Reinforcing Privacy Protection in the Workplace Through the Use of OSH (Occupational, Safety and Health) Law

Loïc Lerouge, Elena Sychenko

Reinforcing Privacy Protection in the Workplace trough the Use of OSH (Occupational, Safety and Health) Law

Loïc LEROUGE

PhD, Research Director at the French National Centre for Scientific Research (CNRS)

Centre for Comparative Labour and Social Security Law (COMPTRASEC UMR 5114, CNRS-University of Bordeaux)

Elena SYCHENKO

Associate Professor

Faculty of law, Saint-Petersburg University

Abstract

Digitalization progresses represent huge challenges to employee's privacy at work, in particular taking into account the e-monitoring issues. Even though a number of European and International instruments provide legal framework for employee's privacy protection at work, information and communication technologies (ICTs) used for monitoring in the workplace require the elaboration of a deeper understanding of what privacy at work is and what are the boundaries of employer's managerial power. Work-related stress is also one of the consequences of e-monitoring. Hence, the legal challenge will be to develop a concept of the employee's right to control the e-monitoring practises. This right can be perceived in our opinion, as a part of prevention and protection OSH strategy. In other words, from fundamental rights bases, we will elaborate the concept of employee's right to control the use of ICTs in the workplace in order to prevent the risk of work-related stress arising from a context of illegitimate e-monitoring and surveillance practices.

Technologies such as keylogging, screenshotting, RFID chips, geolocation of employees are often used in the absence of employee's consent and even awareness of them. Doubtlessly such monitoring is can lead to humiliate the employee and exposes him to the risk of stress at work. The results of such monitoring even though in the majorities of countries cannot be used as a legitimate proof of misconduct for the purpose of sanctioning an employee still might be used for decision making on the worker's career, or might be used for putting pressure on employees to make him quit from job "voluntarily".

The use of some ICTs can cross the barrier of the employee's private life and generate confusion between workplace and private place. In addition, some practices are aggravated by collecting biological data in order to evaluate the employee's health at work because of a healthy workplace policy in the company.

In conclusion, the aim of this paper will be to analyse new challenges to employee's privacy at work and to elaborate a legal concept related to the employee's right to control the use

of e-monitoring, including safeguards against such intrusions. We will provide arguments for the use of ICTs as a part of ensuring OSH at work for determining the e-monitoring programmes installed or used by an employer.

Keywords

Privacy at work – OSH strategies – E-monitoring – ICTs use at work – Work-related stress – Role of legal rules – Work-life balance

Plan

Introduction

Progress in digitalisation represents huge challenges to an employee's privacy at work, in particular taking into account e-monitoring issues. E-monitoring increases management control over the employee, creates additional pressure and can foster the feeling of insecurity in the employee. The management's capability to track and pinpoint a worker's individual contribution separates him from the group of co-workers and makes him feel more vulnerable to his employer.

In the famous Charlie Chaplin's film released in 1936 workers were subject to video monitoring even in the factory's bathroom.[1] In the beginning of the 20th century this film was a kind of sarcasm for the Taylor's scientific approach on the organisation of labour and strict measuring of each working operation. However, in the 21st century, from the point of view of a modern spectator there is very little sarcasm in this film. Some workers

1 Charlie CHAPLIN, Modern Times (1936), https://www.youtube.com/watch?v=HAPilyrEzC4, see by 5:22.

nowadays might find a lot of common points with their own workplace, which might also have much more sophisticated means for monitoring: keylogging, "screenshotting", RFID chips, geolocation, biometrics, connected tools. Who knows how far we can we go through the potential of such technologies such as facial-recognition which potentially provides detection methods incompatible with an anti-discrimination policy?[2] In some workplaces, these technologies are used in the absence of the employee's consent and even awareness of them.

The results of such monitoring cannot be used as a legitimate proof for the purpose of sanctioning an employee in most countries. Still, the information received might be used for decision-making on the worker's career, or might be used to put pressure on the employee to make him/her quit their job "voluntarily", and as such can be a focus of workplace bullying.

The uncontrolled use or the misuse of information and communication technologies (ICTs) and the data they can collect possibly exposes employees to a high risk of work-related stress.[3] Hence, the applicable law is not only related to privacy but also related to occupational safety and health. A lot of data concerning employees is collected and analysed by HR departments (e.g. for career management, hiring, training, payroll processing, schedules for example). It might refer to controlling the employees activity at work (e.g. schedule control, rise of geolocation devices, biological data, video monitoring, etc.) or for ensuring security (e.g. control of access to the workplace, professional alerts, shared-information checking, etc.).

The collection and the use of the data obtained through e-monitoring suggests the need for the development of a concept of employees' right to control e-monitoring practises. The risk of buttressing managerial prerogative and reifying "the status of employee as servant entitled only to such liberty as employers permit[4]" leads to a "call for

2 See for example "What Your Face May Tell Lenders About Whether You're Creditworthy", *The Wall Street Journal*, 10 June 2010.

3 DESSLER (2011); SMITH and AMICK (1989, 275-290); AMICK and SMITH (1992, 6-16).

4 FINKIN (2017 and 2018); HALLINAN, LEENES, GUTWIRTH, & de HERT (2020); LEENES, (2019); van der SLOOT, BROEDERS & SCHRIJVERS (2016).

comprehensive regulatory action, as evidenced in much of the world, not adventitious individual suits for damages.[5]" The aim is also to reduce the "disparity between the notion of privacy in professional literature and on the ground[6]" by new legal approaches.

The legal challenge is to consider this right as a part of privacy policies and justify its being subject to OSH strategies. Our study will address the concept of employee's privacy at work, consider international and some national frameworks for its protection and analyse new technological challenges to privacy in the light of international instruments (Part 1). Having established the insufficiency of existing legal safeguards we will consider the intrusion of privacy in terms of occupational health, arguing that the right to control the e-monitoring should be guaranteed as an OSH right and should be considered within the prevention and protection policies (Part 2). This is a strong challenge for the future of work which must be prepared and anticipated now in the face of highly invasive practices that will become potentially unavoidable and unmanageable. The stakes are very wide but essential to the respect of fundamental rights at work. It is therefore appropriate to ask original questions with some lines of response and reaction before considering a broader research work.

