to look like a mere fiction.

Conclusion

This post has examined the question of whether employee monitoring during WFH is compatible with the right to private and family life protected in Article 8 ECHR. It has sought to show that, for the most part, the answer the Strasbourg Court would give to this question is a resounding 'no'. The majority of the data collection practices developed in response to WFH and recently reported by the BBC and New York Times would be likely to fall short of the privacy protection enshrined in Article 8 ECHR, regardless of whether the employee has been notified or not. Especially in light of the fact that some of these types of monitoring go beyond what was imagined in *Bărbulescu* even for the workplace, as they involve taking screenshots or photos of workers and tracking keyboard activity,a higher standard of scrutiny than that set out in that case should be expected. This is particularly clear when it comes to apps that involve a person's bodily integrity (such as their image), but combined with the special protection of the home afforded under Article 8 and the significant

psychological harm that can be expected in this context, it is difficult to imagine *any* monitoring meeting the Convention threshold for reasons solely of productivity checking.

Indeed, it should be clarified by way of conclusion that, while WFH would raise novel issues for Strasbourg, to which I have sought to allude in the last part of my post, the argument I have advanced has not purported to be solely forward-looking, i.e. intended to suggest that the ECtHR should not apply the rulings in *Bărbulescu/López Ribalda* if WFH monitoring came before it in the future. Instead, I have sought to suggest that it *cannot* do so, without displacing other seminal cases on the enjoyment of private life at home. In turn, building on Philippa Collins's convincing and deeply worrying discussion of domestic case law, my post has sought to point to other relevant aspects of the ECtHR's jurisprudence, which employment courts and tribunals at the national level would be required under s.2 HRA to take into account, when assessing the fairness of any dismissals associated with monitoring during WFH.



About the author: Dr Eleni Frantziou is an Assistant Professor in Public Law and Human Rights at the University of Durham. Her main area of research interest is the application of human rights to private actors. She is the author of a monograph on the EU law dimensions of this topic, entitled *The Horizontal Effect of Fundamental Rights in the European Union: A Constitutional Analysis* (OUP 2019).

(Suggested citation: E Frantziou, 'The right to privacy while working from home ('WFH'): why employee monitoring infringes Art 8 ECHR', UK Labour Law Blog, 5 October 2020, available at https://uklabourlawblog.com)