Białostockie Studia Prawnicze
2019 vol. 24 nr 2

DOI: 10.15290/bsp.2019.24.02.03

Václav Šmejkal
ŠKODA AUTO University,
Charles University in Prague
vaclav.smejkal@savs.cz
ORCID ID: https://orcid.org/0000-0003-1403-9494

Received: 18.12.2018
Accepted: 09.01.2019

High Tech Monitoring Versus Privacy in the Workplace in the Law and Case Law of the Czech Republic

Abstract: Modern technologies ask anew the old question about how employees can be checked during working hours so that legitimate interests of their employers are safeguarded. The answer cannot be solely technological, as the employees right to privacy, even in the workplace, is protected at the highest constitutional as well as international levels. Employers when defending their rights and interest are therefore far from free to use the potential of available technological devices in full and without limits. To strike the right balance between legitimate interests and fundamental rights is by no means easy, as the present text tries to demonstrate by summarizing and analyzing the existing Czech approach to the issue. On the one hand, Czech law on the protection of privacy of employees in the workplace, as well as the authorities applying it, are principally in line with generally accepted European standards. On the other hand, however, this basic consensus on values and their substantive and procedural legal safeguards does not mean that Czech law currently answers all questions and leads employers safely outside the restricted zone of prohibited ways of employee monitoring. The focus of the text is thus directed at those provisions of legal acts, decisions of the highest courts, opinions of supervisory authorities and arguments of commentators that influence the way in which the aforementioned rights and interest are balanced in the current Czech legal practice.
Keywords: privacy in the workplace, monitoring of employees, information technologies, tracking and recording, Labor Code, proportionality, fundamental rights

1. Introduction

Technological advances have a huge impact on the definition of privacy and on different aspects of its protection. In connection with this, they influence also the solution to the old question of how to combine the interests and rights of the employer

with the interests and rights of its employees.[1] On the one side, new technologies permit the supervision of employees with an unprecedented easiness. Every touch of a keyboard, every change in expression of a human face, simply every move of each employee can be monitored. Hired staff can thus be checked and disciplined during working hours much more effectively but also much more intrusively in terms of their privacy. On the other hand, the same information technologies make it also easier for employees to communicate in their private interests during working hours, which means abuse of the equipment provided by their employer (PCs, smartphones, cars, scanners, copy machines etc.) or even to collect and share electronic data to the detriment of the employer.

Abuse of sophisticated information technologies can therefore infringe both legitimate interests and fundamental rights on each side of the employment relationship. Employers have rights to control performance of their employees and to protect their ownership against the abusive behavior of employees. The latter from their side have a legitimate interest and right not to give away their personal privacy and data that may easily fall victim to invasive techniques of monitoring and control put in place by their employers. In short, the subject matter here is the employer´s ownership versus the employee's privacy[2] in our epoch of digital economy. Neither of these highly protected values can be plainly sacrificed to the other and the constant careful balancing of opposite legitimate interests and fundamental rights is therefore necessary.

To strike the right balance is, however, by no means easy, as will be demonstrated in the following text that tries to summarize and analyze the recent Czech approach to the issue. To familiarize the reader with a prevailing situation, it can be noted that in the year 2017 the State Labor Inspectorate (hereinafter SUIP) found a violation of the law in the monitoring of employees by cameras in 80% of the companies controlled. Of the 75 inspections in total, 58 were positive in that there was an inadmissible interference with employee privacy.[3] There is obviously room for improvement, at least in the everyday practice of employer - employee relationships. The present analysis wants to contribute to this goal by showing how the balance between the employer´s ownership and the employee's privacy right is perceived in Czech law,

1 The statement that "The history of privacy is deeply intertwinned with the history of technology" is a truism, whose validity is well proven by the facts of history. The right to privacy as such was first formulated in the US at the end of the 19th century as a reaction to the rise of tabloids and instantaneous photography. No wonder that ICTs and their penetration of our everyday life have opened new perspectives on the issue. See U. Grasser, Law, Privacy & Technology. Commentary series, "Harvard Law Review Forum" 2016, vol. 130(2), pp. 61-62.

2 L. Ticháčková, Vlastnictví zaměstnavatele versus soukromí zaměstnance, "EPRAVO.CZ magazine" 2016, No. 1.

3 K. Kolářová, Většina stížností na nepřiměřené sledování v práci je oprávněná, "Česká pozice", 8.12.2017.

by Czech legal commentators, and most of all, in the decisions of the Czech courts, namely the highest judicial institutions of the country.

For this purpose, the content of the relevant legislation will be analyzed first, then the focus will turn to the key concepts such as privacy, proportionality of intervention, consent to monitoring etc., and in the last part attention will be paid to specific monitoring methods (checking of emails, telephone calls etc.) and their legal consequences. As the Czech courts have not yet had the occasion to interpret all aspects of the issue, the view of experts on what is permissible in the workplace will be added to this (kind of in-country) report. A summary of the findings will be then provided in the conclusion.

2. The applicable legislation

There is no need to stress that the Czech Republic, due to its international engagements and memberships, has to follow the guidance provided by the UN[4] and Council of Europe conventions[5], the European Court of Human Rights' decisions[6] and the European Union standards of fundamental rights and personal data protection.[7] However, as this outer framework is constantly evolving with each new case decision or piece of legislation (recently the GDPR) and as new controversial moments keep emerging from everyday practice, there is undoubtedly a space for a country specific search for answers in a number of situations. This study will therefore not discuss every legal provision that may become relevant when employee privacy rights clash with the employer´s property rights but will focus on the key pieces of Czech legislation and the case law that interpret them.

The constitutional order of the country, namely its Charter of Fundamental Rights and Freedoms,[8] quite naturally provides for the protection of basic rights of both employers and employees. Property rights of owners are enshrined in Article 11. Article 7 guarantees the inviolability of the person and their privacy. Article 10 protects everyone from any unauthorized intrusion into his or her private and family

4 The International Covenant on Civil and Political Rights, Article 17(1).

5 The Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter Convetion), Article 8.

6 See for details: European Court of Human Rights, Guide on article 8 of the European Conventipon of Human Rights – Right to respect for private and family life, home and correspondence. Council of Europe, August 2018. https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (accessed 31.10.2018).

7 EU Charter of Fundamental Rights Arts. 7, 8. For the overview of the EU secondary law in the area see Online Privacy Law: European Union. Library of Congress, report updated on 29. 05. 2018. https://www.loc.gov/law/help/online-privacy-law/2017/eu.php (accessed 31.10.2018).

8 Constitutional act No. 2/1993 Coll. as amended by constitutional act No. 162/1998 Coll. For English translation see https://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Pravni_uprava/AJ/Listina_English_version.pdf (accessed 31.10.2018).

life as well as from the unauthorized misuse of personal data. Finally, Article 13 protects the confidentiality of letters and communications sent by telephone, telegraph, or by other similar devices. The law of the highest legal force thus protects the rights on both sides of the potential conflict. However Articles 7, 11 and 13 of the Charter permit that rights protected by them are in practice limited "in the cases and in the manner designated by law".

This specific law is not a *lex specialis* in the sense of legislation governing, for example, the use of CCTV systems or other specific means of interfering with privacy, or, as the case may be, of specific regulations concerning the direct intervention of employers in the privacy of employees. Such specialized regulations do not exist in the Czech Republic. Concrete legislation should therefore be sought in the provisions governing private law, labor relations and (where employees data are processed) the protection of personal data in general.

The key private law act, the Civil Code (Act No. 89/2012 Coll.) affects all relations of a private nature, including labor-law affairs, and its Division 6 regulates the "personality rights of an individual" (namely in Sections 81-90). Regarding the protection of privacy in the workplace the Civil Code however is of a subsidiarity use, being merely a *lex generalis* to the Labor Code (Act No. 262/2006 Coll.).[9] Chapter VIII of Labor Code, dedicated to the "protection of an employer's property interests and protection of an employee's personal rights", contains just one Section (§ 316). This Section will be thoroughly analyzed in the following pages as it is the provision that shapes the relationship between the protection of employer´s ownership and the employee's privacy.

In the overview of statutory acts affecting the "monitoring at the workplace" cases, one cannot forget the public law *lex specialis*, which up to 25 May 2018 was primarily the Personal Data Protection Act (Act No. 101/2000 Coll.). It has been replaced by the EU´s GDPR[10] together with the local Personal Data Processing Act (not yet approved in November 2018) which is to accompany the GDPR into practice in the Czech Republic. This piece of regulation establishes and governs operations of the Office for Personal Data Protection (UOOU), the administrative body that regulates the rights and obligations in processing of personal data, i.e. when employees are monitored with recordings, which are then stored, categorized, transferred etc. Finally, yet importantly, there is also the Czech Criminal Code (Act No. 40/2009 Coll.) which in its Section 182 sanctions the breach of secrecy of correspondence (which includes not

9 Labor Code No. 262/2006 Coll., as amended. For English translation see https://www.mpsv.cz/files/clanky/3221/Labour_Code_2012.pdf (accessed 31.10.2018).

10 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) (O.J. L 119, 4.05.2016, pp. 1-88).

only letters, but also data, text, voice, audio or visual messages sent by the means of a network of electronic communication and computer systems) with imprisonment for up to two years or with prohibition of activity.