I. International and National Legal Frameworks on Privacy Protection: The Adequacy of Safeguards in Question

Even though a number of European and International instruments provide a legal framework for an employee's privacy protection at work, information and communication technologies used for monitoring in the workplace require the elaboration of a deeper understanding of what privacy at work is and what are the boundaries of the employer's managerial power. This is why we will first try to define this right and define its boundaries through an employer's rights and managerial power which need to be balanced with the employees' privacy rights. The international and national frameworks created to ensure this balancing at the workplace will be examined in Part A, while the new forms of the interference with the employee's right to privacy will be analysed in Part B.

1.1. Delimiting Employer's Rights and Managerial Power Boundaries

5 *Ibid.*

6 KATSABIAN (2018).

Judge Brandeis and Samuel D. Warren wrote in 1890 that the right to life should be understood in an evolutionary way and include the right to be left alone.[7] The authors justified their conclusion by referring to the intensity and complexity of life, arguing that solitude and privacy had become more essential to the individual due to modern enterprise invading upon his privacy and that such intrusion subjected an individual to mental pain and distress, such pain being far greater than could be inflicted by mere bodily injury.[8] Contemporary scholars continue to refer to the analogous circumstances for urging the protection of privacy, adding globalisation and the threats of terrorism into the mix.[9]

However, more than a century after the publication of this article, neither scholars nor case law have elaborated a unique definition of privacy or private life. Existing notions of privacy are often criticised for being extremely vague and lacking a precise legal connotation.[10]

The need to regulate this field was already evident in 1970 when the Resolution 428 (1970) was adopted by the Consultative Assembly of the Council of Europe.[11] This instrument defined the right to privacy as the right to live one's own life with a minimum of interference. European Union (EU) Charter of fundamental rights acknowledged the right of everyone to the protection of personal data concerning him or her.[12] The adoption of EU Regulation 2016/679 of the European Parliament and of the Council of 27 April

7 WARREN and BRANDEIS (1890).

8 *Ibid.* p. 196.

9 See PAGALLO (2008, 37).

10 See RODRICK (2014, 372); ARNAUD (2007, 129-156).

11 Resolution 428 (1970), *Declaration on mass communication media and Human Rights*, Consultative Assembly of the Council of Europe http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=15842&lang=en

12 Charter of Fundamental Rights of The European Union, *OJEU* 2000/C 364/01 https://www.europarl.europa.eu/charter/pdf/text_en.pdf

2016 on the protection of natural persons with regard to the processing of personal data (EU GDPR) is the most recent development in this field in the EU.[13]

This Regulation establishes very strict rules regarding data processing and has been adopted by the EU member States. With its enactment the concept of "Privacy by design" has become part of legal requirements: according to article 25 EU GDPR it is expedient for the controller (e.g. Employer) to integrate the "necessary safeguards into the processing of data*"* in order to meet the requirements of the Regulation and protect the rights of data subjects.

It should be emphasised that although the norms of this regulation are binding only for EU countries (even if most of them already had a developed set of norms on this point), it might be indirectly relevant for the countries of the Council of Europe. For instance, in the recent case considered by the European Court of Human Rights (ECtHR) in 2017, Barbulescu v. Romania[14], the Court largely relied on the norms of this instrument and formulated its new advanced approach to the workers e-privacy in view of the high standards established in EU Regulation. Therefore, once a case on employee's privacy is brought before the Court against any non-EU country subject to the European Convention on Human Rights it is very likely that the way of consideration of the case and the level of requirements for the accommodation of employee's privacy at work will be the same. Thus, the ECtHR framework for consideration of infringements of privacy at work is equally relevant for Switzerland, Russia or Turkey.

Turning to national privacy protection, it must be noted that the right to respect private life is provided for in most European constitutions. The recognition of this right was also a first step towards the protection of an employee's privacy. General claims for privacy protection have been translated in employment law through special legislation, such as in the case of the Finnish Act on Protection of Privacy in Working Life adopted in 2001,[15] or

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJEU* 2016/L 119/O1.

14 ECtHR, Bărbulescu v. Romania (61496/08)GC 05/09/2017, para. 80.

15 See HENDRICKX (2002).

by the introduction of relevant norms to main employment laws such as the *Statuto dei Lavoratori* in Italy in 1970,[16] *Estatuto de los Trabajadores* in Spain in 1995,[17] or the Labour Code in Russia in 2001.[18] French provisions on employment privacy were inspired by scholar publications on computerised forms of workers monitoring.[19]

Balancing the employee's right to privacy with the employer's property and managerial power and rights is the main problem arising on both levels. Prof. Hendrickx pointed out that the employee's right to privacy is qualified by the employer-employee relationship and therefore the employee's privacy expectations must necessarily and be accordingly "reduced."[20] However, it could be said that the right to privacy cannot be reduced to nothing. By analogy with the preliminary question of the Tele2 Sverige AB sentence, made by CJEU on December 21, 2016, "the generalised and undifferentiated storage of data, since it exceeded the limits of the strictly necessary[21]" is contrary to EU law.

There is not any unique vision of the benchmark for such a "reduction." The ECtHR's approach by the Grand Chamber judgement in Barbulescu case[22] can be considered as a reference providing a benchmark for an employee's privacy protection and guidelines to employers as to how not interfere with the employee's privacy for the purposes of property

16 Article 4 of Statuto Dei Lavoratori Legge 20 maggio 1970 n. 30) prohibits audio-video methods of workers'surveillance; See also Codice In Materia Di Protezione Dei Dati Personali. Decreto legislativo 30 giugno 2003, n. 196) that sets out requirements to protect personal information including the sphere of employment relations

17 Article 4 provides for the right of employees to respect for their privacy and dignity. Available at: http://www.boe.es/buscar/doc.php?id=BOE-A-1995-7730 (accessed 29.05.2019)

18 Chapter 14 of the Russian Labour Code "The protection of employee's personal data" which prohibits any gathering or use of such information without the consent of employee.

