HUNGARIAN LABOUR LAW
E - J O U R N A L

# A new side to employee participation

## *A possible tool to protect the employees' right to respect for private life in the era of digitalisation and data protection*[*]

**Katalin Bagdi**[**]

### 1. Introduction

Undoubtedly, employers collect and process great amount of data of a sensitive nature in relation to their employees, way before the employment relationship is established, and even after this relationship ceases to exist. It is not a new phenomenon in itself, however, digitalisation brought smart phones, mobile apps, notebooks, e-mail accounts and such into our everyday work, through which employers are able to collect a huge amount of data – even more than before – and keep track of a person's every move, not only during work, but even during the employees' private time if the employer chooses to do so.

Even if the private usage of such tools is prohibited, it is still inevitable that private information and personal data of the employees is disclosed. Especially because despite the new, flexible forms of employment, most of the workers still spend a substantial part of their life at the workplace, and thus often need to manage even their private tasks from the workplace. However, the use of digital tools at the workplace, including the fast-evolving artificial intelligence, gives a chance to the employer to gain such information about the private life of the employees that they would otherwise keep to themselves. This leads to an even greater imbalance of power, leaving employees more vulnerable.

In the following, the effect of digitalisation on the employment relationship will be analysed, focusing mainly on the protection of the private life of the employees.

* Supported BY the ÚNKP-18-3-IV-DE-222 New National Excellence Program of the Ministry of Human Capacities"

** PhD candidate, University of Debrecen, Marton Géza Doctoral School of Legal Studies. E-mail: bagdi.katalin31@gmail.com

In the third part comes the determination of the tracking tools available for the employer to monitor the employees' actions and performance even outside of the workplace and after working hours. Then the new challenges brought by these tools will be identified, with special regard to how these pose new threats to the right to private life at the workplace and affect the seemingly solid and clear definition of private sphere.

In the fourth part of the paper, a possible connection between employee participation and the protection of private life will be examined with regard to the increasing importance of data protection. After providing a summary on the right to participation, the human right nature of the employees' right to private life will be introduced briefly. Then the restrictive nature of data protection regarding the employer's growing presence in the employees' private life will be considered, pointing out how limited the state resources are to preserve private sphere at the workplace through data protection, despite it being a strong safeguard otherwise.

And lastly will be explored whether it is possible to connect employee participation and data protection in such a way that an even stronger defence is provided for employees' right to private life, thus identifying a new side to employee participation as well.

## 2. New methods of surveillance brought by digitalisation

The Fourth Industrial Revolution (4IR) is happening now meaning that the economy is driven by mobile internet, automation and artificial intelligence, which turn up in several – if not all – fields of economy, including manufacturing, logistics or transportation industry.[1] This means, that the 4IR also has an impact on employment as it brings information technology tools and digitalisation into the workplace. Efficiency reduces costs and raises income which is the main aim of the companies and their shareholders operating either on the local or the international market. The new tools provided by the present industrial revolution often ensure both cost reduction and income increase, as netbooks, tablets, smart phones and the built-in applications are also tools to monitor the employees at the same time, making it easier to enhance performance.

However, the use of such tools poses new kinds of threats to the employees, especially to their right to private life. The EU recognised the importance of data protection not only in general, but also with regard to the special situation of employees, and the result of that recognition is the General Data Protection Regulation (GDPR).

Recent cases showed that strict data protection rules, especially in case of consumers and employees are increasingly significant and are needed in order to guard the workers' private life which must be

[1] Christopher Mims: *Inside the New Industrial Revolution.* The Wall Street Journal. https://www.wsj.com/articles/inside-the-new-industrial-revolution-1542040187 (Last accessed: 13 November 2018)

protected even from those they do not have a direct connection with, but can access their personal (and mostly sensitive) data through those they do have a direct link to. The scandal of Cambridge Analytica brought several problems to the sunlight.

First, it became clear that collecting, selling and/or transferring data without the knowledge of the actual person, or using it for aims other than what was consented is remarkably easy. Secondly, even those were affected who did not have a Facebook account themselves, only had friends who in contrast did have a Facebook account. This highlights that not using a specific platform or application does not mean that one's data is safe and cannot be collected. And thirdly, "industry self-regulation has been a failure",[2] the state, the national and the EU legislator needs to take action in order to ensure the citizens' protection, even if it requires new means or to rethink existing institutions and adjust them to the new circumstances.

In addition, last year Amazon's smart voice assistant, Alexa showed that not only intentional infringement of data protection rules poses a threat, but faults or 'bugs' of the devices/applications the developer and owner do not know about can cause an incident and disclose personal data to known or unknown people without one's consent or one's knowledge.[3]

### *2.1. Emerging threats to employees posed by the evolvement of information technology*

From the point of employment, these conclusions are of great significance as employer's use more and more of these devices, applications and apply new forms of work in order to improve performance and productivity, reduce costs, provide work-life balance and to keep an eye on the employees as much as possible, thus often blurring the line between the workplace and private life,[4] leaving the employees with no or reduced protection. The introduction of technological tools and digitalised supervision systems in the workplace escalated in order to manage the employees in modern workplaces.[5]

Surveillance is not attributed only to blue-collar workers (e.g. workers in warehouses) as electronic performance monitoring (EPM) appeared in relation to white-collar workers.[6] Due to the availability of large unstructured databases and computing power, applications using some kind of artificial

---

2 https://www.businessinsider.com/facebook-cambridge-analytica-shows-the-need-for-a-new-privacy-law-2018-3/?IR=T (Last accessed: 11 November 2018)

3 https://www.businessinsider.com/amazon-alexa-records-private-conversation-2018-5 (Last accessed: 13 November 2018)

4 Fürjes, Annamária – Guba, Veronika Rita: Elektronikus eszközök használata a munkaviszonyban. In: Pál, Lajos–Petrovics, Zoltán (eds.): *Visegrád 15.0 – A XV. Magyar Munkajogi Konferencia szerkesztett előadásai.* Budapest, Wolters Kluwer, 2018. 367.; Kun, Attila: *Munkajogviszony* és *a digitalizáció – rendszerszintű kihívások* és *a kezdetleges európai uniós reakciók.* In: Pál–Petrovics (eds.) op. cit. 391.

5 Valerio De Stefano: *"Negotiating the algorithm": Automation, artificial intelligence and labour protection.* [Employment Working Paper No. 246.] Geneva, ILO, 2018. 7. [hereinafter: De Stefano (2018)]

6 De Stefano (2018) op. cit. 8.

intelligence (AI) and thus making predictions and decisions regarding routine, simple, mechanical – and sometimes even non-mechanical – tasks[7] appeared even at the workplace.[8]

Even though the access to such databases and the use of AI is anticipated to increase objectivity and impartiality regarding the employer's decisions such as during recruiting, the algorithm determining from which databases and how the AI learns, might re-create prejudices and biases (i.e. racism, sexism, etc.) and run the risk that the recruiting process applied by the employer consolidates these prejudices while giving the false illusion of objectivity[9] and amplifying information asymmetries.[10] The fact that the mass amount of data collected at the workplace in order to analyse work performance makes such risks even higher and may make the possible unfair treatment regarding pay rise and such solid without providing the employees (and candidates) any control over it.