Thus, the above-mentioned monitoring of employees in the workplace may fall under the two key laws, namely the Labor Code (hereinafter LC) and, at the same time, GDPR plus the future Personal Data Processing Act (and *ultima ratio* also the Criminal Code). The case may be, however, that only one of the two regulations would be applicable. There may exist two different sets of cases, one of which involves only interference with privacy (if it occurs without data processing enabling the identification of a particular natural person) and the other contains only the processing of personal data (if they can be obtained without interfering with the privacy of an employee). However, both sets of cases would in practice rather overlap - data allowing the identification of a natural person are often obtained by the intervention into privacy and are then usually stored, sorted, evaluated, etc. Due to the ongoing expansion of the concepts of "privacy" and "personal data", it is thus inevitable that the same case of monitoring often leads to application of the two regulations and is then subject to supervision (and eventually to sanction) by two administrative authorities. The Labor Inspection Office (SUIP) deals with violation of employee privacy, while the failure to fulfill the obligations related to the processing of personal data is supervised by the Office for Personal Data Protection (UOOU).[11] In addition, brutal breaches of correspondence secrecy should naturally be seized upon by the competent authorities involved in criminal proceedings (however this option will be left aside in the following analysis).

This double regulation in practice poses considerable problems, as it is evidenced by online discussions and instructions on numerous internet sites trying to explain to stakeholders how the rights should be protected and obligations complied with.[12] Employers must be mindful of the fact that, for example, the system of registering entry to and exit from the workplace would entail the processing of personal data, but not, as a matter of principle, a violation of privacy. On the other hand, an installation of CCTV cameras in the workplace, with no recordings, would amount to a privacy

11 SUIP states on its official website the following: "Control of the above mentioned (i.e. monitoring of employees in the workplace using a camera based surveillance system – added by author) falls within the competence of labor inspectorates. If a breach of Section 316(2) of the Labor Code is detected in connection with the processing of personal data of employees (i.e. when camera recordings would be archived and would allow for the identification of employees), the findings will also be transmitted to the Office for Personal Data Protection"; http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem/ (accessed 31.10.2018).

12 See for instance in E. Janečková, V. Bartík, Ochrana osobních údajů v pracovním právu (Otázky a odpovědi), Wolters Kluwer, Praha 2016, pp. 128, 131.

breach, but not to the processing of personal data. Since the aim of the study is to analyze the legal aspect of the protection of privacy in the workplace in the Czech Republic, the issues discussed below will be viewed primarily through the lenses of the Labor Code and its Section 316. Only where privacy issues cross with personal data protection and such situation would cause interpretive or application ambiguity will related data protection requirements be given attention.

3. Section 316 of Labor Code – a guidance or a puzzle?

The fact that Chapter VIII LC titled "Protection of an employer's property interests and protection of an employee's personal rights" contains just one section, Section 316, might suggest that it is a unified and coherent set of rules. In reality, however, this Section regulates different situations that for the sake of clarity would be better split into separate sections. Paragraphs 1-3 really focus on the checks conducted by the employer in the workplace.[13] Paragraph 4, on the other hand, prohibits employers to require from their employees information that does not "directly relate to work performance and basic labor relationship" (e.g. to question them about pregnancy, sexual orientation, political adherence etc.). However, even within paras 1-3 of the Section, the difference between paragraph 1 (which allows the employer to check that employees do not misuse his "means of production or service" without due consent and for their own purposes) and paragraphs 2 and 3 (which prohibit the employer from encroaching upon his employees' privacy without a serious cause) should be duly noted.

Paragraph 1 does not mention employee privacy and uses the term "to check" in order to empower the employer to oversee that his means of production or service etc. are not misused by employees. A proportionate way of conducting such a check is required, but the law sets no specific conditions for that. On the other hand, paragraphs 2 and 3 deal with the employee's right to privacy that may be encroached upon by employer´s surveillance (monitoring), interception (recording) of telephone

13 Section 316 (translation taken from *op.cit*. n. 9): (1) Without their employer's consent, employees may not use the employer's means of production or service and other means necessary for performance of their work, including computers and telecommunication technology for their personal needs. The employer is authorized to check compliance with the prohibition laid down in the first sentence in an appropriate way. (2) Without a serious cause deriving from the nature of the employer's activity, the employer may not encroach upon employees' privacy at workplaces and in the employer's common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee. (3) Where there is a serious cause on the employer's side consisting in the nature of his activity which justifies the introduction of surveillance (monitoring) under subsection (2), the employer shall directly inform the employees of the scope and methods of its implementation.

calls, checking of electronic mail etc. An employer can do this only if he has a serious cause deriving from the nature of his activity and if he has directly informed employees of the scope and methods of his monitoring, checking etc.

Even though the terms "to check", "to survey", "to monitor" used in these paragraphs may sound like synonyms, they are not in the context of Section 316 LC. Otherwise, it would be difficult to tell how an ordinary employer may routinely have use of paragraph 1, without being prohibited from doing so by the condition set in paragraph 2, which authorizes the monitoring of employees only if a non-ordinary nature of activity provides a serious cause for it. The commentary literature has therefore shown the senselessness of understanding paragraphs 1, 2, and 3 of Section 316 as rules regulating the same situation. If there were one rule expressed in 3 paragraphs, the right to check employees would only be given to an employer carrying out a particularly dangerous or threatening activity.[14] To avoid that, both parts of Section 316 need to be read separately. More precisely, paragraphs 2-3 need to be understood as setting the rules for special situations (interference with the privacy of employees if a specific cause so requires), whereas ordinary control by the employer takes place in accordance with paragraph 1.[15] In the existing wording, however, Section 316 LC remains rather "incomprehensible and meaningless, especially for the employer, whose legal certainty it undermines".[16] Unfortunately, even the Czech courts and administrative authorities do not produce in their decisions and statements any clear and easy-to-understand guidelines.

The Czech Supreme Court (hereinafter SC) and the Czech Supreme Administrative Court (hereinafter SAC)[17] standardly interpret the distinction between paragraph 1 and paragraphs 2-3 of Section 316 LC so that paragraph 1 is devoted to the protection of the employer's property while paragraphs 2-3 are dedicated to the protection of the privacy of the employee.[18] Under paragraph 1, every employer is entitled, to the extent of what is necessary and proportionate, to check his employees. It must be done without any interference with privacy greater than that given by the relationship of subordination between the employer and the

14 See for instance M. Štefko, Soukromí zaměstnanců pod ochranou inspelce práce, "Acta Universitatis Brunensis Iuridica" 2018, vol. 604; also M. Hromanda, Ochrana osobnosti zaměstnance při elektronické komunikaci, (in:) H. Barancová, A. Olšovská (eds.), Pracovné parvo v digitálnej dobe, Leges, Praha 2017, p. 166.

15 Judgment of the Supreme Administrative Court on the case 5 As 158/2012 – 52 (23.03.2013). The Court stated: "The employer has the right to proportionate control according to the provisions of Section 316 (1) of the Labor Code while the provisions of Section 316 (2) of the Labor Code are corrective of possible ways of performing such control".

16 J. Morávek, Kontrola a sledování zaměstnanců, "Právní rozhledy" 2017, No. 12.

17 The Supreme Court is the last instance for disputes between employees and employers, the Supreme Administrative Court for disputes of employers with supervisory state authorities.

18 Judgment of the Supreme Court on the case 2 Cdo 747/2013 (7.08.2014); Judgment of the Supreme Administrative Court on the case 5 As 158/2012 – 52 (23.03.2013).

employee and by the fact that each manager has to supervise his subordinates (which naturally limits the extension of their privacy). Without need to comply with other conditions, each employer is thus authorized to check whether his employees use the entrusted means of production or service solely to perform the entrusted work, properly manage them, guard and protect them from damage, loss, destruction or misuse and do not act in contradiction with the legitimate interests of the employer. Therefore, the "checking" under paragraph 1 is fundamentally and qualitatively different from "monitoring or surveillance" according to paragraphs 2-3 of the same Section: it can be carried out under all circumstances and, if appropriate, it is not subject to the restrictions contained in paras 2-3 because it does not intervene into employees' privacy. It looks as if Section 316(1) LC creates a safe harbor for Czech employers and the only question that must be answered is how to stay safely within its limits.

On this issue, the SC ruled in 2012 in the most cited Czech case of an employer´s control over the activity of an employee on the Internet.[19] The employer found that his employee had spent 102.97 hours out of 168 working hours in a single month by viewing non-job-related content on the Internet (always using a work PC). As a result, the employment relationship was immediately terminated for a particularly gross breach of duty because the employer did not consent to the use of his equipment for the private purposes of the employee. A series of litigation followed, as the evidence, in the form of a list of web pages with non-work content visited by the employee, was produced without the employee's consent and knowledge. Czech courts, including the SC, and ultimately also the Constitutional Court,[20] found that in this case, there had been no unacceptable interference with privacy of the employee and hence no act of the employer that exceeded the authorization given to him under Section 316(1) LC.

According to the SC, the employer with his checking did not fall under Section 316 (2-3) LC, as the degree of interference with the complainant's privacy was, in the opinion of the judges, totally negligible (if any at all). The fact that the employer's control fell exclusively within the scope of the authorization given in Section 316 (1) LC was explained by the SC as follows:

– first, the Court found that the employer had not proceeded "completely arbitrarily (in terms of scope, length, thoroughness, etc.)" and checked in a proportionate way, because the content of the websites visited (and what exactly the employee was searching for, watched, etc.) was not detected. The employer only ascertained whether the pages visited were job related;

19 Judgment of the Supreme Court on the case 21 Cdo 1771/2011 (16.08.2012).

20 Resolution of the Constitutional Court no. I. ÚS 3933/12 (7.11.2012) stated that the constituional complaint of the employee was manifestly unfounded.

– second, the SC considered it essential that the employer did not use wiretapping, telephone call logging, e-mail monitoring, or mail order inspection (the forms of employee monitoring explicitly mentioned in Section 316(2-3) LC), but he reviewed only a statement of the PC's activity conducted with the employee's login.[21]

The fulfillment of these two conditions: a) the limitation of the length and reach of the control, and exclusion of the content of visited web pages from its scope; b) the non-use of employee tracking means specifically listed in Section 316(2) LC, was sufficient for the SC to admit that the object (target) of the employer´s control was not to intervene into the employee privacy but only to determine whether the employee violated the absolute statutory prohibition of abuse of the employer's equipment for personal purposes.