19 HENDRICKX (2002).

20 HENDRICKX (2002, 185).

21 CJEU, joined cases: C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department contro Tom Watson and others of 21 December 2016, ECLI:EU:C:2016:970, published in the electronic Reports of the cases cited by LIAKOPOULOS (2020).

22 See supra note 13.

protection. This ruling also lists the factors which should be taken into account by national courts while considering relevant cases:

- notification of the possibility that the employer might take measures to monitor an employee, and of the implementation of such measures. The notification should normally be clear about the nature of the monitoring and be given in advance;
- the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy (distinction between monitoring of the flow of communications and of their content, time and space limits, the number of persons who have access to the information); robust reasons to justify accessing their content of communications and the impossibility to use less intrusive methods;
- the consequences of the monitoring for the employee subjected to it, the use made by the employer of the results of the monitoring operation;
- provision of adequate safeguards which should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.[23]

The elaboration of these rules was an important contribution to employee's privacy protection in Europe. National courts were constantly confronted with this problem for almost the last 30 years and their approaches differed from country to country. For instance, the Spanish Supreme Court stated that the right to workplace privacy does not prevent employers from monitoring employees.[24] The Spanish Constitutional Court in 2000 acknowledged that video surveillance and video recording of an employee could be justified if the employer had detected irregularities in the performance of the employee's contract, and such surveillance and recording did not (in those circumstances) constitute a violation of the employee's privacy if it resulted in an appropriate, necessary and balanced measure for assessing the veracity of the employer's suspicion of serious violations on the

23 ECtHR, Bărbulescu v. Romania (61496/08)GC 05/09/2017, para. 121.

24 Tribunal supremo 4ª, sentencia de 19/07/1999, cited from Colección De Sentencias Relativas A La Actuación De Detectives Privados, APDPE. Sevilla, 2010. Available at: http://apdpe.es/sites/default/files/Jurisprudencia.pdf (accessed 20/05/2019).

part of employee.[25] In France, rules were made as far back as 1987 stating that an employer could not open employees' personal lockers unless employees were notified in advance and the lockers were inspected for reasons of periodic cleaning.[26] In 1998, the French State Council[27], in a case concerning secretly installed video cameras in a petrol station cash booth, ruled that the employer was not entitled to rely on evidence obtained in breach of an individuals' rights via those cameras so as to justify dismissals.[28] The same line of reasoning can be found in the decisions of Italian Courts. The French State Council in 2000 stated that photos obtained from cameras installed at the workplace in order to check the fraudulent conduct of the worker, without informing the latter, could not be used as evidence in the proceedings.[29] In later cases, however, Italian courts have expressed a more employer-friendly legal position, permitting "defensive" control of employee's mail in order to establish a behavior which endangers the employer's business provided that it did not amount to "significant elimination of any form of guarantee of the employee's dignity and privacy."[30]

The Russian courts adopt a fundamentally different approach and their case law is an example of arbitrary employers' managerial rights sacrificing the privacy rights of employees. Any instalment of monitoring facilities are found to be in line with law without any research of its necessity and proportionality, there were cases when the employee was disciplined for putting up balloons in order to mask the video camera that was filming only

25 Sentencia 186/2000 de Tribunal Constitucional, 10/07/2000, available at: http://www.boe.es/boe/dias/2000/08/11/pdfs/T00029-00036.pdf (accessed 20/05/2019).

26 See Société Gantois, Conseil d'État, 12 June 1987 and Centre Renault Agriculture, Conseil d'État, 9 October 1987, cited from FORD (2002, 146).

27 The French Council of State is judge, legal advisor of the Government, carries out studies and follows enforcement of courts' decisions.

28 *Ibid.*

29 Suprema Corte di Cassazione, Sentenza 17 giugno 2000 n. 8250, cited from Monica GOBBATO, Controllo dei lavoratori: le pronunce del Garante e la recente giurisprudenza, published 21.07.2006. Available at: http://www.altalex.com/documents/news/2006/07/21/controllo-dei-lavoratori-le-pronunce-del-garante-e-la-recente-giurisprudenza (accessed 20.05.2019).

30 Corte di Cassazione, sezione Lavoro, Sentenza 3 aprile 2002, n. 4746.

her working place all day long, including breaks and before – after-working hours.[31] Even the lack of employee's notification about video monitoring is not considered by national courts as the factor evidencing the infringement of privacy rights.[32] In one case the redundancy procedure was justified by the employer by providing data regarding the use of the business computer for social network communications. This data made the employer think that the employee did not have enough work and can be dismissed for redundancy reasons. The court considered this evidence as admissible without any research into the employee's notification or the limits of surveillance.[33]

We can only guess how many cases of interference with the employees' privacy remain non-reported to the courts or the labour inspections. This field often remains completely within the employer's discretion and often the employee can suspect that the monitoring is taking place when he/she is addressed with comments on his/her performance or there are comments on something he/she did during the day. The list of methods of interference with the employee's privacy in the digitalised world is open. It comprises relevantly old ones as video or audio recording, widely used by the employers and new methods of surveillance. As such we can list the employee's psychological testing, keylogging and "screenshotting" at work and the geolocation of employees. The availability of covert equipment which can be easily bought on the Internet,[34] the possibility to use as such a simple smartphone, the variety of programmes for spying leave the employee very vulnerable to the abuse of his privacy and well-being at work. The existing frameworks do not protect employees from such abuse. All the legal norms referred to above can only be efficient once the employee knows about the e-monitoring and can prove it. None of the privacy protection frameworks guarantee an employee's right to check the use of these methods of surveillance. There are

31 Decision of the Judicial Board on civil cases of the Orenburg Regional Court of December 3, 2014 in case No. 33-7039 / 2014; See also: Appeal decision of the Krasnoyarsk Regional Court of November 14, 2012 in case No. 33-9899, Appeal decision of the Altai Regional Court of 15 October 2013 in the case of N 33-8403 / 2013

32 The decision of the Leningrad district court of the city of Kaliningrad on 05/25/2017 in case No. 2-2243 / 2017.

33 Appeal decision of the Novgorod Regional Court of June 6, 2012 in case No. 2-1935 / 12-33-823

34 On websites as eBay, Alibaba, etc.

no safeguards against such abuse if the employer does not use the obtained data in judicial proceedings. An employer remains free to use this data in a covert way while making decisions on redundancy, promotion, bonus payments and so on.