The appearance of new forms of work such as work on demand via apps and the performance of activities or services online, irrespective of the location (crowdwork)[11] may expand the scope of employee surveillance and makes it easier as well which – in the long term[12] – might undermine the existing level of legal protection provided for employees due to the large amount of their personal data possibly held by online platforms and employers, which also shows a need for new legal policies of data protection in order to protect workers' right to privacy and confidentiality.[13] There are also concerns regarding the lack of voice of the employees using online platforms for work,[14] and such concerns do not relate only to crowdworkers and new types of workers, but to all employees being supplied with tasks and monitored through IT channels. The reduction of direct human contact between the employer and the employee, and also between the customer and the employee run the risk of dehumanisation of the workers and them being considered an "extension of an IT device or online platform".[15]

---

7 Ekkehard Ernst – Rossana Merola – Daniel Samaan: *The economics of artificial intelligence: Implications for the future of work.* [ILO Future of Work Research Paper Series, 5.] Geneva, ILO, 2018. 13.

8 *The impact of technology on the quality and quantity of jobs.* Issue Brief Prepared for the 2nd Meeting of the Global Commission on the Future of Work 15–17 February 2018, No. 6. Global Commission on the Future of Work, ILO, 2018. 6.

9 Ernst–Rossana–Samaan op. cit. 13.; *Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion)* European Economic and Social Council, 31 May 2017, JO C 288, 31.8.2017. 43.

10 Jon Messenger: *Working time and the future of work.* [ILO Future of Work Research Paper Series, 6.] Geneva, ILO, 2018. vii.

11 *Job quality in the platform economy.* Issue Brief Prepared for the 2nd Meeting of the Global Commission on the Future of Work 15–17 February 2018, No. 5. Global Commission on the Future of Work, ILO, 2018. 1.

12 Statistics show that employment through digital labour platforms is small at present (5% in Europe), however, with more and more jobs and tasks moving to the online space, digital employment will increase. [*Job quality in the platform economy.* Issue Brief Prepared for the 2nd Meeting of the Global Commission on the Future of Work 15–17 February 2018, No. 5. Global Commission on the Future of Work, ILO, 2018. 1.].

13 Ursula Huws – Neil H. Spencer – Dag S. Syrdal – Kaire Holts: *Work in the European Gig-Economy.* FEPS, UNI Europa, University of Hertfordshire, 2017. 51.

14 Valerio De Stefano: *The rise of the "just-in-time workforce": On-demand work, crowdwork and labour protection in the "gigeconomy".* [Conditions of Work and Employment Series No. 71.] Geneva, ILO, 2016. 21.

15 De Stefano (2018) op. cit. 5.

### *2.2. Surveillance at the workplace – A variety of tools to monitor employees*

If we accept that most of the employers use (digital) devices different from those of the past in order to carry out the monitoring of the workers, and that the new tools enable the constant and close surveillance of the employees, recording their every move, making it possible to follow the workers in real time or to search for a specific movement later, it can be directly concluded that the employer gathers and processes an unthinkable amount of data, having almost as great an authority above the employees as the state has over the citizens,[16] and the employer is enabled to use such means to monitor the employees that are similar to the tools the state and the intelligence services use when following the citizens.[17]

The surveillance of employees can take many forms, data – including personal data – are collected from various sources, and each method endangers the workers' privacy in a different way, especially because using various devices that record different types of data at the same time enables the employer to profiling, setting up typical human behaviour based on the collected data and, in some cases, to draw conclusions regarding the employee's political opinion, sexual orientation, personal tastes, physical and mental health, pregnancy including the intention to become pregnant or other fields of the employee's life that would not be disclosed for the employer otherwise.[18]

Methods of surveillance include "e-mail monitoring, phone tapping, tracking computer content and usage times, video monitoring and GPS tracking",[19] indicating among others productivity, efficiency, location, e-mail usage, web browsing, printer use, the number of breaks, social contacts, the time and duration of phone calls, the number of chat messages, etc.[20] Employees are often enabled or – in most cases – ordered to use wearable work instruments which register their movements and location minute by minute.[21] These wearables – including sociometric badges or sociometers[22] – measure the worker's work pace, the number of tasks done, the time needed for a specific task, and the number and length of breaks taken.

---

16 According to István Kukorelli, former judge of the Constitutional Court, the mere existence of CCTV cameras instill a sense of continuous visibility which automatically places the observer in a position of authority. Concurring opinion of judge István Kukorelli to decision 36/2005. (X. 5.) of the Constitutional Court, par. 1.

17 "You can become your own mini-NSA." said David Tucker, CEO of Australian-based Event Zero. https://www.cbc.ca/news/technology/how-new-data-collection-technology-might-change-office-culture-1.3196065 (Last accessed: 17 November 2018)

18 Andrea Peterson: *Some companies are tracking workers with smartphone apps. What could possibly go wrong?* https://www.washingtonpost.com/news/the-switch/wp/2015/05/14/some-companies-are-tracking-workers-with-smartphone-apps-what-could-possibly-go-wrong/?utm_term=.a27959afdaf8 (Last accessed: 17 November 2018). See also: Decision 36/2005. (X. 5.) of the Constitutional Court, Reasoning, IV.1.

19 De Stefano (2018) op. cit. 8.

20 See also Hajdú, József: *A munkavállalók személyiségi jogainak védelme.* Szeged, Pólay Elemér Alapítvány, 2005. 21–22. [hereinafter: Hajdú (2005)]

21 De Stefano (2018) op. cit. 7.

22 Sociometers are designed to measure „the amount of face-to-face interaction, conversational time, physical proximity to other people, and physical activity levels using social signals derived from vocal features, body motion, and relative location." http://hd.media.mit.edu/badges/ (Last accessed: 17 November 2018)

Analysing the data of all employees also enables the employer to see which workers spend their break together and thus can draw conclusions regarding the nature of the relationship between the workers, who are on good terms with each other and whether there is an outcasted and/or bullied employee. With the use of such devices, the employer is enabled to extract and analyse non-verbal features (speaking speed, tone of voice, conversational time, speech features, physical proximity to other people, physical activity levels[23]), individual and collective patterns of behaviour at the workplace including the behavioural change, predict human behaviour from unconscious social signals, identify social affinity among individuals working in the same team,[24] emotional states such as trust, stress, anxiety and interest, and furthermore conversational dynamics.[25]

It is questionable whether these conclusions are accurate as a specific behaviour can be induced by different reasons, and since these conclusions will also become a part of the data stored about the worker, false conclusions may affect future promotions and job opportunities in a negative way.[26] The use of these devices also runs the risk that the employer can follow the workers' every move even during their breaks and thus, based on their behaviour during their private time, it is possible to draw conclusions regarding the employees private life (e.g. which workers like to spend their private time together, where they spend their lunch, frequent visits to the bathroom can disclose health issues, etc.).