However, it was not convincingly explained by the SC why tracking only the kind, but not the content of the web pages visited by the employee did not mean encroachment upon his privacy. It can be argued that the information needed to determine whether a certain web page is job-related or not is information about the personal preferences and hobbies of the employee concerned (one can guess whether he is fond of shopping, lifestyle, sports, sex etc.). The SC surprisingly did not even address the question of whether the criterion of proportionality would not be better satisfied by blocking websites that are often abused for out-of-work activities than by an ex-post control of the employee's PC activity.[22] Nevertheless, the SC decided very similarly on the inspection of a list of telephone calls made by an employee from the workplace.[23] Although it can be argued that inspecting traces of the employee's usage

21 *Verbatim* the Supreme Court stated (author´s translation): "Control of compliance with this prohibition, however, may not be exercised by the employer in an arbitrary manner (in terms of scope, length, thoroughness, etc.), as the employer is entitled to do so in an appropriate manner only…. In particular, the court will take into account, whether it was an interim or a follow-up check, its duration, its scope, whether it did at all (or to what extent) limit the employee in his activities and also whether and to what extent did it interfere with the employee's right to privacy etc. Of course, the subject matter of a check can only be to find out if the employee has violated the statutory absolute prohibition (or taking into account to what extent did the employer consent to mitigate such prohibition) to use his equipment, including his PCs and telephones for the employee´s personal purposes. It must always only be a check on non-compliance with those obligations which have not been expelled or reduced by the employer. Only such a control can be considered as reasonable (proportionate) and therefore legal (in accordance with the authorization under the provisions of Section 316 (1) LC)".

22 For reservations against the Supreme Court decision see for instance J. Vobořil, Nejvyšší soud k možnostem utajeného sledování zaměstnanců, "Zpravodaj Gender Studies" 2012, No. 12, 30.10.2012, http://zpravodaj.genderstudies.cz/cz/clanek/nejvyssi-soud-k-moznostem-utajeneho-sledovani-zamestnancu (accessed 31.10.2018).

23 In the case of abuse of a service phone for unauthorized private calls, the Supreme Court decided in 2014 in conformity with its earlier decision regarding the inspection of websites visited by the

of facilities from PC activity or telephone call logs is also a certain type of monitoring or surveillance, the SC drew a dividing line between the targeted *ad hoc* collection of such "footprints" and the continuous monitoring of the employee's activity (all the more so if it includes interference with the secrecy of messages transmitted by him etc.).

The SC's emphasis on the non-use of the means and methods of control listed explicitly in Section 316(2) LC, i.e. open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee, can be understood as their qualitative differentiation from all other means of control, including the acquisition of electronic statements of employee activities at corporate facilities (PCs, printers, copy machines, telephones).

Morávek, one of the frequently publishing experts on the issue, explained such a recommendation made by the SC as follows (author´s translation):

"*Pursuant to Section 316 (1) exclusively, those cases are handled, regardless of the means of control chosen, where it is probable (or de facto certain) that no encroachment upon the employee's privacy can take place. Furthermore Section 316(1) is applicable, even if there is interference with the privacy of an employee, if a different form of control is chosen other than that enumerated by Section 316 (2) (surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee), it can be for instance an inspection of a service vehicle's usage log or other random checks performed in real-time for ad hoc cases.*"[24]

It can be seen here that adding the value of an exhaustive enumeration to the list of monitoring methods expressly mentioned in Section 316 (2) LC one may draw the conclusion that, if the employer finds other methods, he may interfere with the privacy of his employees. It is very dubious whether the SC really meant that, because such an interpretation would deny the logical construction of Section 316, built on the assertion that when acting within the limits of its paragraph 1, no violation of employee privacy occurs. Abandoning this approach would blur the aforementioned distinction between paragraph 1 and paragraphs 2-3 of this Section with all negative consequences for legal certainty. The fact that, unfortunately, there is such confusion in the current Czech debate, can be illustrated by two opinions issued by supervisory authorities in 2014, i.e. two years after the above cited judgment of the SC.

---

employee. If the content of the employee's telephone calls was not detected and the check was focused only on the employee respects for the private use prohibition of the service telephone (by review of the telephone numbers called), it was not an employer's intervention into employee privacy but an inspection falling under Section 316 (1) LC. See the Judgment of the Supreme Court on the case 21 Cdo 747/2013 (7.08.2014).

24 J. Morávek, Kontrola a sledování zaměstnanců…, *op. cit*. n. 16, p. 573.

The UOOU maintains in its statement that every check of an employee's internet activity falls under the paras 2-3 and not para 1 of Section 316 LC:

"It is not possible to monitor the use of the Internet by employees for the purposes of the employer, unless the statutory conditions are met, i.e. the employer has a serious reason rooted in the specific nature of his activity … Neither the statistical monitoring of the use of Internet access, such as the time spent by an employee "surfing" the Internet is not in line with the new Labor Code, unless the conditions set out above are met".[25]

Contrary to that, the SUIP in its information brochure defended the possibility for employers to stay within the limits of para 1 of Section 316 LC:

"Monitoring of an employee's activity on the Internet – when it comes to controlling the use of the employer's means by an employee during his/her working hours, must always stay within reasonable (proportionate) limits, e.g. if the employee visits a "personal page", such as electronic banking, its content cannot be traced".[26]

As can be seen, the same activity called "tracking employee activity on the Internet" falls under paras 2-3 of Section 316 according to one supervisory body, while the other admits that an appropriate and targeted control of private misuse, not disclosing the content of the sites visited, would still be at hand to any employer. For greater approximation to what kind of monitoring of employees is always permitted under Section 316 LC and what can be used under certain conditions only, or rather not allowed at all, the further analysis will focus on the individual criteria which influence it.

4. Section 316(1) of Labor Code and the proportionality issue

Paragraph 1 of Section 316(1) requires that checking must be conducted by an employer in an *appropriate* or *reasonable* or *proportionate* way (depending on the translation).[27] The proportionality of the employer's checking is underlined by commentators[28] as well as by supervisory bodies in their instructions for general

25 UOOU Opinion Nr. 2/2009 updated in February 2014, https://www.uoou.cz/stanovisko-c-2-2009-ochrana-soukromi-zamestnancu-se-zvlastnim-zretelem-k-monitoringu-pracoviste/d-1511 (accessed 30.10.2018). The UOOU is not, strictly speaking, in a position to give an authoritative interpretation of the Labor Code or to supervise employers´ compliance with its provisions. However, any recording or monitoring of the employee becomes a processing of the employee´s personal data. Therefore, the UOOU opinion cannot thus be easily dismissed as irrelevant.

26 SUIP, Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele (Protection of employees' personal rights and protection of the employer's property interests), květen (May) 2014, http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance (accessed 31.10.2018).

27 "Přiměřeným způsobem" in the Czech original, which can be translated by each of the expressions used above, however, the term "proportionate way" seems to be the most literal translation.

28 J. Morávek, Kontrola a sledování zaměstnanců…, *op. cit*. n. 16.

public.[29] However, in view of the structure of Section 316, it must be emphasized that we encounter here the dual meaning or use of the concept of proportionality.

Under para 1 of this Section, the fulfillment of the proportionality requirement means that the employer's checking would not encroach upon his employees privacy at all or in such an insignificant way that paras 2-3 of the same Section would not be activated. In this first paragraph, therefore, the proportionality is important as a backstop, which ensures that the employer when protecting his ownership does not interfere with the employee's fundamental right to privacy.

Only when the employer's control is not proportionate in the sense of para 1 and affects the privacy of employees, the requirement of proportionality gains importance of the constitutional test of the same name. It means that the employer's control must be tested whether it is really suitable, necessary and proportionate (in a narrow sense of balancing between clashing constitutional right and values). Unfortunately, the proportionality in this meaning, which is relevant for the understanding and application of paragraphs 2-3 of Section 316 LC, is not mentioned at all in its statutory provisions. Its relevance and importance must be inferred from standards of constitutionality review conducted by the Czech Constitutional Court (hereinafter CC) and after this court by the ordinary courts of the Czech Republic. An employer without legal training in this field of law, however, would not learn about any proportionality requirement from the wording of paragraphs 2-3 of the Section.

The definition of proportionality in the first sense, i.e. as a backstop which should keep the employer's control within the safe harbor of paragraph 1 of Section 316 LC, was, as a matter of fact, already discussed in the previous chapter on the basis of analysis of the SC decision from 2012 regarding the monitoring of employee activities on the Internet.[30] It can only be added that the SC stressed *expressis verbis* on account of proportionality that (author´s translation):

"As the law fails to specify what is the most proportionate way of control, it is a legal norm with a relatively indefinite (abstract) hypothesis, i.e. a legal norm whose hypothesis is not directly prescribed by law, thus leaving it to the court to define in each individual case, from a wide, unlimited range of circumstances, what specifically would be the hypothesis of the legal norm".