It is worth bearing in mind here the quote of Judge Brandeis: "such intrusion [with the right to privacy] subjected an individual to mental pain and distress, such pain being far greater than could be inflicted by mere bodily injury."[35] Indeed, unauthorised intrusions with privacy might lead to the deterioration of the employee's health, create a hostile environment at work and the feeling of vulnerability. To substantiate this argument, we will further consider the possible technologies of unauthorised[36] monitoring at the workplace.

1.2. Forms of the Interference with the Employee's Right to Privacy

In order to show clearly how some technologies are able to interfere with the employees right to privacy and how they could be so invasive, polygraph testing (1) and new methods of employee's monitoring (2) will be analysed according to privacy issues in the workplace.

1.2.1. Polygraph testing

is a way to gather the information the employee does not wish to share. Such testing is required by some employers in misconduct investigations or suspicion in fraud/material damage/information disclosure cases. In Russia[37], Ukraine,[38] Kazakhstan[39] polygraph testing is widely used to ensure regular checks of some categories of public servants. The employees are required to sign a paper affirming their voluntarily agreement to undergo such testing, however the refusal to undergo such testing will amount to disciplinary misconduct in the case of public employees. For private employees such refusal

35 WARREN and BRANDEIS (1890, 196).

36 "Unauthorized monitoring" is understood broadly in this paper as including all the processes of private data gathering without the employee's voluntary consent.

37 Order of the Ministry of Internal Affairs of Russia No. 201 DSP "On Approving General Requirements for the Procedure for Psychophysiological Research Using a Polygraph", March 18, 2010.

38 The Law of Ukraine on the National Police No. 580-VIII.

39 Decree of the Government of the Republic of Kazakhstan, June 19, 2014, No. 683.

traditionally leads to further pressure being put on employee to make him "voluntarily" quit the job, or declaring him redundant.[40]

According to the ILO Code of Practice "Protection of workers' personal data" polygraphs, truth-verification equipment or any other similar testing procedure should not be used by employers.[41] The prohibition recommended by ILO is rarely implemented in national law. Domestic legislation often remains silent on the use of the polygraph and such tests are widely practised in employment relations. One can easily find on the Internet advertising on "lie detector" services for employment screening processes which "significantly reduce the possibility of volatility in the workplace in the future."[42] There are cases where the refusal to undergo a polygraph test or the information on misconduct gained through such tests constituted the reasons for dismissals.[43]

This context and these evolutions raise several questions: Do such dismissals violate the human right to respect private life? Does polygraph testing interfere with the right to dignity and constitute a degrading treatment or could it be considered so only in the light of procedural requirements of the right to a fair trial? Does it in the end provoke an employee's stress and lead to deterioration of his health? The same questions can be asked regarding the evolvement of facial-recognition technology. To answer these questions, it is interesting to remember the case considered by the ECtHR in 2013, Fazliyski v. Bulgaria, and speculate about the possible approach of this court to polygraph testing. In this case the applicant as a result of polygraph testing was declared mentally unfit to work at

40 Decisions of Russian courts: No. 2-6210 / 2016 of July 26, 2016, Leninsky District Court of Orenburg (Orenburg Region); No. 2-14381 / 2016 of March 31, 2017 Central District Court of Chelyabinsk (Chelyabinsk Region).

41 ILO code of practice Geneva, International Labour Office, 1997, p. 3

42 https://www.ukliedetectortest.co.uk; the same may be found at: https://liedetectors-uk.com (accessed 20.08.2019).

43 US case: O'Brien v. Papa Gino's of America, Inc., 780 F.2d 1067 (1st Cir. 1986, cited from WARREN (1994, 149); See Bulgarian case considered by the ECtHR: FAZLIYSKI v. BULGARIA 40908/05 16/04/2013; Decisions of Russian courts: No. 2-6210 / 2016 of July 26, 2016, Leninsky District Court of Orenburg (Orenburg Region); No. 2-14381 / 2016 of March 31, 2017 Central District Court of Chelyabinsk (Chelyabinsk Region)

Bulgarian Ministry of Internal Affairs and dismissed. The results of the test were classified and the applicant was not allowed to see it. The applicant claimed the violation of the right to a fair trial and did not argue the violation of his right to privacy (article 8 of the European Convention of Human Rights [ECHR]).

However, let us imagine that Mr Fazliyski did claim the the violation of his right to privacy. The Court in this case would have firstly considered whether the necessary polygraph test constituted the interference with the right respect for private life. We will try to surmise such reasoning: parties to an employment contract have a mutual implicit obligation of trust and confidence. The necessity of passing a polygraph test in certain circumstances or a general requirement to periodically undergo such testing vividly demonstrates the absence of confidence. Such rules create the climate of distrust and offend an employee's dignity. Scholars note that polygraph testing also constitutes profound intrusion into the personal zone of privacy as it is directed at the human mind and thought, which are core interests protected by personal privacy.[44]

Therefore, the obligation to undergo polygraph testing can be considered as an interference with the right to respect private life, in particular, the right to physical and psychological integrity of a person.[45] We can admit that it was in accordance with law, as there were relevant instructions and regulations. Without going deeply into the assessment of the quality of law in this case we will proceed with the review of the legitimate aim. In our view, the employer, the Ministry of Internal Affairs, would prove that it was acting in the interests of national security and public safety.