Regarding privacy, workers referred to the feeling of wearing sociometers as being Orwellian,[27] since the badges enable the employer to track the precise path a person takes through the office, and it seems that data collection can potentially be expanded to private areas of the workplace such as bathrooms.[28] Employees also compared the employer's tracking devices to a prisoner's ankle bracelet,[29] which shows that it makes them feel as if they conducted a crime and the situation is analogous to when the highest authority, the state restricts their freedom of movement and right to private life. A research suggests that depending on the workplace culture – and the employer's decision – wearing a sociometer might result in the invasion of the employee's privacy, since the settings make it possible to monitor every step taken.[30] This would reduce any reasonable expectation of privacy at the workplace

---

23 https://bmslab.utwente.nl/knowledgebase/sociometric-badges/ (Last accessed: 17 November 2018)

24 http://hd.media.mit.edu/badges/ (Last accessed: 17 November 2018)

25 Benjamin N. Waber – Sinan Aral – Daniel Olguin Olguin – Lynn Wu – Erik Brynjolfsson – Alex "Sandy" Pentland: *Sociometric Badges: A New Tool for IS Research.* 2011. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789103 (Last accessed: 17 November 2018)

26 In an experiment conducted by journalists voluntarily, the report compiled based on the data collected by the sociometer showed that a journalist was part of a group who talked more among themselves compared to other workers, and the final conclusion of the employer was that "Surely, they must be complaining." which clearly will influence the employers future attitude towards these workers when it comes to pay rise, promotion, etc. https://www.fastcompany.com/3051324/we-spent-two-weeks-wearing-employee-trackers-heres-what-we-learned (Last accessed: 17 November 2018)

27 Waber–Aral–Olguin–Wu–Brynjolfsson–Pentland op. cit. 30. https://www.fastcompany.com/3051324/we-spent-two-weeks-wearing-employee-trackers-heres-what-we-learned (Last accessed: 17 November 2018).

28 Waber–Aral–Olguin–Wu–Brynjolfsson–Pentland op. cit. 30.

29 Myrna Arias v. Intermex, http://s3.documentcloud.org/documents/2082322/myrna-arias-lawsuit.pdf. 4. (Last accessed: 14 November 2018)

30 Waber–Aral–Olguin–Wu–Brynjolfsson–Pentland op. cit. 31.

even regarding areas exclusively reserved for employee use such as bathrooms, break rooms or locker-rooms, which would infringe the employees' right to respect for private life.

While wearables are often used to instruct workers while tracking and measuring the speed and efficiency of every individual worker inside the building, GPS devices enable the employer to track employees even outside the building, measuring the speed and efficiency of managing a task, the number of breaks taken and determining whether the worker uses the vehicle to manage tasks not related to work. However, using GPS, especially when the worker is allowed to use the vehicle for private matters as well, may be considered an invasion of privacy. Employers often instruct employees to download apps onto their smartphone in order for the employer to track their activities. It is a relevant question though whether the employer requires the app being on even during off-duty, since the location and movement of the employee outside of work strictly belongs to the worker's private sphere and the employer cannot instruct the employee to disclose such information continuously and without a just cause.

Business-sponsored wellness programs or fitness wristbands provided by the employer also run the risk that the employer may track the workers even during their off-duty activities,[31] ending up in an endless surveillance without factual limits.

Teleworkers and remote workers are often monitored by taking screenshots of their computers and webcam photos[32] while also keeping track of keyboard activity, application usage including private messaging apps (e.g. WhatsApp), web-browsing patterns, text messages, the frequency of switching between apps, and keystrokes to determine the activities of the employee during working time.[33] There are softwares offered to employers which are able to scan the whole workplace network searching for specific words[34] or even context switching.[35] Some companies provide activity trackers to their employees and thus able to collect data on their sleep, physical activity and nutritional choices.[36]

Even though asking the employees to disclose their social network passwords is prohibited,[37] implementing tracking softwares with keylogging runs the risk of acquiring the workers' passwords to

---

31 De Stefano (2018) op. cit. 9.

32 For instance, the https://hu.clevercontrol.com/features/website provides real-time live and remote monitoring, and enables the following functions: monitoring website activity, application activity, search engines activity, keylogger, removable storages devices, recording screenshots, control printing, recording microhpone sound and webcam video, monitoring Facebook, LinkedIn and Skype activity.

33 De Stefano (2018), op. cit. 8.; https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology (Last accessed: 14 November 2018)

34 https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology (Last accessed: 14 November 2018)

35 Context switching is when a person suggests the others to continue the discussion in encrypted apps such as WhatsApp to take the conversation offline, „indicating that the subject matter is too risky for the corporate network". https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology (Last accessed: 14 November 2018)

36 https://hubstaff.com/employee_monitoring (Last accessed: 14 November 2018)

37 The employees clearly have a reasonable expectation of privacy on their own social network, especially if not all of their posts are open to the public but only to a few close friends. Therefore, the employer's request to disclose the relevant passwords and letting them look into one's own social network or e-mail account is not different then looking into a person's diary or personal correspondence clearly meant for a small group of people chosen by the employee, definitely excluding the employer. The latter is already clearly protected by the law, however, the former is no different in essence, that is why it is prohibited to ask an employee

their social network and private e-mail account. The European Court of Human Rights ruled that the employer cannot reduce private sphere to zero at the workplace and communications in the workplace are covered by the concepts of private life.[38] It would also be unrealistic to prohibit the workers from managing any and all private tasks from the workplace, especially if flexible working hours and home office are not provided.

Referring back to the malfunction of Amazon's Alexa, it must be highlighted that employer's tracking devices pose a possible threat of third parties accessing the personal data of employees, and corporate espionage raises the possibility of using the existing bugs. The more data the employer collect, the more vulnerable the employees become towards hackers and identity thieves, risking that other persons besides the employer invade the workers' privacy as the employer's actions and tools enlarged the digital footprint of the employees.[39]

### *2.3. An additional risk – The "paternalist" employer*

Employers – partly due to the paternalist nature of the employment relationship – intend to be 'omnipresent' in the lives of their employees even when they are off-duty. The idea that the nature of the employment relationship ensures a right to surveillance of the employees is also widely accepted by employers[40] and by scholars.[41] With the help of apps which are possible to switch on from a great distance, without the knowledge and consent of the employee,[42] the surveillance practically becomes limitless.

The already mentioned dehumanisation also makes such continuous presence in the workers' life seemingly right and just, especially when the employer provides devices for work, such as notebooks, smart phones, fitness trackers or sociometers which remain the property of the employer despite granting the employees possession over these.[43] Therefore the surveillance literally becomes endless as the employer is able to access the data any time without the employee's consent, even after the

to disclose their passwords. The Hungarian Labour Code provides protection from such employer requests, ruling that only such data or declaration may be asked from the employee which does not violate the employee's personality rights – including the right to private life – and is essential in connection with establishing, performing or terminating the employment relationship. Act I of 2012 on Labour Code, § 10(1)

38 Case of Bărbulescu v. Romania, Application no. 61496/08, 5 September 2017, § 80.

39 https://www.cbc.ca/news/technology/too-orwellian-companies-monitoring-personal-time-for-self-improvement-1.3196321 (Last accessed: 14 November 2018)

40 Hajdú, József: A munkavállalók magánszférájának védelme, különös tekintettel az adatvédelemre. *Acta Universitatis Szegediensis, Acta Juridica et Politica,* Tomus LXII, Fasc. 7. Szeged, SZTE ÁJK, 2002. 12. [hereinafter: Hajdú (2002)]

41 PAW (2012) opt. cit. 21.

42 Ifeoma Ajunwa – Kate Crawford – Jason Schultz: Limitless Worker Surveillance. *California Law Review,* Vol. 105. Issue 3. (2017) 772.