If we want to escape from this general reference to circumstances of each individual case, it can be specified, based on the abovementioned decisions of the SC, that "proportionate" in the sense of Section 316(1) LC would be the control that would remain rather limited in scope, that would be better focused on an ex-post check of whether the ban on using the employer's equipment for employees' private purposes has been respected. It is thus possible to check the "footprint" that the employee leaves behind that can be ex-post reviewed through a record or statement

29 UOOU Opinion no 2/2009, *op. cit.* n. 25, SUIP, *op. cit.* n. 26.

30 Judgment of the Supreme Court on the case 21 Cdo 1771/2011 (16.08.2012).

of PC, telephone or service vehicle use etc. Such a record may cover even a longer period of the employee's activity, such as one full month, as in the abovementioned SC case. The purpose of such tracking, however, must never be the discovery of content of private internet browsing, of sent and received correspondence, of telephone calls or privately printed copies or employee monitoring in general.[31]

For practical purposes, it can be added, first, that if the ban on using the employer´s equipment for private purposes remains absolute, it would always be easier to control it as any trace of misuse would signal an employee's inappropriate behavior. If, on the other hand, the ban has been mitigated by the employer's consent to limited private use of his equipment, there must be clearly stated (and to all employees explained) a boundary between authorized and non-authorized use. This can logically lead to misunderstandings and consequent problems. Second, it is of no relevance, if the employee "footprint" was recorded by a high-tech or by a more traditional means of control as all that is important whether or not the conditions of the safe harbor set by Section 316(1) LC were fulfilled. However, as will be shown further, some of the available technical means are more problematic in terms of their suitability, because they are rather tools for continuous and intrusive monitoring (like on-site cameras) than of an ex-post and limited control.

Undoubtedly, it remains a shortcoming in the wording used in Section 316 LC, if there is not stated clearly enough, that an appropriate checking in the sense of paragraph 1 is qualitatively different from "monitoring" or "surveillance" mentioned in paragraphs 2-3 of this Section. If an ex-post, *ad hoc* control is not unambiguously differentiated from real-time and systematic monitoring – reaching beyond the need to verify whether an employee is abusing the employer's equipment – then, in practice, both the courts and the supervisory authorities keep speaking about "monitoring", regardless of whether they mean control under paragraph 1 or monitoring encroaching upon employees' privacy in the sense of paragraphs 2-3. For example, if we concede that in the statements quoted in the previous chapter, the UOOU had in mind the "monitoring" that is systematic and extensive, affecting the privacy of employees, while the SUIP referred to "monitoring" proportionate by its scope and methods, there may be no contradiction between the advice they each give addressed to employers. The confusion here is once more caused by the use of the same term to "monitor" activities on the Internet.

31 In the following part of this paper, the decision of the Municipal Court in Prague from 2017 is mentioned, in which the court assessed the GPS tracking of the Czech Post deliverers, i.e. all of their movement throughout working hours. Although it was also carried out for "statistical" purposes only, there was a significant difference from a survey of the employee's use of the employer's equipment. GPS tracking of all movement allowed to reconstruct the whole day of the employee, not just the inappropriate manipulation of the means entrusted, and that is why it interfered with his privacy.

5. Section 316(2) of Labor Code and the proportionality issue

In cases where the employer interferes with the privacy of the employee, the requirement of proportionality in the second meaning comes under the spotlight, i.e. the requirement to interfere with the fundamental right in a way that is suitable, necessary and proportionate (in a narrow sense). Regarding this second proportionality there is a more developed jurisprudence in the Czech Republic due to the fact that the majority of litigations having monitoring of employees as their subject matter fell under paragraphs 2-3 of Section 316 LC, as the methods used had an appreciable impact on employee privacy. It can logically be expected that when deploying modern technologies to monitor employees, it becomes very easy to "let them run" without restrictions, as opposed to the complexity of their needful and precise targeting within a strictly limited time frame.

Virtually since the beginning of the existence of the Czech Republic, the Czech CC has applied the aforementioned proportionality test to cases of interference with fundamental rights in the public interest, as well as in the event of collision of two fundamental rights.[32] According to the CC, fundamental rights also have effects in horizontal relations, and the State has the duty to protect them, even if they are interfered with by individuals, for example in relations between employees and employers.[33] The precedence of one fundamental right over another is not and cannot be given once and for all, so the proportionality test must always be carried out again for each particular case, taking into account its unique circumstances.

In its application of the proportionality test the CC follows the European Court of Human Rights and the European Court of Justice, and on the theoretical level, it refers itself to the understanding of proportionality developed by the German theorist R. Alexy.[34] The CC, however, has not been dogmatic to apply the test all the time in a standardized way and in every detail. It has replaced, on case-by-case basis, the universal three-tier proportionality test by the requirement of reasonableness of the method of enforcement of one party's fundamental right, and by the requirement to avoid extreme disproportionality in the possibility of exercising the fundamental right of the other party.[35] Courts dealing with civil and administrative disputes follow this approach in deciding cases of employee privacy breaches by the employers' monitoring, that is, those covered by Section 316 (2-3) LC.

32 Decision of the Constitutional Court on the case Pl. ÚS 4/94 (12. 10. 1994). See also D. Kosař, M. Antoš., Z. Kühn, L. Vyhnánek, Ústavní právo. Casebook, Wolters Kluwer, Praha 2014, pp. 362-366.

33 Decision of the Constitutional Court on the case IV ÚS 1735/07 (21.10.2008).

34 Z. Červínek, Standardy přezkumu ústavnosti v judikatuře Ústavního soudu, "Jurisprudence" 2015, No. 4, pp. 21-29.

35 D. Kosař, M. Antoš., Z. Kühn, L. Vyhnánek, Ústavní právo… *op. cit*. n. 32, pp. 374-375.

The ruling of the CC from 2014 may be considered symptomatic in this regard.[36] The case involved a conflict of the right to privacy of an employer against the right to fair process of an employee, as in the core of the dispute was a hidden record of an employer taken by an employee who opposed the termination of his work contract because of redundancy. The CC first stated that the proportionality test is the method used to assess the collision of two fundamental rights and recalled the standard three steps of the test. However, in the practical application of the test, the CC was satisfied with the first step when it found that the hidden record was the only possible (and therefore suitable) way in which the weaker party (i.e. employee in relation to employer) could prove its claim about the real motive for dismissal. The other two steps of the proportionality test were not carried out by the CC and its conclusion was that ordinary courts had erred in not recognizing as admissible evidence the recording of the employers' arguments secretly acquired by the employee. The courts thus violated the employee's right to a fair trial and the constitutional principle of weaker party protection.

The SAC follows the CC and considers the proportionality test as a standard step of procedure that has to be taken when it comes to the choice of one of the two fundamental rights guaranteed by the Constitution. In the Court's decision-making in matters of employee monitoring, there are cases in which the SAC consistently carried out the three-step proportionality test, as well as those where it was satisfied with the reasonable balance between the target and the means of its achievement.[37] An example of a rigorous application of the proportionality test was the case of camera monitoring of drivers and stewards of long-distance buses decided by the SAC in 2015.[38] The employer claimed the protection of lives and safety of the transported persons as well as of his own property (bus and fare). The possibility to add an inspector to each bus was rejected by him as difficult and inefficient. He therefore defended the camera crew watching during the entire duration of the shift (capturing image, not sound) as perfectly justified.

His intention to introduce such type of monitoring was notified to the UOOU, this supervisory body however, disagreed as it deemed the measure to be disproportionate. The UOOU itself has examined the notified method of monitoring for suitability (found that it could not achieve the declared goals, e.g. better safety of passengers), then for necessity (there would be less problematic methods of achieving the purpose, as for instance the testimony of passengers) and finally also for proportionality in the narrow sense. In this respect, the UOOU held that the employees' right to privacy would be violated and the provisions of Section 316(2) LC breached as filming the entire crew of a bus for the entire duration of the journey

36 Decision of the Constitutional Court on the case II ÚS 1774/14 (9.12.2014).

37 Judgment of the Supreme Administrative Court on the case 5 AS 158/2012– 52 (23.03.2013).

38 Judgment of the Supreme Administrative Court on the case 10 As 245/2016 – 41 (20.12.2015).

amounts to deprivation of privacy as such. Conversely, for example, the scanning of the driver's cabin space only for the time when cash is handled, would be for the UOOU a more acceptable form of monitoring. The Municipal Court in Prague, hearing the employer's action against the UOOU, fully confirmed the correctness of the proportionality test carried out by the UOOU and concluded that "camera monitoring of the driver and the steward and of their immediate surroundings is an unjustified and disproportionate interference with privacy of the employees concerned".[39]

The SAC, ruling on the employer's cassation complaint against the decision of the Municipal Court, also applied the proportionality test. Its judges (as opposed to the UOOU and the Municipal Court opinions) concluded that the measure envisaged by the employer could fulfill the criterion of suitability, as it could act preventively. However, the criterion of necessity was no longer fulfilled because the employer did not prove the inefficiency of less intrusive means of checking that could not prevent real-life damage and threats that occur during the bus operation. The SAC then dropped the third step of the proportionality test, because non-fulfillment of the second criterion made further testing pointless.

In the argumentation of the SAC, it is necessary to emphasize a.o. the following: if there are no proofs of employees' misbehavior, which should be prevented by their monitoring, then an open intervention into their privacy is unjustified and thus will not stand the proportionality test. This could mean that the employer's ordinary, non-intrusive protective measures should first be overcome by inappropriate employees' acts, and only then could the employer resort to a more sophisticated method of tracking them. Without proof of the employer's negative experience, or at least, without reasonable suspicion that employees breach statutory rules and legitimate requirements, it is more than probable that interference with employee privacy would be deemed disproportionate.

Such conclusion is supported and further developed by another SAC judgment[40] concerning camera systems, in which the Court stated (author´s translation):

"The Supreme Administrative Court considers it necessary to emphasize that the installation of camera systems, having regard to their nature and interference with the personal integrity of persons, can only be achieved if all less invasive devices have failed or would not be able to fulfill the intended purpose of monitoring".