The next step of consideration should be aimed at establishing the necessity of the interference. Remembering the ECtHR approach to privacy protection as discussed in this paper, such examination shall permit the Court to discover whether the employer might have chosen less invasive methods to reach the aim pursued. It should also take into account the relevant scientific data on validity of data obtained by polygraph testing.

44 Craig (1999, p. 18).

45 ECtHR, G.B. and R.B. v. The Republic of Moldova (16761/09) 18/12/2012.

The employer in our case had to determine whether the employee was mentally fit for work in the Ministry of Internal Affairs. We suppose that he might have used for that a number of methods without involving "highly offensive"[46] polygraph testing. The requirement to provide the medical certificate on psychological health seems to be the most appropriate way for that.

The research regarding the validity of polygraph testing as such demonstrates that the accuracy of indexes is far from perfect,[47] that too many factors may impact upon the applicability of the polygraph to determine deception,[48] that "the bulk of polygraph research can accurately be characterised as theoretical".[49] A number of commissions that have reviewed if such tests are reliable have concluded that they are not.[50]

In our opinion, these scientific assessments of polygraph use is more than enough to conclude that any obligatory polygraph testing of employees should be found unnecessary in a democratic society. Thus, without any need to proceed with the proportionality analysis we can conclude that in our imaginary case the Court would be very likely to find that there was a violation of article 8 of the ECHR.

These reflections illustrate that polygraph testing, if carried out at the will of an employer, is strongly incompatible with the right to privacy.

1.2.2. New methods of employee's monitoring

New methods of employee's monitoring, such as keylogging and "screenshotting", are also incompatible with the right to privacy. Keylogging means installing special software, permitting the recording of every keystroke made by a computer user, especially in order

46 This epithet is cited from the judgment of US court and reflects the impact of this type of testing on employee's personality. O'Brien v. Papa Gino's of America, see supra, note 38.

47 FIENBERG, BLASCOVICH, CACIOPPO, DAVIDSON, EKMAN, FAIGMAN, ... & McCUTCHEN (2002, 149)

48 MEYER & WEAVER (2013, 155); SAXE, DOUGHERTY & CROSS (1985, 355-366).

49 NATIONAL RESEARCH COUNCIL (2003, 102).

50 *Ibid*; Scientific Validity of Polygraph Testing: A Research Review and Evaluation (1983) A Technical Memorandum. Washington, D. C.: U.S. Congress, Office of Technology Assessment (OTA-TM-H-15), available at: http://ota.fas.org/reports/8320.pdf (accessed 28.11.2019);

to gain fraudulent access to passwords and other confidential information.[51] "Screenshotting" is the use of special programmes permitting the screen capturing of an employee's computer or any other device, and sending the images to the employer's account, it is up to the employer to set a custom time for capturing screens.

Here is the small list of citations from the advertisement of such software: "interception of pressed keys on the keyboard", "recording screen shots", "interception of personal messages in social networks", the last but the most eloquent citation is "it is almost impossible to notice this programme and delete it from the computer."[52]

The information provided in the advertisement is enough to conclude that these methods of monitoring represent a deeper interference with the right to privacy than video-surveillance or the monitoring of e-mails. Both these methods provide access as to the content of the sent documents and to any drafts which might contain "raw" ideas or certain mistakes/misunderstandings. Thus, the employer might become aware of the information that the employee did not wish to disclose to anyone at all and was going to erase from the computer. The right for dignity is evidently at stake in this case. The severity of interference with this right is evident, these programmes are aimed at making transparent the ideas and writings of the employee which perhaps he never thought might become public. This interference, in our opinion, cannot be justified by balancing employee's privacy with the employer's rights. There would be in any case less intrusive methods for maintaining workplace discipline, such as, for example, reviewing the flow of the information or controlling the results of work. The secrecy of such software, as the main publicised trait of these applications, means that no safeguards to the employee's privacy right are available.

We assume that the profound intrusiveness of such interferences beats to the very heart of an employee's right to private life and his right to dignity. Defining dignity is not an easy thing, scholars noticed that it can be used for different contradictory purposes[53] and might be defined according to a particular purpose. Dignity carries with it a suppletive

51 Oxford dictionaries. https://en.oxforddictionaries.com/definition/keylogger (accessed 20.04.2020).

52 See, among others, https://www.mipko.ru/covert-surveillance, https://neospy.net, https://hubstaff.com.

53 VINCENTI (2009), cit. from PAPA (2012).

character which makes it possible to protect new rights which do not find refuge under the cover of other legal principles. Dignity is considered as a cornerstone of human rights by providing them an explanation and legitimacy.[54] By ensuring the primacy of the human being, dignity enforces the principle of protecting the physical and mental integrity of the person, *a fortiori* in the workplace. Axiom in major international and national legal texts, dignity is the essence of humanity like freedom is the essence of human rights. Hence, we suppose that certain methods of monitoring due to their high intrusiveness or, we might say, offensiveness for the person concerned, cannot be justified under any circumstances because they represent the violation of the very core principle of labour law and attack the fundamental right of an employee. These kinds of deep intrusions into an employee's private life evidences inadequate working conditions and should be considered as an occupational hazard. In other words, occupational safety and health law is one of the responses to the invasion of privacy at work.

2. Intrusion with Privacy: An Occupational Health and Safety Issue

Occupational safety rules have significantly evolved during the last 30 years. Scholars have noted that the scope, direction and magnitude of OSH have evolved both at national and international levels.[55] According to the ILO Occupational Safety and Health Convention, 1981 (No. 155) the aim of the national policy shall be "to prevent accidents and injury to health arising out of, linked with or occurring in the course of work, by minimising, so far as is reasonably practicable, the causes of hazards inherent in the working environment." Occupational Safety and Health Recommendation, 1981 (No. 164) fixes the obligation of the States "to undertake or promote studies and research to identify hazards and find means of overcoming them." The list of hazards is naturally growing with the development of science and technologies. In our opinion, the risk of e-monitoring might also be integrated into OSH assessment policies.