43 Ajunwa–Crawford–Schultz op. cit. 766–767.

employment relationship is terminated as the employers often have legal obligations to store such data in the long term.

## 3. The effect of digitalisation on the definition of employees' private life

Data protection and the right to respect for private life have a close connection. Though, it must be noted that the term 'data protection' is inaccurate and refers in fact not to the protection of the data, but to the protection of the data subject, meaning an actual person.[44] Privacy protection is a broader term and incorporates – among others – data protection, the protection of individual autonomy, the freedom of choice, physical and mental integrity, the protection of personal identity, freedom from surveillance, protection of correspondence[45] and the right to informational self-determination. The latter constitutes the active side of the right to data protection: the data subject can and is enabled to know and follow the route of his/her personal data and the circumstances of the use of his/her personal data.[46]

### *3.1. Arising difficulties in determining the line between employees' private life and the workplace*

Private sphere is not limited to the private premises of the employee,[47] though the exact extent of the employee's private life has long been in the focus of discussion of academics and practitioners, and the definition of private life varies greatly depending on the context and the environment in which it is used.[48] Due to the fast evolvement of the devices, softwares and applications people use on a day-to-day basis, these devices, electronic monitoring systems and tracking softwares installed on the work computer easily invade employees' privacy, and are able to record and collect sensitive data.[49] Thus the line between the workplace and the worker's private life becomes ever more blurred,[50] hence making it necessary to rethink what areas belong exclusively to one's private life and also the obligations of the employer in relation to the monitoring of the employees and of the work performed.

Even more so since, after our private life, the usage of Internet and social media became an essential part of our workplace as well, though fundamental rights shall be respected, regardless whether the

44 Halmai, Gábor – Tóth, Gábor Attila (eds.): *Emberi jogok.* Budapest, Osiris, 2008. 579.

45 Halmai–Tóth op. cit. 579–580.

46 Decision 15/1991. (IV. 13.) of the Constitutional Court, Reasoning III.2.4.

47 Decision 36/2005. (X. 5.) of the Constitutional Court, Reasoning III.2.

48 Hajdú (2002) op. cit. 4.

49 Decision 36/2005. (X. 5.) of the Constitutional Court, Reasoning III.2.

50 Hajdú (2005) op. cit. 20.

employee's presence and activity is online or offline.[51] Whether employees create a Facebook group/ Facebook message to discuss the actual tasks at the workplace on a regular basis, or they simply use it to private purposes, it enables the employer to collect personal data on these employees under the pretext of legal workplace surveillance.[52]

Therefore, even though the abovementioned tools technically enable the employer to invade the employees' privacy much more than before, some limits have already been established by legislators and courts with the help of data protection rules, trying to make an explicit line between the workplace and the private life by rethinking the definition of private life. Data protection aims to protect a person's private sphere by restricting third parties in acquiring, collecting, restoring and using personal data, especially with regard to sensitive data. Since there is a strong connection between one's private sphere and data protection, the latter is also considered as one of the limitations of the employer's right to monitor the employees and a tool to protect employees' private life.[53]

### *3.2. The shift in case-law in response to the new challenges when defining private life*

With regard to the above, it is necessary to rethink the extent of employees' private sphere and along what criteria privacy shall be determined. Since it is difficult to make such a distinction on the legislative level, it is the task of the national and regional courts and some have already taken the first steps. In a recent case, the ECtHR confirmed its guidelines set in the case of Bărbulescu, ruling that "in some circumstances non-professional data, for example data clearly identified as being private and stored by an employee on a computer supplied to him by his employer for professional use, may be deemed to relate to his 'private life'.", especially if the employer "tolerates the occasional use of work computer facilities by staff for their private use".[54] While it has great significance if the employee marked a file, folder or message clearly as private, there are also limitations on the employees' side as one cannot mark a whole hard disk as 'personal' or 'private' and take up a substantial amount of the storage space of the employer's computer.

In a French case an employee shared her opinion about the employer in a closed Facebook group composed of only fourteen people to whom the worker gave permission to join. Later, the employee was dismissed based on this opinion. The court ruled that a closed Facebook group with a few members is of private nature[55] and thus opinions shared there shall be considered a private discussion belonging

---

51 Hajdú (2005) op. cit. 20.

52 Gergely László Szőke – Zsolt György Balogh – Gábor Polyák – Balázs Rátai: *Privacy in the Workplace.* National Report on Hungary. PAW project, January 2012. 32. Available: http://pawproject.eu/en/sites/default/files/page/web_national_report_hungary_en.pdf (Last accessed: 17 January 2019)

53 Hajdú (2005) op. cit. 10.

54 Libert v. France, Application no. 588/13, 02 July 2018, § 25. and § 52.

55 Cour de cassation, Chambre sociale, Arrêt n° 1231 du 12 septembre 2018 (16-11.690) ECLI:FR:CCASS:2018:SO01231.

to the private sphere of the employee. This means that certain areas of Facebook are exclusively identified as the private life of the worker.

According to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), body cameras clearly invade the employees' private sphere, therefore, the use of such tools is hardly in compliance with data protection and employment rules.[56] As a general rule, it is not allowed to place CCTV cameras in areas which are for the sole purpose of continuous work (e.g. offices) in order to monitor the employees' performance and behaviour.[57] It is strictly prohibited to place such cameras in break rooms, changing rooms, showers, bathrooms and medical rooms[58] which are clearly meant to provide private time and private sphere for the employees at the workplace. It is not allowed to use monitoring systems with the purpose of influencing the employees' behaviour.[59]

Activating tracking apps without the employee's knowledge and consent on the work phone provided by the employer while not prohibiting private usage also constitutes an infringement of the right to respect for private life, especially if the application enables non-stop monitoring of the employee's movements by recording the exact location every 15 minutes[60]. Furthermore, it is actually irrelevant in such cases whether the employer banned private usage of the work phone because merely keeping the phone in one's pocket all the time, even after working hours, while having the tracking device activated all the time, enabled the employer to unlawfully monitor the employee's private time and collect data on the worker's off-duty location and movements.[61]

Despite the fact that courts and authorities on national and European level have already started to interpret the definition of private sphere and the reasonable expectation of privacy in the light of the technological developments and the new devices used for the surveillance of the employee, reshaping the term 'private life' is only beginning, still leaving more questions open than answered.

Nevertheless, it is undeniably necessary to look for new ways in the protection of employees' privacy either by finding new solutions or by rethinking existing institutions. Especially, because the employees themselves are often unaware of the fact that they are tracked and also unaware of the diverse apps and devices that the employer may use. Also, employees have no means to verify whether the employer informed them about the facts related to monitoring entirely and correctly. However, workers' representatives generally have more knowledge, means and rights to control the employer's actions, hence it is necessary to involve them in the protection of the employees' private life. As the interests of trade unions clash with the interests of the employer more frequently, this paper focuses

56 NAIH/2018/865/2/V.

57 NAIH-4384-2/2012/V.

58 NAIH-4384-2/2012/V.; Recommendation of the National Authority for Data Protection and Freedom of Information on the basic requirements of electronic monitoring systems at the workplace, NAIH-4001-6/2012/V., 5.