This reasoning implies the idea of a certain range of means of control, from the least to most intrusive, from which the employer should first select those less intrusive. Only in the case of their failure, or an a priori manifest inadequacy, can the employer consider switching to more invasive means of monitoring employees. Systematic camera scanning throughout the entire workday is of course the most

39 Judgment of the Municipal Court in Prague on the case 5A 107/2013 (18.10.2016).

40 Judgment of the Supreme Administrative Court on the case 5 As 1/2011 – 156 (28.06.2013).

intrusive in terms of employee privacy. Conversely, capturing only certain "sensitive" moments of an employee's work, like cash handling, access to certain protected areas (box office, server room etc.), are naturally far more appropriate. The commentary literature, based on analysis of the aforementioned case law, rightly emphasized that "if any aspect of monitoring cannot be considered as strictly necessary, it is necessary to say goodbye to it".[41]

In this regard, the second step of the proportionality test, consisting of seeking an equally effective but less intrusive means of control, coincides in both the UOOU decision and in subsequent judgments, with the third step of this test. The latter consists in the assessment of proportionality of interference with privacy in the narrow sense (i.e. the search of an acceptable imbalance of rights where one of them, for good reason, temporarily wins but the other is not at the same time totally denied). In the above-mentioned cases, however, the extensive camera surveillance of employees (almost) fully suppressed privacy in the workplace. It was, therefore, natural to conclude that the proportionality test was failed when the monitoring was affecting the entire workplace throughout working hours. This conclusion is confirmed by decisions of the Municipal Court in Prague in two other cases of employee monitoring.

In the first case, the Municipal Court in Prague carried out the test of proportionality of a measure by which the Czech Post monitored 7770 of its mail delivery staff for one whole year. All had to carry a GPS locator each day throughout their working hours.[42] The employer justified the deployment of GPS trackers by the need to accelerate and improve services provided within the framework of the legally defined service of general interest consisting in proper delivery of consignments and other values to recipients. At the same time, the Czech Post claimed to be interested in mere statistical data without linking them to employee personal data. However, the identification of offline data collected with individual deliverers was, of course, technically possible. The Court therefore agreed with the UOOU that the interference with the privacy of the employees was inappropriate because the method of monitoring was not a suitable means of verifying that a consignment had actually been delivered. This was not a necessary measure either, because in order to achieve the declared objectives, it would have been sufficient to verify whether the delivery person actually visited the places to which consignments were to be delivered. Regarding the proportionality in the narrow sense, the Court stated that the employer did not assess all various possibilities of monitoring and did not choose the one that had the least effect on the privacy of delivery staff, e.g. not recording all movement only the information on time of visit at the place of delivery.

41 J. Tomšej, J. Metelka, Ochana soukromí nad zlato? "EPRAVO.CZ", 16.09.2013 https://www.epravo.cz/top/clanky/ochrana-soukromi-nad-zlato-92358.html (accessed 31.10.2018).

42 Judgment of the Municipal Court in Prague on the case 6 A 42/2013 – 48.183 (5.05.2017).

In the second decision of the Municipal Court, the dispute was about camera surveillance in PC games stores.[43] A substantial part of these stores were continuously monitored, including employees behind the cash counter. The Court found that if one of the essential purposes of such monitoring was to prevent employees from offering discounts to fictitious customers (as really happened in practice), the cameras had to monitor the area in front of the counter in order to verify whether a customer was present at the time of working with the cash. It was therefore unnecessary to deprive employees of their privacy by capturing the space behind the counter where they were standing most of the time. In both cases it was thus confirmed that only by deploying the least intrusive means of control, however good enough to achieve the legitimate goal, the monitoring would be kept within proportionate limits.

Even though other case law findings regarding cameras in the workplace could have been cited, they would not change the following conclusion regarding the proportionality of means used to monitor employees in the sense of Section 316 (2-3) LC:

a) employee is under labor contract with employer always as a dependent, a weaker party whose privacy in the workplace is therefore by definition a weakened one. However, he should never be completely deprived of his privacy and therefore any means of control, that does so, can only in very exceptional cases pass the test of proportionality;
b) appropriate means of control must be *suitable* to attain the legitimate aim, i.e. only those that directly and genuinely lead to that aim would be acceptable. *Necessary* will only be those means that still lead to the goal but are the least intrusive of the set of suitable means. Such are the means that target only certain risk moments of the employee's behavior, not all of his behavior at work;
c) employer should initially apply "minimal monitoring" (narrowly focused, limited in scope and time) and only when this fails and it becomes clear that the protection of legitimate interests and rights, or fulfillment of legal obligations of the employer, would not be secured, it is possible to move to more extensive and intrusive means of monitoring.

6. Scope of employee privacy

The statement that an employee has the right to protection of his/her privacy in the workplace requires at least a brief outline as to where such privacy in the workplace extends.

43 Judgment of the Municipal Court in Prague on the case 8 A 182/2010-69.77 (2.09.2014).

The right to privacy has a relatively long and fascinating history, in which privacy in the workplace is one of the newer chapters whose content is not yet closed. In this respect, the European Court of Human Rights (ECtHR) is the most influential promoter within Europe. The authorities of the Czech Republic followed the guidance of ECtHR already in the 1990s, as evidenced by the 1998 decision of the SC[44] pointing to the inadmissibility of the secret recording of an employee's call as evidence in a labor dispute. The SC referred to the ECtHR case law in *Halford v. UK* and *Klopp v. Switzerland*, that telephone calls made from the workplace may be covered by the protection of privacy and inviolability of correspondence within the meaning of Article 8(1) of the ECHR. Although the SC originally tried to draw a certain dividing line between professional, commercial and public communication on the one hand and speeches of a personal nature on the other,[45] it is under the influence of the ECtHR jurisprudence that the SC currently holds the opinion that privacy may have a place even where communication is of a professional nature. No definite conclusions, therefore, can be drawn regarding this or that type of recording of a particular act and it is always necessary to proceed in the light of the circumstances of each individual case.[46]

Commentators also agree with the fact that even in the workplace the rights of employees to private and family life must remain real and effective.[47] They justify this in line with the ECtHR and the Czech authorities' statements, stressing that every individual has the right to create and maintain relationships with other human beings and thus to develop his private life including in the workplace.[48] Only rarely, a rejection of this extensive construction of privacy occurs, pointing to the fact that if an employer does not allow employees to use his equipment for their private purposes, the content of all corporate PCs, servers and mailboxes can be controlled without limitation because the employer can logically assume that no private items will be found there.[49] However, such voices remain exceptional and without influence on the decision-making of supervisory bodies and courts. Actually, there is no dispute in Czech law that even in the workplace an employee has always the right to a private

44 Judgment of the Supreme Court on the case 21 Cdo 1009/98 (21 10.1998).

45 Judgment of the Supreme Court on the case 30 Cdo 64/2004 (11.05.2005)

46 Judgment of the Supreme Court on the case 30 Cdo 1585/2012 (27.03.2013).

47 P. Molek, Základní práva. Svazek 1. Důstojnost, Wolters Kluwer, Praha 2017, p. 335. Likewise M. Štefko, Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod. "Jurisprudence" 2012, No. 7, p. 17.

48 Judgment of the European Court of Human Rights of 12 December 1992 on the case Niemietz v. Germany, application No. 13710/88 and UOOU Opinion No. 6/2009.

49 L. Ticháčková, Vlastnictví zaměstnavatele versus soukromí zaměstnance…, *op. cit.* n. 2. The UOOU, for instance, in its Opinion No. 1/2003 emphasizes that for the existence of the employee's right to privacy it is irrelevant that the employee uses communications or other facilities of the employer. The location and ownership of an electronic device cannot exclude the right to confidentiality of its communications and correspondence.

sphere, be it in an office or in any different kind of workplace (including in company vehicles etc.).[50] As one commentator rightly explained, it is an employee's space in which, although for a limited time and perhaps only partially, he can stop playing his social roles or can change them.[51] It also implies that in the workplace there are areas with different degrees of privacy, from those where monitoring is justified and basically foreseen (access to workplaces, risk areas, etc.), to those in which any intrusive monitoring will always be inadequate and illegal. These are especially the places reserved for hygiene (showers, toilets) and employee rest areas, as the SAC has repeatedly emphasized in its decisions.[52]

The approach of the Czech supervisory and judicial authorities follows the ECtHR's case law also in the rejection of attempts to give to the concept of privacy an always valid exhaustive definition. Privacy is in Czech law a "fuzzy" term as to its scope and content and its exact meaning must be found in each individual case.[53] The SAC has literally stated in one of its abundantly quoted decisions[54] that, in following the ECtHR, it does not intend to bind the concept of private life, understood in a broad sense, to any exhaustive definition. It is not always possible to distinguish clearly what constitutes the work of an individual and what constitutes his private life. The decision of the SAC concerned the audiovisual recording of a taxi driver inside his car, acquired by the staff of the control body, i.e. the Lord Mayor of Prague Office. The case therefore differed from private law disputes between employees and employers, but it is significant for the present analysis that the Prague Municipal Court first found that such a recording did not catch anything private and the taxi driver's right to private life was not affected.[55] The SAC, however, took an opposite view. The taxi driver spends most of his working day in the vehicle, communicates with customers during journeys and thus develops his contacts with the outside world, which implies that the public authority has prima facie affected the right to private life of a taxi driver within the meaning of Article 8 ECHR.

Referring to the previous analysis (relating to the interpretation of Section 316(1) LC), it is worth recalling that the extent of the private sphere of an employee in the workplace is, *a contrario*, defined by those options of employee checking that, although implemented through sophisticated technological devices, are not considered as an interference with privacy. The private sphere of an employee, as we have seen, does

50 E. Janečková, V. Bartík, Ochrana osobních údajů v pracovním právu…, *op. cit*. n. 12, p. 132.

51 J. Morávek, Kontrola a sledování zaměstnanců…, *op. cit*. n. 16, p. 573.

52 For instance, in the Judgment of the Supreme Admnistrative Court on teh case 5 As 158/2012 – 49 (23.08.2013) it was stated that: "Monitoring must be directed at the employer's property, not the employee's person (camera direction), and must be done at the workplace, not in the hygienic or resting places".