54 BENCHIKH (1999, 37-52).

55 Benjamin O. Alli, *Fundamental principles of occupational health and safety*. Second edition. ILO, 2008, p. 4.

The ILO recommends to focus on working environment surveillance, among other factors, organisation of work and psychosocial factors.[56] Consideration should therefore be given to criteria and actions for the planning and design of healthy and safe workplaces in order to establish working environments that are conducive to physical, psychological and social well-being.[57] We suppose that the intrusion with the employee's privacy is one of the factors of the working environment. The infringement of an employee's privacy is a hazard to a worker's health and well-being at work. Therefore, we suppose that hazard surveillance at work which is defined by scholars as "the process of assessing the distribution of, and the secular trends in, use and exposure levels of hazards responsible for disease and injury",[58] should include the assessment of e-monitoring policy.

Again, in Chaplin's movie "Modern Times", the tramp finally suffered a nervous breakdown at work and had to quit. Employees of today are luckier: work-related stress is acknowledged as an occupational risk,[59] there are publications evidencing the impact of e-monitoring on the level of stress.[60] However, what lacks today is a possibility to estimate the level of intrusion with the employee's privacy at work as a part of a stress prevention policy. The need is to allow a right to check the instalment of secret e-monitoring software, which should be granted to the employees, the Trade Unions and the safety representatives.

The link between occupational health and safety regulation and the need to protect privacy at work is straightforward: since occupational safety rules should cover physical, mental health and ensure dignity protection; intrusions with privacy should be considered as an occupational risk. Therefore, such intrusions should be determined, prevented,

56 ILO: Technical and ethical guidelines for workers' health surveillance, Occupational Safety and Health Series, No. 72 (Geneva, 1999). See also Convention 190, Article 9 (b).

57 ALLI (2008, 94).

58 KOH, AW (2003, 705-710).

59 VERCAMER (2018); WHO (2003).

60 Eurofound and the International Labour Office, Working anytime, anywhere: The effects on the world of work, Publications Office of the European Union, Luxembourg, and the International Labour Office, Geneva, 2017; European Agency for Safety and Health at Work, Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025 European Risk Observatory Summary. Luxembourg: Publications Office of the European Union, 2018.

monitored and controlled as other occupational risks. Such risk will be more significant in respect of employees whose activities present particular value for the employer and the lack of supervision of whom might lead to significant harm. For instance, it appears that the employees having access to commercial and state secrets, those who are working with money (cashiers, sellers) and other values, executive officers, high ranked managers are more exposed to the risk of being abusively monitored. The EU Directive 1152/2019 on transparent and predictable working conditions in the European Union reminds the legal obligation of the employer to inform employees on ongoing basis about the conditions defining the working environment in which they work.

Such monitoring is a breach in the right to dignity that is enshrined in a number of constitutions and in specifically fixed in labour legislation in some countries. For instance, the Constitution of Italy[61] does not directly mention the dignity of the employee, but it is made by interpretation of several articles.[62] In 1989 the Court stated a fundamental possibility of limitation of employer's power by the dignity of employee.[63] Section 1 of the Italian Employees' Act 1970 is devoted to the Liberty and dignity of employee and thus proclaims **t**he right for privacy as a foundation of dignity by: 1. fixing the prohibition of supervision on the working process by security guards, 2. forbidding the use of audiovisual equipment and other equipment for the purpose of distant control of the activity of employees[64], 3. prohibiting employer's assessments of the suitability and disability of

61 Italian scholars find a double constitutional interpretation of dignity: as a necessity in material terms, which is suitable for guaranteeing a dignified existence; and as a wider notion, which obviously implies the first, but which 'takes into consideration all the other social conditions which make the individual "a fully participating member of society" see Papa (2012) and Marella (2007).

62 Of Articles 3 (proclaiming equal social dignity of people), art. 35 (protecting all forms of labour), art. 36 (protecting wages that must be sufficient for "free and dignified existence"), art. 41 (limiting economic freedom by "safety, liberty, and human dignity"). Italian scholars consider that idea of protection of human dignity is implicitly present in many other Constitutional provisions. (see D. Bifulco, Inviolabilita dei diritti sociali, Napoli, 2003, pag. l24 cit. from PICCININI (2005, p. 743).

63 Cit. from GUGLIELMUCCI (1997).

64 Exception is made by judicial practice by allowing video registration of employee's work without notice if there is a suspicion of his illegal conduct (see Cass. sez. Legge n. 4746/02, Secur-pol srl / Pizzutelli NI., CED rv. 553469, e v. n. 15892/07, Piluso / Eni spa, cit. from Corte di Cassazione Sezione 5 Penale Sentenza

employee, 4. general prohibition of personal security check of employees. Article 2087 of the Italian Civil Code obliges an employer to protect the physical integrity and personality of employees. Judicial practice in Italy gives a wide interpretation of this norm, using it for protecting employee's dignity from offensive, or humiliating conduct of an employer, harassment, mobbing in the cases when anti-discrimination mechanisms are not applicable.[65] The same might also be spread upon protection from abusive e-monitoring.

As the use of the monitoring methods discussed in this paper violate the employee's right to dignity and the respect for this right is acknowledged to be the main part of a worker's well-being at work[66] this situation might be considered in the context of ensuring protection from psychosocial risks, therefore as a part of OSH issues. A number of scholars have highlighted that e-surveillance increases the level of stress at work and that monitoring creates a hostile environment at work.[67] The consequences of monitoring through the use of the programmes discussed in this paper might be even worse as the lack of opportunity to check or to delete them develops the feeling of vulnerability and insecurity. The use of the data collected through such monitoring is another important issue. Once the abuse of the employer's right to monitor the employee's performance has been detected the recorded data should be erased.