59 NAIH-4001-6/2012/V., 5.

60 In the actual case, the employee came to know only after 3 years that a tracking device was activated on his phone previously. Despite the employee's request, the employer refused to answer when and for how long the tracking device was activated. Mfv.I.10.077/2013/7.

61 Mfv.I.10.077/2013/7.

on employee participation which is rather based on cooperation with the employer,[62] excluding trade unions.

## 4. Rethinking employee participation from the perspective of data protection

Even though some accept the idea that employee participation is a form of democracy at the workplace and that the right of citizens to take part in the public affairs either directly or through their representatives is the basis of employees' rights to participate in the employer's decision-making[63] ("citizen at the workplace"[64]) which is analogous to the former, the extent of this right and whether it has a human right nature has long been the subject of disputes among scholars and legislators. While it is clear that people must have the right to take part in the decisions affecting them, the power of the company is derived from its shareholders who majorly bear the costs and risks of the company's operation, and not from the employees. Still, in order to gain quality workforce, workers must be closely and permanently involved in decision-making at all levels of the company.[65]

### *4.1. The position of employees' right to participate in international and EU law – A brief summary*

While there is a direct link between democracy and involvement in decision-making, it seems that, even at present, several EU member states reject the idea of employee participation becoming a fundamental right, partly because of the uncertain scope of co-determination issues, since this strong right clearly imposes strict limitations on the employer's decision-making power. Partly due to the various labour law systems, the approaches of workers' participation are situated on different parts of a scale, having total rejection of providing anything alike to the employees on one end, and with granting strong and effective participatory rights on the other.[66]

Such diversity may be derived from the governments' and nations' different economic and political perception of economic and employment rights, which might be the reason why attempts to incorporate

---

62 Lehoczkyné Kollonay, Csilla (ed.): *A magyar munkajog.* Vol. II. Budapest, Vince Kiadó, 2004. 174.

63 Szamuely, László*: Ipari demokrácia Nyugat-Európában? – Társadalmi reformok és gazdasági harc.* Budapest, Magvető, 1980. 7.; Dajka, Ferenc: *Hogyan éljen a dolgozó az üzemi demokráciával?* Táncsics, 1971. 5. Cited by: Erőss, László: *Az üzemi demokrácia és az emberi kapcsolatok. Fejezetek a társadalom-lélektan köréből.* Budapest, KJK, 1977. 27.; Gianni Arrigo – Giuseppe Casale: *A comparative overview of terms and notions on employee participation.* Geneva, ILO, 2010. 6.; Kiss, György: *Munkajog.* Budapest, Osiris, 2005. 441.

64 *Why co-determination? A collection of good arguments for strong workers' voice.* Hans-Böckler Stiftung (2017). https://www.worker-participation.eu/About-WP/Why-Worker-Participation (Last accessed: 11 November 2018)

65 *Final report of the EU High-level expert group on workers' involvement (Davignon group)*, 1997.

66 Sigurt Vitols: *The European Participation Index (EPI): A Tool for Cross-National Quantitative Comparison.* Background paper. European Trade Union Institute, October 2010, p. 2. https://www.worker-participation.eu/About-WP/European-Participation-Index-EPI (Last accessed: 26 January 2019)

the right to participation into international human right conventions failed in most cases. For instance, the International Labour Organization (ILO) does consider employee participation an important right, clearly stating though, that only in a narrow sense, defining the term as the participation in the employer's decision-making and not the participation in the employer's operation in general.[67] However, no ILO convention recognises employees' right to participation, neither in the broad, nor in the narrow sense.[68]

In 1996, Articles 21 and 22 of the revised European Social Charter – in accordance with the Protocol of 1988 of the European Social Charter – established separately the workers' right to information and consultation and the right to take part in the determination and improvement of the working conditions and working environment. It is obviously a quite broad right and so it would seem to guarantee employees' right to participation. However, the system of undertakings set up by the Charter makes it discretionary for the member states whether they choose to grant one or both of these rights to the employees or not. As of today, 34 member states ratified the Charter, out of which 4 member states grant the right to information and consultation, 2 member states grant the right to participation, and 21 member states grant both rights.[69]

The European Convention of Human Rights (ECHR) does have a considerably effective system to enforce the rights set out in the form of the European Court of Human Rights (ECtHR), however, no right to participate is established by the Convention. Even though the ECtHR could possibly state through interpretation that such a right is provided by the ECHR, however, it is not very likely to happen soon. The ECtHR is very careful when it comes to collective labour law rights and so far mainly interpreted the right to association as the right which encompasses for instance the right to strike. Based on the case-law of the ECtHR regarding the freedom of association, it is clear that employees right to participation falls outside the application of the ECHR, because works councils do not fulfil the requirement of 'voluntary'.[70] However, there is a rather broad case-law regarding the right to respect for private life, including private life at the workplace.

The harmonisation of labour law standards regarding employee participation also falls outside the scope of EU law,[71] even though it is an important aim of the EU to strengthen all forms of workers' participation in the Member States. That is why the Charter of Fundamental Rights of the European

---

67 Arrigo–Casale op. cit. 10.

68 The Workers' Representatives Convention, 1971 (No. 135) of the ILO establishes rules concerning the protection and facilities to be afforded to workers' representatives in the undertaking. However, in the convention's interpretation the term 'workers' representatives' does not automatically cover forms of employee participation such as works councils, only in case national laws contain such reference. In comparison, the convention does not contain such a restriction in relation to trade unions. ILO Convention No. 135., Art. 3.

69 Bounded by Art. 21 (the right to information and consultation): Ireland, Moldova, Romania, Macedonia. Bounded by Art. 22 (the right to participation): Armenia, Cyprus (only partially). Bounded by both: Albania, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Estonia, Finland, France, Greece, Hungary, Latvia, Lithuania, Russian Federation, Serbia, Slovakia, Slovenia, Sweden, Turkey, Ukraine. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/163/signatures?p_auth=KKx4GQFN (Last accessed: 11 November 2018)

70 Mümtaz Karakurt v. Austria, Judgement of 14 September 1999 (Application no. 32441/96).

71 Treaty on the European Union, Art. 5(3) and Treaty on the Functioning of the European Union Art. 145–149.

Union does not contain workers' right to participation, only the right to information and consultation within the undertaking.[72] Therefore, the right to participation including joint decision-making (co-determination) is not considered a fundamental social or employment right at EU level either, despite the fact, that earlier the European Community established the right to information, consultation and participation in the Community Charter of the Fundamental Social Rights of Workers in 1989.[73]

### *4.2. The employees' right to private life as a fundamental right*

While employee participation still lacks a human right nature and seems to be stuck at the point where only the weaker rights to be informed and consulted are granted, the right to respect for private life is clearly incorporated in many national, international and EU instruments.[74] In this respect, it is not relevant whether the right is specifically provided for employees as well, because employees are citizens as well at the same time, therefore in many cases it is impossible to differentiate between their status as an employee and their status as a citizen when it comes to private life.