53 J. Morávek, Kontrola a sledování zaměstnanců…, *op. cit*. n. 16, p. 573.

54 Judgment of the Supreme Administrative Court on the case 1 AFs 60/2009 (5.11.2009).

55 Judgment of the Municipal Court in Prague on the case 10 Ca 99/2007 (22.01.2009).

not go so far as to prevent the employer from registering the employee´s access to the Internet at the workplace. However, if an employer controls also the content of websites visited, the legal border will already be exceeded.[56] Similarly, an employer does not interfere with employee privacy by tracking the number of emails received and sent, and with whom they are exchanged.[57] Likewise, Czech commentators concede that GPS monitoring of a service vehicles location is also outside the privacy of an employee, because in this case it is indeed about protection of the employer's property (and there is a qualitative difference from the tracking of employees as such - by which Czech Post violated their privacy in the above-mentioned case).[58]

7. The nature of activity justifying intrusion into privacy

If under the Section 316(2) LC, a proportionate encroachment upon employee privacy may be justified by "a serious cause consisting in the employer's nature of activity", every employer would certainly wonder whether activities carried out by his company are of such a sensitive nature. At the same time, it is unlikely that anyone will be surprised that the law or subordinate regulations (or the explanatory memorandum to the Labor Code) contain no list of such activities, and again everything is defined case-by-case, within the reasonable discretion of judicial and administrative decision-makers.

Here, again, the above-mentioned recommendation to distinguish control, from surveillance or monitoring of employees, makes sense. This is because every employer can check whether employees are abusing his resources, whether they effectively use working time, produce good results etc., but only if he does not interfere with their privacy.[59] On the contrary, to survey or monitor employees, i.e. to interfere with their

56 Judgment of the Supreme Court on the case 21 Cdo 1771/2011 (16.08.2012). Likewise in H. Zemanová Šimonová, Právní prostředky ochrany osobnosti zaměstnance, "Buletin advokacie" 31.10.2016, http://www.bulletin-advokacie.cz/pravni-prostredky-ochrany-osobnosti-zamestnance?browser=mobi (accessed 31.10.2018)

57 UOOU Opinion no. 2/2009 confirms that assessment especially "if there is suspicion of misuse of the means of work".

58 J. Metelka, GPS na pranýři aneb sledování zaměstnanců, "Právní prostor", 15.04.2014, https://www.pravniprostor.cz/clanky/pracovni-pravo/gps-na-pranyri-aneb-sledovani-zamestnancu (accessed 31.10.2018). This author emphasizes that if an employer allows employees to use a service vehicle for private use, its GPS monitor unit must give the possibility to switch between private and service régime of the car, in order to avoid tracking while the employee is using the car privately. Likewise see in S. Bednář, Metelka J., GPS monitoring zaměstnanců podruhé, "EPRAVO.CZ", 18.07.2017, https://www.epravo.cz/top/clanky/gps-monitoring-zamestnancu-podruhe-106141.html (accessed 31.10.2018).

59 According to H. Zemanová Šimonová, Právní prostředky ochrany osobnosti zaměstnance…, *op. cit*. n. 56, these reasons are generally in the interest of each employer and therefore are not specific enough to represent serious cause. Nonetheless, in the instructions posted on the Internet,

privacy in a proportionate way, can only be introduced by an employer who has serious cause to do so. This cause usually does not exist, according to the SUIP, in the production of ordinary products or the provision of routine services.[60] However, such a simple answer is not a sufficient guide to practice, although it can be deduced from it that the protection of the employer's property in general is not, in any circumstances, a legitimate reason for limiting the fundamental right of employees to privacy.

Both the commentary literature and the UOOU in their statements suggest that a better guideline as to whether there is an increased or extraordinary need for oversight at the workplace can be provided by a kind of "situational analysis", made from the position of an objective, impartial observer. The serious cause for such monitoring is thus given when:

- important sums of cash are handled (e.g. international bank transfers[61]);
- the workplace is subject to a special regime (e.g. prisoners' work,[62] classified information[63]);
- there is an increased risk of injury, explosion etc.[64] (chemical plants, nuclear power plants[65]);
- there is a prevailing reason for the protection of intellectual and industrial property rights or very valuable know-how, personal data of third parties,[66] equal treatment and non-discrimination, if these rights are reasonably endangered.[67]

confusing enumerations of reasons that should justify employee monitoring which include not only the protection of life and health in the workplace, but also the control of employee performance. See for instance D. Řezníček, T. Černický, Problematika kamerového systému na pracovišti, "EPRAVO.CZ", 27.07.2018, https://www.epravo.cz/top/clanky/problematika-kameroveho -systemu-na-pracovisti-107905.html (accessed 31.10.2018). However, in the case of high-tech monitoring, it is not possible to agree with such suggestions.

60 See the web of SUIP http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem/ (accessed 31.10.2018).

61 UOOU opinion No. 2/2009, *op. cit.* n. 25.

62 *Ibidem*.

63 See for instance in H. Zemanová Šimonová, Právní prostředky ochrany osobnosti zaměstnance…, *op. cit.* n. 56.

64 E. Janečková, V. Bartík, Ochrana osobních údajů v pracovním právu…, *op. cit.* n. 12, p. 132.

65 J. Vych, Navrhovaná změna v oblasti ochray soukromí zaměstnanců, "EPRAVO.CZ", 4.09.2015, https://www.epravo.cz/top/clanky/navrhovana-zmena-v-oblasti-ochrany-soukromi-zamestnancu-98803.html (accessed 31.10.2018).

66 L. Jouza, Ochrana osobnosti zaměstnance v pracovněprávních vztazích, "EPRAVO.CZ", 9.10.2017, https://www.epravo.cz/top/clanky/ochrana-osobnosti-zamestnance-v-pracovnepravnich-vztazich-106434.html (accessed 31.10.2018); K. Valentová, Jak legálně sledovat zaměstnance, "Právní rádce", 8.07.2016, http://www.vilmkovadudak.cz/Media.aspx?id=534 (accessed 31.10.2018).

67 P. Molek, Základní práva… *op. cit.* n. 47, p. 339.

Of course, such enterprise as the State Printer of Valuables (*Státní tiskárna cenin*) would be included in this enumeration, but only in a situation where it actually prints banknotes, stamps or state bonds. Camera surveillance of employees (and subsequent processing of the filmed material without their consent) done at the moment when less sensitive products, such as meal vouchers and tickets were being printed, was found to be unjustified by the UOOU and then by the Municipal Court in Prague.[68] The use of sophisticated tracking techniques must be proportionate to the seriousness of the cause. In the above-mentioned cases, the camera surveillance of bus crews and the GPS tracking of Czech Post delivery staff during their entire work period could not be justified by the nature of their activity and by the risks it may cause. Similarly, the SAC has stated in the case of cameras designed to ensure the safety and protection of guests and hotel staff that the luxury category of the hotel was not in itself sufficient justifiable reason for such an intense encroachment upon privacy.[69]

A logical question of every employer operating a shop would be whether the work with cash (of what volume?) justifies the monitoring of sales staff and cashiers. Even in these cases, the monitoring of employees at work is usually very disproportionate, especially when it is a pre-emptive measure to prevent possible cases of fraud. The use of (most often) cameras must be based on reasonable suspicion and should be focused on cash movements, discount coupons, etc., not on employees at work.[70] This follows both from the aforementioned case law of Czech Courts (tracking the fares collected by a bus crew,[71] or discounts provision in a PC game shop[72]) and from the ECtHR case law. The Strasbourg Court found in *Köpke v. Germany* (2010)[73] that a time-limited video surveillance aimed exclusively at persons reasonably suspected of theft was permissible, while in the case *Lopez Ribalda and others v. Spain* (2018)[74] it outlawed the extensive camera surveillance of cashiers in a supermarket, even though it had led to five of them being convicted of theft.

The amount of cash or values in general handled by an employee, which would justify a "serious cause" for monitoring, is nowhere precisely defined. A reasonable consideration suggests that the value concerned must not be negligible. Sounds like

68 Judgment of the Municipal Court in Prague on the case 6 Ca 227/2008 (27.09.2011).

69 Judgment of the Supreme Administrative Court on the case 5 As 158/2012 (23.08.2013).

70 The commentators also stress the condition that "the threat must be real", see in P. Molek, Základní práva…, *op. cit.* n. 47, p. 339, or that "frequent thefts" occur, see B. Jarošová, Co je a není protiprávní, když vás šéf sleduje nejen kamerou, "Idnes.cz", 5.05.2017, https://finance.idnes.cz/legislativa-kamery-na-pracovisti-kontrola-aut-e-mailu-a-telefonu-phf-/podnikani.aspx?c=A170427_2321709_podnikani_kho (accessed 31.10.2019).

71 Judgment of the Supreme Administrative Court on the case 10 As 245/2016 – 41 (20.12.2017).

72 Judgment of the Municipal Court in Prague on the case 8 A 182/2010- 69.77 (2.09.2014).

73 Judgment of the European Court of Human Rights of 5 October 2010 on the case Köpke v. Germany, application No. 420/07.

74 Judgment of the European Court of Human Rights of 9 January 2018 on the case Lopez Ribalda and others v. Spain, application No. 1874/13 and 8567/13.

an anecdote in this regard, a case where the ÚOOÚ had to deal with the deployment of cameras in a kitchen of an office building, which was to prevent the theft of yogurts from a fridge.[75] The cases mentioned above, however, show that even "normal" operating amount of cash collected by the cash register does not constitute a sufficient reason for continuous camera monitoring. For the difficulty of determining what cash at the cash register is already a reason to monitor, it is always preferable to give priority to an agreement on employees' responsibility for the amount entrusted, which relieves the employer of the obligation to prove fault of employees in the event of loss or deficit.