According to the EU framework directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work[68] "The employer

---

del 1 giugno 2010, n. 20722), though in the later practice was underlined that "such data cannot be used to prove the breach of contract of employment" (see Sentenze Cassazione civile sez. lav. 01 ottobre 2012 n. 16622)

65 The Supreme Court of cassation held that the employer's power aimed at production maximizing must be limited by the necessity of protection of the safety, freedom and human dignity of employee (la Corte suprema di Cassazione, decisione del 14 febbraio 1997 n. 8267).

66 Valentina Forastieri, Improving health in the workplace: ILO's framework for action: www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/publication/wcms_329366.pdf (accessed 13.05.2018)

67 See for instance WATSON (2001), AIELLO and KOLB (1995), AMICK and SMITH (1992), MARTIN, WELLEN, and GRIMMER (2016).

68 Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work, *OJEU* A83, 29.6.1989, p. 1.

shall have a duty to ensure the safety and health of workers *in every aspect related to the work*" (Article 5 § 1); "within the context of his responsibilities, the employer shall take the measures necessary for the safety and health protection of workers, including prevention of occupational risks and provision of information and training, as well as provision of the necessary organisation and means. The employer shall be alert to the need to adjust these measures to take account of changing circumstances and aim to improve existing situations." (Article 6 §1). The employer shall carry out occupational risks assessment and is in charge of ensuring occupational health and safety prevention policies "in every aspect related to the work" as the ECJ reminded us it in its ruling Commission of the European Communities v Italy adopted on November, 15th 2001.[69] We suppose that this obligation includes occupational risks in terms of work-related stress, harassment and discrimination caused in some circumstances by the intrusion in the privacy of the employees by some employers.

By the way, this approach can be found in the European Social Partners Agreement on Digitalisation[70]. Indeed, the agreement raises a paradox, that of the possibility of securing the workplace and ensuring better working conditions thanks to digital technologies and the progress of artificial intelligence, but also the risk that these technologies may compromise human dignity, particularly in cases of personal surveillance. The agreement recommends clear rules on personal data to limit the risk of intrusive surveillance and misuse of personal data. To achieve this, the agreement refers to Article 88 of the EU GDPR, which provides for rules on the processing of employees' personal data in the context of employment relationships. This article refers to the possibilities of establishing specific rules at Member State level, by law or collective agreements, to ensure the protection of the rights and interests of workers with regard to the processing of personal data. The agreement also suggests measures to be taken to protect workers from misuse of personal data. The first measure is to allow employee representatives to address this issue through consent. Consent must be obtained by making the concrete and transparent details

69 ECJ, Commission of the European Communities v Italian Republic, Case C-49/00, European Court reports 2001 Page I-08575, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0049.

70 https://www.etuc.org/en/pressrelease/eu-social-partners-reach-agreement-digitalisation.

of the data collection clear to them. Data should not be collected because it is technically possible or for an undefined future purpose. Finally, in a pragmatic way, the agreement suggests providing labour representatives with digital tools to enable them to carry out their duties in the digital age.

Conclusion

The need to protect the right to privacy together with the right to establish safe working conditions makes us conclude that new safeguards are needed to protect employees from e-monitoring, polygraph tests (even eventual facial recognition) which is a huge infringement to the very heart of human dignity. The recognition of the employee's right to check the installation or the use of such programmes through the installation of other special programmes might be such a safeguard.

The provision of the same right to labour inspections is also of value. It is also necessary to take seriously the risk of privacy intrusion, to include it within the list of occupational hazards, to assess it and to provide employers with the frameworks for its prevention. The prevention of the privacy intrusion risk is a complex and multidimensional task, it will require labour inspection systems to have special competences, digital resources and institutional capacity, which should be achieved through the appropriate training in line with the development of digital technologies.

The right of employees to control e-monitoring practices should be recognised as part of the right to safe working conditions. The satisfaction of this right will notably pass through a rigorous control of the authorisations, coupled if necessary with the anonymisation of the data, and the automatic and definitive deletion of the data at the end of the recommended period of conservation.

The employee has the right to be informed of the "conditions of his working conditions" with the possibility to control and to give his/her consent to the e-monitoring practices by having access to the collected data with a right of opposition or control by the labour inspectorate. This right would itself be integrated within the law of health and safety at work. Criteria and actions for designing safe workplaces should therefore take into account harmful disorders caused by e-monitoring in order to create a working environment

conducive to physical, psychological and social well-being without any violation of privacy and arbitrary supervision of workers.

A requirement of transparency and information of the penalties related to the violation of rights regarding the protection of privacy must weigh on the employer as to the form and substance of the information to be transmitted. The fulfilment of this requirement will be conditioned on the employers' ability to provide an unambiguous explanation of how the employees' personal data will be collected and processed. The establishment of a e-monitoring system must also be conditioned by the opinion of the personnel representatives. In addition, the use of spyware can lead to decisions that meet the qualification of discrimination. Such an assumption, if it is proven that these data were used in the decision-making process, would open the possibility for the employee to go to court in order to obtain removal of the discriminatory measure and the compensation of the damage suffered.

Under this perspective to provide safeguards to employees about the use of their private data, it would be also a matter of integrating these actions from the conception of the work organisation projects, to lay down the borders or the links between health and safety at work and dignity. Positioning oneself with an approach that takes into account an ethical reflection aimed at questioning or raising awareness of the impact of decisions made in terms of control and surveillance on the health of the targeted workers could be another approach.

Bibliography

AIELLO J. R., and KOLB Kathryn J., 1995, "Electronic performance monitoring and social context: Impact on productivity and stress", *Journal of Applied Psychology,* 80.3: 339.