There are opinions that "the possibility of management unduly and excessively compressing workers' autonomy and privacy is a structural feature of the contract of employment" and "unless regulation specifically limits managerial prerogatives, in the workplace, there is no legal protection against surveillance per se".[75] While it is true that the imbalance of power and the employer's strong right to control are main features of the employment relationship, existing fundamental human rights provided by national, international and EU legislation ensure protection of employees even without actual labour law legislation setting limits to employee surveillance since basic human rights, such as the right to human dignity and the right to respect for private life, exist even at the workplace and are preferred over the employer's right to monitor. Thus the state is expected to ensure through legislation that the right to private life prevails over the right to property[76] and the material interest of the employer, or at least a balance must be ensured between these two basic rights.

The ECtHR also interprets the employer's act of track and surveillance at the workplace in the light of the right to privacy, ruling that business activities are not excluded from the notion of private life either.[77] The ECtHR also stated that without prior notification of surveillance, monitor or

---

72 Charter of Fundamental Rights of the European Union, Art. 27.

73 Community Charter of the Fundamental Social Rights of Workers (1989), Art. 17.

74 See for instance the International Covenant on Civil and Political Rights (Art. 17.), the European Convention of Human Rights (Art. 8.), the Charter of Fundamental Rights of the European Union (Art. 7.), the Fundamental Law of Hungary (Art. VI.), or the Basic Law for the Federal Republic of Germany (Art. 10.).

75 De Stefano (2018), op. cit. 11.

76 Decision No. 22/2004. (VI. 19.) AB of the Hungarian Constitutional Court; Arany-Tóth, Mariann: A munkahelyi elektronikus megfigyelés jogszerűsége adatvédelmi nézőpontból. *Magyar jog,* 2008/3. 148–157.

77 Ivana Roagna: *Protecting the right to respect for private and family life under the European Convention of Human Rights.* Strasbourg, Council of Europe, 2012. 22.

investigation, the employee has a reasonable expectation of privacy at the workplace. E-mails sent from the workplace are also covered by the right to respect for private life.[78] It also must be noted that the respect for private life generally has two sides from an employment point of view: the employee's private life outside of working hours is subject to protection and so the employer cannot monitor it and cannot restrict it unreasonably and disproportionately; the other side of the right is that the employee has the right to social life even at the workplace, and so private social life in the workplace cannot be reduced to zero.[79]

This human-rights based approach of employees' right to privacy means that this right "can only be limited insofar as this is indispensable to the exercise of other human rights and that any limitations must be proportionate to this end", which "can indeed provide a meaningful general framework of protection that may prove beneficial, in contrast to spot-remedy approaches adopted in systems where recognition of workers' rights as fundamental rights is still lagging behind".[80]

### *4.3. Data protection as a restriction on the growing presence of the employer in the employees' private life – The limited resources of the state*

Several countries – including EU member states as well – and scholars reject the idea of promoting employee participation into a fundamental right fully and completely, so there is no genuine chance in the short or medium term to realise the idea. However, while it is true that the legislator can hardly determine the exact line between the workplace and private life in an abstract way, the state can and must establish institutions to ensure that the legal obligations are executed and the standards developed by the case-law are upheld by the employers. The legislation achieves its goals only if the legal rules are enforceable. The need to ensure enforceability[81] establishes a positive obligation on the state's side to take necessary and proportional, but effective measures.

This means that the protection of private life as a basic human right and individual freedom is not only ensured by the state refraining from interference (negative obligation[82]), it is also important to establish rules and institutions which ensure enforceability (positive obligation[83]). The GDPR itself imposes strict obligations on the states themselves besides the employers and other data processors, including the obligation to establish and sustain a monitoring system which provides adequate, immediate and continuous protection to data owners. Providing the (human) resources to such a

78 Roagna op. cit. 22.

79 Bărbulescu v. Romania [GC], § 80.

80 De Stefano (2018) op. cit. 19.

81 Marta Otto: *The Right to Privacy in Employment. A Comparative Analysis.* Oxford–Portland (Oregon), Hart Publishing, 2006. 196.

82 Halmai–Tóth op. cit. 84.

83 Ibid.

system clearly requires an enormous amount of money. The aim of the GDPR and the strict data protection rules in the realm of employment is clearly to balance the difference in power between the employer and the employees and to protect employees' private life.

While the improvement of employment conditions and the increase in the level of employment protection somewhat started to bring balance at the workplace, the 4IR brought the invention of tracking devices which expanded the existing information asymmetry to the employees' disadvantage. It is also the result of technical development that while employers are able to invade the employees' privacy more and more – often by ignoring the existing legal prohibitions and moral obligations – the state remains to be strictly bound by financial and legal issues when it comes to enhancing the efficiency of the investigation against the employer regarding workplace data protection.

Nowadays, however, the employer is the one being present in every field of an employee's life and the state is the one restricted from being omnipresent. This gives employers more room to invade and restrict the private life of employees since the tight central state budget and the limited resources do not enable the state authorities to investigate all employers and workplaces, neither periodically, nor constantly. Statistics clearly show that the states' resources regarding the monitoring of workplace data protection are quite limited and insufficient.

The NAIH increased the number of its staff in 2017 from 65 to 73 persons expecting a rise in cases due to the GDPR coming into force,[84] which number rose to 87 in 2018. In contrast, according to the Hungarian Central Statistical Office, 3,118,700 employees[85] were employed in Hungary in 2018[86] and there were 1,906,664 companies and other organizations which are possibly employers.[87] In the UK, according to the Office for National Statistics, there were 32.39 million people in work in 2018,[88] while there were 5.7 million businesses, 24% of which are employers (appr. 1,368,000).[89] In contrast, the Information Commissioner's Office (ICO) in 2017 had 472 staff (439 full time equivalents) of which 69 were new staff in order to prepare for GDPR,[90] though numbers suggest that a 70% increase in the ICO's budget – including hiring 200 new staff[91] – would be required.[92] In 2018, ICO's staff raised to 565 (528.5 in full time equivalent).[93]

---

84 Proposal No. T/503. on Hungary's central budget of 2019. http://www.parlament.hu/irom40/10377/adatok/fejezetek/01_naih.pdf, Par. III.1.

85 http://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_qli001a.html?down=2525 (Last accessed: 14 November 2018)

86 The NAIH has 1 investigator per appr. 36.000 employees/22.000 employers.

87 http://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_qvd018a.html?down=573 (Last accessed: 14 November 2018)

88 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/october2018 (Last accessed: 14 November 2018)

89 Chris Rhodes*: Business Statistiscs.* Briefing Paper Number 06152, 28 December 2017. House of Commons Library, 2017. 4.