8. Information or consent, open or covert monitoring

It is probably the least obvious to Czech employers, also to their advisers and legal commentators, whether and when it is possible to monitor employees in secret, or vice versa, whether it is always necessary to inform them or even to obtain their consent. It is perhaps not surprising that the prevailing uncertainty and diverging opinions are due to the unclear wording of legal provisions on the one hand, and case law that is sometimes inadequate and sometimes difficult to interpret on the other.

Section 316(2) LC speaks of "open or concealed surveillance (monitoring) of employees" and it can therefore be construed that both forms of monitoring are, as the case may be, permissible. Para 3 of the same Section however requires, that in case of any surveillance in the sense of para 2, the employer shall directly inform employees about the scope and methods of his control. To conciliate the concealed or covert surveillance mentioned in para 2 with the obligation to keep employees informed about it, is possible if such information is given only ex-post, after the monitoring was carried out. However, such an interpretation of obligation set by law seems superfluous or even redundant as in any subsequent conflict between the employer and the employee, the latter would always learn that the former gathered evidence about his or her misbehavior through surveillance in the workplace. On the other hand, preliminary information given to an employee that "starting from tomorrow cameras will monitor your activity" would hardly meet with the consent of that employee and is most unlikely to catch him doing something wrong. What then is the correct conduct, which would not infringe the law and still be efficient in securing protection of the employer´s rights and legitimate interests?

Relatively simple is the answer to the question of whether or not the employer needs the employee's consent. Section 316 LC does not provide for such consent and it is assumed that obtaining approval from an employee to interfere with his privacy would be unlawful and void. With such approval, an individual in the position of

75 A. Vejvodová, Šéf není velký bratr. Za šmírování zaměstnanců hrozí firmám nově milionová pokuta, "Právní rádce", 4.10.2017.

a weaker party would give up his or her fundamental right in favor of the stronger party. Such is the unambiguous position of Working Party 29 at the EU level,[76] as well as of the Czech UOOU[77] and of local commentators.[78] Section 316 is formulated as a mandatory provision of law, and the employer must assume that his monitoring is either legal under the Labor Code or is not. The employee's approval cannot change anything there, and certainly cannot legalize an intervention into privacy that does not meet the requirements of paras 2-3 of Section 316 LC.

Also, an employer can partly be confused by the wording of Section 86 of the Civil Code, according to which "it is not possible to disrupt privacy without the consent of the person concerned". Every employer, however, must remember that for the monitoring of employees there is a *lex specialis* to this provision of the Civil Code, and that is Section 316 LC. Only if, vice versa, the employer were to be tapped by an employee, as in the case discussed above[79] (that ended with the Constitutional Court decision), the general provisions of the Civil Code (Sections 86-88) would apply. If the defense of fundamental rights of the weaker party were depending on it, the secret recording of an employer by an employee (and its subsequent use as evidence in a labor dispute) would be admissible.

An employer's uncertainty may also derive from the provisions of Article 6(1) of the GDPR, i.e. from the personal data protection requirements. This provision allows for the processing of personal data when the data subject has given consent to it for one or more specific purposes (Art 6(1)a GDPR), or also when such processing is necessary for the legitimate interests pursued by a controller or by a third party, except where such interests are overridden by interests or fundamental rights and freedoms of the data (Art 6(1)f GDPR). Here, the employer must consider once more that if he wants to make a record of a particular employee's behavior and further process it, he must stay within the limits of proportionality. In view of all that has been said so far, it is (almost) certain that any wider and systematic monitoring of employees at the workplace will not fit into the option provided by Art 6(1)f GDPR. And since the consent of employees with such monitoring under Art 6(1)a GDRP would violate the provisions of Section 316 LC, the employer should not be even tempted to seek to acquire it.

76 WP 29 was established as an independent advisory body to Article 29 of (now no longer valid) the Data Protection Directive. On the issues of obtaining the consent of the employee it took a position in its Opinion No. 2/2017, p. 4.

77 See for instance D. Dostál, GDPR ovlivní také kamerové systémy ve firmách. Na co si podniky musí dát pozor? "BusinessInfo.cz", 9.01.2018, http://www.businessinfo.cz/cs/clanky/gdpr-ovlivni-take-kamerove-systemy-ve-firmach-na-co-si-podniky-musi-dat-pozor-99784.html (accessed 31.10.2018).

78 E. Janečková, V. Bartík, Ochrana osobních údajů v pracovním právu…, *op. cit.* n. 12, p. 132.

79 Decision of the Constitutional Court on th case II. ÚS 1774/14 (9.12.2014).

Information to employees, however, is not the same as their consent and the real puzzle for employers, therefore, is whether and when employees can be monitored in the sense of paras 2-3 of Section 316 LC without their knowledge. Although paragraph 2 refers to the possibility of employee concealed (or covert) monitoring, a clear answer to the question of whether and when it is possible is missing in Czech law. Section 316(3) LC specifically requires employers to inform employees directly but does not say to do so beforehand.

On the one hand, there is the SAC judgment from 2013,[80] in which the Court for the interpretation of Section 316 clearly states (author's translation):

"Monitoring of employees is only possible on prior notice and only where it is necessary to protect the health of the person or property of the employer ... The information to the employee before the start of monitoring should also explain the scope and method of carrying out such control".

The SAC in this statement, unfortunately, also mixes the terms "control" and "monitoring", which could lead to uncertainty as to whether the employer proceeds according to para 1 or para 2 of Section 316 LC. From the circumstances of the case (the permanent camera surveillance of hotel premises) and from the content of the SAC judgment, it can be safely inferred that this was about monitoring within the meaning of para 2 of this Section. For these types of employee tracking, the SAC requires prior notification. In connection with this, some commentators urge employers to forget about hidden monitoring of employees. They recommend them to include the possibility of monitoring to the company´s internal regulations, to discuss it in advance with employees' representatives and to post relative information on notice boards in the company's premises.[81] Such approach ultimately points to the priority of prevention over intrusion into privacy. An employer warning his employees about the possibility of monitoring in the workplace can practically reduce the risk of their inappropriate behavior without risking violation of the Labor Code.

Nevertheless, opinions can also be found which, for particularly serious reasons, and thus exceptionally, allow the covert monitoring of employees.[82] Logically, these are not cases which fall under Section 316(1) LC, within which the employer, through his control without warning, does not interfere with the privacy of employees. Here, it is about those exceptional cases where the employer's tracking technology will interfere

80 Judgment of the Supreme Administrative Court on the case 5 As 158/2012 – 49 (23.12.2013).

81 M. Štefko, K problému sledování vlastních zaměstnanců, "Právo a zaměstnání" 2005, No. 1; M. Štefko, Soukromí zaměstnanců pod ochranou inspelce práce…, *op. cit.* n. 14; T. Kadlecová, Monitoring zaměstnanců, "Praktická personalistika" 2015, No. 11-12, p. 27; J. Zahradníček, Sledování elektronických komunikací na pracovišti, "Právní rádce" 2016, No. 11; M. Hromanda, Ochrana osobnosti zaměstnance při elektronické komunikaci… *op. cit.* n. 14.

82 J. Morávek, Kontrola a sledování zaměstnanců…, *op. cit.* n. 16; Kalvoda A., Ochrana majetkových zájmů zaměstnavatele, ochrana osobních práv zaměstnance a inspekce práce, "Práce a mzda", 2018, No. 6.

with the privacy of employees without their knowledge, and yet it will be legal. The SC had the opportunity to comment on the issue in 2017 when a GPS monitoring device was installed in a service vehicle used by an employee and the employee concerned learned about it only during the use of the vehicle.[83] Unfortunately, due to a procedural error of the complainant-employee (when submitting an extraordinary remedy he changed his objections and arguments in comparison with the previous court proceedings), the SC rejected his appeal without assessing the merits of the case. The guideline can thus be found only in the existing case law of the ECtHR, which the Czech courts usually follow.

The ECtHR in the *Köpke v. Germany* case from 2010, found no breach of the Convention in the way the German courts approved the covert video surveillance of employees in one supermarket department operated by a hired detective agency. Surveillance was based on suspicion and the Court took it as being relatively targeted, and also proportionate in terms of time-span, even though all employees of the department were monitored over several weeks. To what extent the result of this case can be generalized, however, is a matter of debate.[84] Given that Section 316 LC does not contain an explicit ban on covert monitoring, the domestic situation is not unlike the conditions in Germany that played a role in the given case. Everything would probably depend on the proportionality test that the Czech courts would apply in similar cases. On the other hand, in the newer decision of 2017, in the case *Bărbulescu v. Romania*,[85] where the e-mail communication of an employee was monitored (i.e. not only the privacy but also the secrecy of correspondence was violated), the Grand Chamber of the ECtHR stressed that "for the measures to be deemed compatible with the requirements of Article 8 of the Convention, the notification should be clear about the nature of the monitoring and be given in advance."[86]

If a Czech employer wants to be sure that he will not enter into conflict with the law, he should (also for the sake of compliance with the requirements of personal data protection) indicate the possibility of monitoring in his work regulations and inform about it to every employee before an employment contract is signed.[87] And

83 Judgment of the Supreme Court on the case 21 Cdo 817/2017 (7.06.2017).

84 See especially the above mentioned ECtHR descision in *Lopez Ribalda v. Spain* from 2018. Unlike the *Köpke v. Germany* case, the camera filming here was contrary to the Convention because it was focused enough, it was not based on suspicion of specific employees, and the Spanish law explicitly required preliminaryinformation about such monitoring.