AIELLO J. R., 1993, "Electronic performance monitoring", *Journal of Applied Social Psychology*, 23. 499-507

ALLI B.O.,2008, *Fundamental Principles of Occupational Health and Safety*, ILO, Geneva

AMICK III, BENJAMIN C., and SMITH Michael J., 1992, "Stress, computer-based work monitoring and measurement systems: A conceptual overview", *Applied Ergonomics*, 23.1: 6-16

ARNAUD S., 2007, "Analyse économique du droit au respect de la vie personnelle : application à la relation de travail en France", *Revue internationale de droit économique*, Vol. t. XXI, 2, issue 2, p. 129-156

BENCHIKH M., 1999, "La dignité de la personne humaine en droit international", *in* PEDROT P. (ed.), Éthique, *Droit et Dignité de la personne, Mélanges en l'honneur de Christian Bolze*, Economica, Paris, 1999, p. 37-52

CRAIG, J. D., 1999, *Privacy and employment law*, Hart Publishing Limited

DESSLER, G., 2011, *Human resource management*, Harlow, (12th ed.). UK: Pearson Education

FIENBERG, S. E., BLASCOVICH, J. J., CACIOPPO, J. T., DAVIDSON, R. J., EKMAN, P., FAIGMAN, D. L., ... & McCUTCHEN, S. R., 2002, *The polygraph and lie detection*, Committee to review the scientific evidence on the polygraph, NASA Report

FINKIN; M. W., 2018, *Privacy in employment law*. (Fifth edition. ed.) Bloomberg BNA

FINKIN, M. W., 2017, Chapter 7: Privacy and Autonomy. *Employee Rights & Employment Policy Journal*, *21*(2), 589-621.

FORD M., 2002, "Two conceptions of worker privacy", *Industrial Law Journal*, 31.2, p. 135-155

GUGLIELMUCCI C., 1997, "Potere imprenditoriale,dignità dell'uomo lavoratore e parità di trattamento", *Diritto del lavoro*, 1997, n 1-2, p. 25-26

HALLINAN, D., LEENES, R., GUTWIRTH, S., & DE HERT, P. (Eds.), 2020, *Data protection and privacy: Data protection and democracy*, Hart Publishers, Computers, Privacy and Data Protection Serie (No. 12)

HENDRICKX F., 2002, *Protection of workers' personal data in the European Union*, European Commission, Available at: http://ec.europa.eu/social/main.jsp?catId=708 (accessed 20.05.2019)

KATSABIAN, T., 2018, "Employees' Privacy in the Internet Age – Towards a New Procedural Approach", *Hebrew University of Jerusalem Legal Research Paper*, No. 18-19, 29 March

KOH D., AW T., 2003, "Surveillance in Occupational Health", *Occupational and Environmental Medicine,* 60:705-710

LEENES, R., 2019, "Regulating new technologies in times of change", *in* Reins L. (Ed.), *Regulating New Technologies in Uncertain Times*, Information Technology and Law Series; Vol. 2019, No. 32, Heidelberg: TMC Asser Press | Springer, p. 3-17

LIAKOPOULOS D., 2020, "The Protection of Personal Data According to CJEU and ECtHR jurisprudences", *International Journal of Digital and Data Law*, Vol 6

MARELLA M., 2007, "Il fondamento sociale della dignita umana. Un modello costituzionale per il diritto europeo dei contratti", *Rivista Critica di Diritto Privato*, Vol. 25, n° 1, p. 67-103

MARTIN Angela J., WELLEN Jackie M. and Grimmer Martin R., 2016, "An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours", *The International Journal of Human Resource Management*, 27.21: 2635-2651.

MEYER, R. G., & WEAVER, C. M. 2013, *Law and mental health: A case-based approach*, Guilford Publications

NATIONAL RESEARCH COUNCIL, 2003, *The Polygraph and Lie Detection*.: The National Academies Press, Washington, DC

PAGALLO U., 2008, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè Editore

PAPA V., 2012, "Dignity as the foundational paradigm of Labour law", *European Journal of Social Law*, No 1. March 2012, p. 14-40

PICCININI I., 2005, "Sulla dignità del lavoratore", Argomenti di diritto del lavoro, N° 3, p. 739-743

RODRICK S., 2014, “Open justice, privacy and suppressing identity in legal proceedings: 'what's in a name?' and would anonymity 'smell as sweet'?”, *in*: Normann Witzleb, David Lindsay, Moira Paterson, Sharon Rodrick (eds.), 2014, *Emerging Challenges in Privacy Law: Comparative Perspectives*, Cambridge University Press

SAXE L., DOUGHERTY D., & CROSS, T., 1985, “The validity of polygraph testing”, *American Psychologist*, 40(3), 355-366.

SMITH Michael J., and BENJAMIN C., AMICK III, 1989, “Electronic monitoring at the workplace: Implications for employee control and job stress”, *in* Sauter Steven L., *Job control and worker health*, John Wiley and Sons Ltd, Wiley series on studies in occupational stress p. 275-290

van der SLOOT B., BROEDERS D. & SCHRIJVERS E. (eds.), 2016, *Exploring the boundaries of Big Data*, Amsterdam University Press, Amsterdam

VERCAMER S., 2018, “Stress at work”, *Report. Committee on Social Affairs, Health and Sustainable Development*, 4 December, URL: http://website-pace.net/documents/19855/4491159/20181204-WorkStress-EN.pdf/6c87997b-366a-4a92-8e80-b540d4cc06d8 (accessed 20.06.2019)

VINCENTI U., 2009, *Diritti e dignità umana*, Laterza, 4th ed., Bari

WARREN F., 1994, *Internal Company Investigations and the Employment Relationship*, Greenwood Publishing Group, 1994

WARREN Samuel D. and BRANDEIS Louis D., 1890, “The Right to Privacy”, *Harvard Law Review*, Vol. 4, No. 5 (Dec. 15), p. 193

WATSON N., 2001, “The private workplace and the proposed “notice of electronic monitoring act”: is “notice” enough?”, *Federal Communications Law Journal*, 54(1), 79-104

WHITMAN James Q. and FRIEDMAN Gabrielle S., 2003, “The European Transformation of Harassment Law”, *Columbia Journal of European Law*, Vol. 9, p. 341-274

WHO, 2003, *Work Organisation & Stress: systematic problem approaches for employers, managers and trade union representatives*, Geneva, http://www.who.int/occupational_health/topics/stressatwp/en/