90 Information Commissioner's Annual Report and Financial Statements 2016/17, https://ico.org.uk/media/about-the-ico/documents/2014449/ico053-annual-report-201617-s12-aw-web-version.pdf. 16. (Last accessed: 14 November 2018)

91 https://qz.com/1249076/the-uk-regulator-investigating-cambridge-analytica-gets-awesome-new-powers-next-month-but-it-cant-compete-with-private-sector-salaries/ (Last accessed: 14 November 2018)

92 Information Commissioner's Annual Report and Financial Statements 2016/17. 54.

93 https://euobserver.com/digital/141875 (Last accessed: 14 November 2018)

The staff number of EU Data Protection Authorities (DPAs) vary on a wide range, even if the numbers are applied per million inhabitants: Luxembourg 52.48, Malta 23.9, Ireland 20.9, Cyprus 19.89, Slovenia 18.39, Estonia 13.68, Latvia (2017) 12.82, Bulgaria 9.7, Czech Republic 9.45, Hungary 8.88, UK 8.03, Slovak Republic 7.36, Croatia 6.74, Netherlands 6.6, Sweden 6.5, Denmark (2015) 6.09, Belgium 4.67, Poland 4.21, Greece 4.09.[94] The numbers are quite different if calculated based on the number of employees, for instance Hungary has 28 staff per million employees, while the UK has 16. Clearly, the state can provide employee data protection staff in a limited number and this number – as everything – depends on the amount of money the state can provide for this task. The salaries offered to data protection professionals which are considerably lower than in the private sector are a clear sign of the state's limits. This also means that (experienced) data protection professionals will not necessarily join the DPAs as "the data-protection authorities simply don't have the necessary funds to compete with the private sector".[95]

If employers are aware of the limited (human) resources of the DPA that makes the potential legal consequences of breaching the data protection rules uncertain as the employers have a higher possibility of avoiding an investigation. Therefore, the possible and certain advantages of infringing the legal obligations and invading employees' private life might surpass the large but uncertain disadvantages. It is analogous to the efficiency of criminal punishments: if the chances of being caught and punished are high and administered with high certainty and swiftly, the number of crimes committed reduces irrespective of the severity of the penalty; however, if the punishment which could be imposed is severe but uncertain, deterrence will be low.[96] It is clear though that certain and swift 'punishments' of breaching data protection rules which themselves encourage the employers to abide by the law, require large amount of resources from the state. Close and continuous monitoring with the certain possibility of fines and penalty forces the employers to maintain the high level of protection not only during the occasional inspection of the authorities, but permanently and in the long term. However, the states clearly lack such amount of resources.

### *4.4. A possible role of employee participation in data protection – Complementing the protection provided by the state regarding employees' private life*

Providing the right to participation to employees and/or their representatives, however, could fulfil the state's positive obligation in connection with the protection of the employees' private life, and

94 https://euobserver.com/digital/141875 (Last accessed: 14 November 2018)

95 https://qz.com/1249076/the-uk-regulator-investigating-cambridge-analytica-gets-awesome-new-powers-next-month-but-it-cant-compete-with-private-sector-salaries/ (Last accessed: 14 November 2018)

96 William C. Bailey – Ronald W. Smith: Punishment: Its Severity and Certainty. *Journal of Criminal Law and Criminology*, Vol. 63., No. 4. (1973) 531.

hence mean the appearance of an 'internal watchdog' at the workplace in the sense of data protection. Employee participation in workplace data protection as a fundamental right would actually be an important tool to ensure that the employers respect the workers' right to private life at the workplace and off-duty. This idea is supported by the "enabling rights" approach of collective labour rights. Collective rights are sometimes referred to as enabling rights because they secure and effectively enforce other rights at the workplace – such as the right to privacy –, therefore "collective rights act as a fundamental tool to rationalise and limit the exercise of managerial prerogatives".[97]

Therefore, the lack of state resources does not necessarily imply that the legislator has no other means to ensure close and constant monitoring regarding data protection at the workplace. As it was mentioned before, employees lack any control over the employer's means to track them and gather data on them of a sensitive nature, thus workers lose their autonomy regarding their personal data, leaving them vulnerable towards the employer and sometimes towards third parties as well.[98] Data autonomy may be interpreted as a side of the right to respect for private life, thus constituting an essential human right the need for which has already been expressed.[99] There are also suggestions[100] and attempts to persuade the employers to involve workers' representatives in the creation of workplace data protection codes and policies and to allow specific monitoring means and the related procedure on the condition that the staff affected give their consent.[101]

The ILO's code of practice on the protection of workers' personal data includes provisions proposing the involvement of workers' representatives in certain areas of workplace data protection, along the already existing rights of representatives as the right to be informed, the right be consulted and the right to participate in certain decisions and measures of the employer. The ILO recommends granting workers' representatives the right to be informed of any data collection process and the rules that govern that process, the right to cooperate in developing policies on workers' privacy. The code would also provide a right to be informed and consulted concerning the introduction or modification of automated systems that process worker's personal data; before the introduction of any electronic monitoring of workers' behaviour in the workplace; and about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of the workers.[102]

97 De Stefano (2018) op. cit. 19.

98 The data collected through tracking softwares and devices purchased by the employer often stored on servers owned by the companies selling the software (device), and in some cases the evaluation of the collected data is also carried out by them. In addition, third parties may access employees' data due to poor security measures and as a result of corporate espionage.

99 Ajunwa–Crawford–Schultz op. cit. 775.

100 De Stefano (2018) op. cit. 22–23.

101 *World Employment Report 2001 – Life at Work in the Information Economy.* Geneva, ILO, 2001. 283.

102 *Protection of workers' personal data – An ILO code of practice.* Geneva, ILO, 1997. par. 5.8., 5.11. and 12.2.

Based on the commentary on the code of practice, it can be concluded that the more workers' representatives are given the opportunity to influence the employer's data processing practices, the less the employer has chances to collect data despite legal prohibitions, without the employees' consent.[103]

The EU legislator also expressed a need in the past to involve workers' representatives in monitoring the employer's measures regarding employees' personal data and a proposition for a directive specifically establishing a regulatory framework of data protection to employment-related issues was prepared. Even though the GDPR contains special provisions to employee data, it seems that these provisions give an incoherent and ad hoc impression, making it difficult to interpret the regulation as a coherent workplace data protection framework.[104] A need for a coherent, supplementary directive on data protection in employment relations is expressed, which should consider unions and workers' representatives as actors that can act on behalf of data subjects in the employment context, ensuring consultation on a regular basis between the social partners and the DPAs both at national and at European level.[105]

It is unclear though, whether the EU member states would agree to establish workers' right to participate in the employer's data protection decisions affecting them and thus granting the right to workers' representatives to take part in such decisions as it would constitute a major limit on the employer's discretionary power. However, it may be a subject to examination whether such an interpretation of existing fundamental rights and national or EU employment rules can be established by courts and authorities which would allow to lay the foundations to the right of participation in the employer's data-related decisions affecting employees.

For instance, Hungary established a works council system similar to the German model which was expressly the role model at the time. Even though compared to the German works councils the Hungarian ones were granted few rights, especially regarding co-determination, the existing provisions of the Labour Code[106] might provide an opportunity to interpret them in favour of employee participation. Art. 262 (1) of the Labour Code states that works councils shall monitor compliance with the provisions of employment regulations, which include monitoring compliance with data protection rules. The Labour Code is silent what rights the works council has in case of finding a breach of rules, but in practice the works council can at least either persuade the affected employee to take adequate measures either before the DPA or – if necessary – before the court, or to notify itself the DPA that the employer does not respect the data protection rules in relation to the employees. Also, Art. 264 (2) c)-d) states that employers shall consult the works council prior to passing a decision in respect of

103 Protection of workers' personal data (1997), commentary to par. 6.11.

104 Paul De Hert – Hans Lammerant: *Protection of Personal Data in Work-related Relations.* Directorate General for Internal Policies. Brussels, European Parliament, 2013. 67.

105 Hert–Lammerant op. cit. 69.

106 Act I of 2012 on the Labour Code.

processing and protection of personal data of employees and the implementation of technical means for the surveillance of workers.

In case the employer breaches the obligation to consult with the works council, the works council is entitled to file a suit against the employer before the court. However, this right to be consulted is quite weak as the employer is only obliged to initiate a discussion with the works council regarding the means planned to adopt, and in case of fulfilling this requirement, the employer can completely disregard the opinion of the works council in the end. This means that the employees do have a voice to express their thoughts, but they still lack the control over the applied measures.

Analysing existing national laws and practices in this field does hold a significance as it would reveal whether EU member states already have legal rules similar to the Hungarian ones that are a great foundation for granting the right to participation and can be interpreted even now as providing workers' representatives an entitlement to influence the employer's decisions regarding the processing of employee personal data and surveillance devices and procedures.

What is clear and definite is that all EU member states and the EU itself provides employees the right to respect for private life, ensuring that the employer has limits while monitoring the worker. However, ensuring this fundamental human right at the workplace is only possible in my opinion if the following three requirements are met: (1) workplace data protection measures are transparent, (2) workers and their representatives are provided the opportunity to influence the employer's decisions in relation to the personal data of employees, and (3) the state and/or the employees (representatives) monitor whether the first two requirements are met and whether the employer abides by the data protection rules. While (2) is also important in order to protect the private life of employees, it must be noted that monitoring compliance and having the opportunity to notify the authorities in case of a violation of legal rules may also be considered a way of influencing the employer's decisions, at least in the sense whether the employer decides to respect the existing legal rules or breaches them.

Providing employees the right to take part in the decisions on the types of devices used at the workplace, steps taken to prevent incidents, the methods of protecting the employees' data and private sphere, the actions taken in case of an incident, etc. furthermore enables the employees to enforce the protection of their private life at the workplace as they get a greater view on the devices used by employer for their surveillance and also on the applications the employee needs to use for work.

This resonates with the growing need to educate employees how technology works, what the possibilities and limitations are when it comes to the (private) use of devices provided by the employer and the improvement of employees' digital literacy in general is also needed due to the fast changing technological environment.[107] Employees often lack the knowledge of their rights relating to their

[107] https://channels.theinnovationenterprise.com/articles/uk-government-calls-on-businesses-to-embrace-the-fourth-industrial-revolution (Last accessed: 14 November 2018)

private life as well.[108] The state itself lacks adequate financial and human resources to (re-)educate employees on job-related electronic devices and the limits of a worker's private life and the employer's right to monitor.

It would be more efficient if employees having the right to be involved in the employer's decisions in connection with procedures affecting employees' data would educate the employees at the workplace themselves. That would also bring the issue much closer to the workers, personal experiences and the possibility to associate what one learns to their own circumstances make data protection much more real and physical. While education organised by the state is also essential, it would be too general in itself without the specific knowledge related to the workplace. Therefore, another reason to ensure the right to participate in the employer's decisions regarding workplace data protection is that it enables to provide adequate education to the employees both in technological and in legal issues which is more accurate and sensible from the employees point, and it is cheaper for the state since it is enough to train workers' representatives who then will pass the knowledge to the employees.

With regard to the above, it can be concluded that workers' representatives – including works councils and other participatory forms – are in possession of the knowledge and means to monitor the employee in relation to workplace data protection. Providing employees the right to take part in decisions regarding the improvement of data protection policies at the workplace ensures that the employer can exercise its right to track employees while puts a stop to the feeling of the tracking being Orwellian. Especially, because employees referring to their surveillance as Orwellian or it being a prisoner's ankle bracelet does show that the main problem with employee tracking from the worker's point of view is that an employee does not have any influence over when and how to be tracked since most of them do admit that surveillance itself is not unreasonable and some forms of it feel quite natural.

Otherwise, the dehumanisation effect of technology gains space even at non-platform workplaces if workers have no voice and control over their surveillance conducted against them. The 'human-in-command' principle may be interpreted as such that besides others it also refers to the employees being in command at least partly when the monitoring of their work is carried out by algorithms. It is not enough if the employer or a third party is in command over the algorithm, as it is important to ensure the command of those affected and being monitored by the algorithm, AI or an advanced tracking device. If we accept that collective bargaining may contribute to ensure human-in-command,[109] than it is possible to be carried out through workers' representatives and their right to participate in all decisions and processes that focuses on data protection and surveillance at the workplace.

---

108 Johnathan Yerby: Legal and ethical issues of employee monitoring. *Online Journal of Applied Knowledge Management,* Vol. 1., No. 2. (2013) 53.

109 De Stefano (2018) op. cit. 23.

## 5. Summary and conclusion

While the main aim of employee surveillance is to improve working performance, another reason of close monitoring is the employer's paternalist attitude towards the employees which explains why employers have a tendency of wanting to monitor even the workers' private life.[110] Another reason might be that employers fear of the worker's private life affecting the employee's work performance and workplace behaviour. A rather exaggerated case was when the employer started to check the employees' Facebook profile in order to prevent fraud, looking for changes for instance in their relationship status from married to divorce, based on the – not necessarily true – assumption that the costs of divorce could put a person under pressure to commit fraud.[111] Therefore employers use softwares and devices which track the employees' every move not only at the workplace and during working hours, but enable the employers to disclose information regarding the workers' private life which run the risk of a retaliation professionally due to personal choices in private life.[112]

It also occurs that since people spend most of their day at the workplace and as more and more tasks are possible to manage online, the need to manage private matters from the workplace increases. However, this also contributes to the blurring of boundaries between work and private life, making the employees much more vulnerable towards the employer and often leaving them unaware of the surveillance and tracking the employer carries out against them.

The EU – sensing the growing importance of data protection – introduced the GDPR, however, it only consists a few provisions regarding workplace data protection and several issues are left to the authorities and courts to solve the disadvantage of which is that case-law at the beginning is random and uncertain, taking a long time to become coherent as various problems arise later in time. It seems though that a few legal questions have already been addressed by the ECtHR and national laws with regard to the right to respect for private life which is provided at the workplace as well.

Ensuring the right to privacy when technically the employer can access any personal data of the employees and is able to track and monitor their every move is rather important. However, without providing adequate tools to enforce the respect of this right against employers, the right to private life becomes illusory and theoretical. National DPAs struggle with the boost in the number of cases due to GDPR and some are still understaffed, suggesting that financial and human resources of the state are fairly limited. Hence DPAs are able to monitor and investigate a limited number of employers, and thus a considerable number of data protection rule violation may remain unnoticed.

---

110 "If you are a parent and you have a teenage son or daughter coming home late and not doing their homework you might wonder what they are doing. It's the same as employees.". Brad Miller, CEO of Awareness Technologies. https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology (Last accessed: 14 November 2018)

111 https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology (Last accessed: 14 November 2018)

112 Peterson op. cit.

The original goal of employee participation was also to substitute the state's authority at the workplace due to the state's limited presence, and as an enabling right, workers' participation is an adequate tool to ensure that the employer respects the employees' right to private life, especially because providing employees control over the algorithms and advanced devices used to track them is inevitable in order to avoid implementing the fear and constant feeling into the employees that Big Brother is watching them day and night, in and outside of work. Granting employees (and their representatives) the right to take part in the employer's decision in work-related data protection issues would be an adequate supplement to DPAs representing state authority, ensuring that less infringement remain unnoticed and that the line between private life and the workplace will become more distinct.