85 Judgment of the European Court of Human Rights on the case of 5 September 2017 on the case Bărbulescu v. Romania, application No. 61496/08.

86 The European Court of Human Rights, Q & A Grand Chamber judgment in the case of *Bărbulescu v. Romania* (application No. 61496/08), Press Unit, Strasbourg 5.09.2017.

87 UOOU in its Opinion No. 2/2009 emphasizes that this information duty is not fullfilled by a mere placement of signboard with the words "camera surveillance", but only by providing full information about who is the data controller, where he/she can be contacted, as well as the details on how the collected data are processed.

then only, if there is a reasonable suspicion that such precautionary warning has not been enough and employees are seriously damaging the employer´s rights and legitimate interests, threatening health and safety in the workplace, he could then risk a very targeted and short-term deployment of sophisticated techniques to monitor them. Under such circumstances, this can be done without warning them again, that precisely on them and from tomorrow on, this monitoring will be used. Even in this case, as highlighted above, the monitoring should target the protected values (cash, keys, servers, access to special objects, hazardous handling of chemicals, etc.) rather than people in the workplace. Of course, the best assurance that could be given to Czech employers is by the Czech legislators if they would clarify the wording of paras 2-3 of Section 316 LC so as not to raise doubts as to whether the mention of concealed (covert) surveillance means its admissibility or not and whether direct information means advanced information or not.

9. Notes on individual methods of employee monitoring

Notwithstanding the extent of the previous analysis, it has not been possible to present all information that can be gained from the existing practice of the Czech administrative and judicial authorities regarding the legality of using various tracking tools that may cause different types of interference with employees' privacy. Therefore, this sub-chapter briefly summarizes the findings on different types of modern technologies that are usually used for tracking of employees.

Regarding *cameras in the workplace*, which has been given overwhelming attention so far, there should be no doubt that nowadays they represent one of the most obvious violations of employee privacy. As mentioned in the Introduction, control by the SUIP recently discovered that employers' abuse of camera monitoring featured in 80% of cases inspected by this authority. Camera surveillance of the workplace itself (i.e. not of entry to the company premises, or in lifts and corridors) must always be the last option for safeguarding property and health, during specific activities that justify such monitoring in the sense of Section 316(2) LC. Therefore, it can never be used to monitor the efficiency of employees' performance. To keep within the limits of proportionality, cameras should be aimed at the employer's sensitive equipment or facility rather than on the staff. Cameras should be totally excluded in places where the employee is changing and performing hygiene. For example, an employer may use a photo trap on a sensitive device or a camera to monitor empty premises after termination of working hours.[88] In these justified and reasonable cases of camera monitoring there should not even be the problem of having to inform everyone in

88 V. Odrobinová, Narušení soukromí zaměstnanců může nově trestat i inspektorát práce. Firmám hrozí až milionová pokuta. post on https://www.vox.cz/naruseni-soukromi-zamestnancu-muze-nove-trestat-i-inspektorat-prace.html (accessed 31.10.2018).

the workplace. However, in the case law of the Czech courts, so far there has not been a single case where camera surveillance of employees in the workplace has been found suitable, necessary and proportionate.

GPS trackers are most commonly used in service vehicles, where such method of tracking may be fully proportionate. Service vehicles are the property of the employer and should be protected correspondingly. It is however difficult to justify the deployment of GPS trackers only by better traffic safety, because these devices cannot avert traffic accidents. In the case of a company car intended both to commute to work and to visit clients, the GPS device should operate (be switched on) only during "work related" journeys. Therefore, the use of a GPS tracker is more appropriate if the employer does not permit the use of the vehicle for private purposes. When a vehicle is assigned to a particular employee, the processing of GPS data always means the processing of his personal data. The employee does not have to agree to GPS tracking of the vehicle (see art. 6(1) f GDPR) but should be informed about it. The employer is also legally entitled, even required, to record usage data for the vehicle in a log book of journeys made and mileage accrued (for accounting and tax purposes).[89] A completely different case would be a GPS tracking of employees as individuals during working hours. For that, justification could only be found in extraordinary situations, such as the movement of rescue workers in a burning factory, but not, for example, to track the accuracy and efficiency of mail delivery personnel.[90]

The biometric identification of employees is in some way close to GPS tracking, although it is most often used to record their time of arrival to and departure from the workplace. The UOOU considers that the use of these systems for routine recording is a disproportionate collection of personal data and hence an interference with employee privacy if the biometric data are stored in a device in a form that permits their further processing.[91] In some cases, however, biometric identification can be used to control access (in the case of nuclear installations it is even mandatory in the Czech Republic[92]), respectively, to monitor whether there are only authorized employees in the workplace, or also other persons. For these authentication/verification purposes, it may not be necessary to retain the collected personal data in any stable database. Therefore, certain uses of biometric identification may be both proportionate and legal. The UOOU itself, however, points to a contradiction with Section 316 LC in the use of biometric identification beyond the records of employee presence in the workplace, e.g. to control employee movements within the premises

89 S. Bednář, J. Metelka, GPS monitoring zaměstnanců podruhé…, *op. cit.* n. 58, with reference to the practice of the UOOU, state that an electronic book of journeys is considered by this supervisory body much more leniently than direct employee monitoring.

90 Judgment of the Municipal Court in Prague on the case 6 A 42/2013 – 48.183 (5.05.2017).

91 UOOU Opinion No. 1/2017, https://www.uoou.cz/stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu/d-23849/p1=3569 (accessed 31.10.2018).

92 Decree No. 144/1997 Coll., on physical protection of nuclear materials and facilities.

(collection and processing of data on individuals resulting from traces left by such movements, etc.). In essence, if GPS and biometric tracking would become similar to a chip implanted under the skin of an employee, it will always be disproportionate and therefore prohibited for the overwhelming majority of employers.[93]

E-mail monitoring is also a very sensitive issue, because of the possibility to violate the secrecy of correspondence, which is explicitly protected at both international and constitutional levels, (beyond the scope of general privacy protection). However, according to the SUIP, this type of monitoring is currently the most frequent case of privacy violation in the Czech Republic.[94] In previous chapters, the difference was explained between, on the one hand, the employer's control over whether an employee does not abuse a work PC for unauthorized private communication, which can be achieved by a random check of number of emails received and sent to non-job-related addresses and, on the other hand, the invasion of employee privacy and secrecy of communications.[95] The employer can access the content of an E-mail sent to the address containing the name of an employee (even if the domain is a company name) but only in very exceptional cases where it is necessary for the performance of work tasks, the negligence of which would seriously harm the employer´s business. This can happen, for example, in the case of a sudden illness or injury of an employee and only during the period of time taken to redirect all of his business communications to another employee.[96] Even here of course, the employer is not permitted to read E-mails whose content is obviously not connected to the employee's business activity. The described limitations do not apply to E-mails addressed to the company address such as info@company.cz.

The monitoring of employee activity on PCs and social networks is again a question of the proportionality of the protected purpose and the chosen means of control. It was shown above that the SC did not consider as a violation of privacy the control of number of hours spent by an employee on a company PC and the internet viewing web pages unrelated to company business.[97] The proportionality threshold here, as in the case of E-mails, was to abstain from inspecting the content of web pages visited or files downloaded by the employee concerned. Very interesting in this context is

93 P. Molek, Základní práva…, *op. cit.* n. 47, p. 340.

94 K. Kolářová, Většina stížností na nepřiměřené sledování v práci je oprávněná…, *op. cit.* n. 3.

95 The UOOU requires that if the employer steadily monitors and evaluates only the volume of e-mails and whether they are directed to work-related addresses, then the employees must be informed about the implementation of the tracking tools. See web UOOU https://www.uoou.cz/zamestnavatele/ds-5057/archiv=0&p1=2611 (accessed 31.10.2018). This should be done even when monitoring may be necessary, for instance to prevent employees from contravening Act No. 127/2005 Coll. about electronic communications by disseminating spam from the company's E-mail address. Likewise J. Mikulecký, Monitorování zaměstnanců je legální!, "DSM" 2010, No. 3.

96 A. Kubíčková, V. Patáková, Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z, "Práce a mzda" 2017, No. 11.

97 Judgment of the Supreme Court on the case 21 Cdo 1771/2011 (16.08.2012).

the recent ECtHR case law, *Libert v. France*, from 2018[98]. In it, the Court allowed the possibility of checking the PC content of a redundant employee (without his knowledge), in which pornographic material was discovered in a folder labeled "personal". The peculiarity of this decision is the fact that had the employee placed these files in a folder marked "private", the employer would not have been allowed to perform such control without the former employee's knowledge and presence (as limited use of the PC for "private" purposes was authorized). Despite some formalism of the decision, there is a consistency with the recommendation of the Working Party (hereinafter WP) 29 (reflected in the opinions of Czech supervisory bodies as well as in the literature), that on the company's server or cloud service, each employee should have a designated space (appropriately labeled) to which other employees and the employer cannot enter.[99]

A clearly disproportionate interference with privacy is found when an employer tries to covertly monitor employees' personal profiles on social network sites such as Facebook or Twitter. WP29, as well as Czech commentators, however, believe that in exceptional cases and with the awareness of the employees concerned, such targeted and unsystematic monitoring could be lawful, if for instance a valuable business secret is to be protected.[100] Finally, it is beyond doubt that the employer has the right to check whether employees install illegal software on a company PC or do not connect to it devices that could endanger the protection of company data, since in these cases of protection of property the content of files created by employees would not be disclosed.

Telephone call recording is quite common in call centers where it is used to control the quality of client requests´ processing. In these cases, undoubtedly service calls from a dedicated service line and equipment are made, and both parties are warned from the outset that their conversation may be monitored.[101] In other cases, where an employer is interested in whether and to what extent employees use his facilities and working time to deal with their private matters, the analogy with E-mails and with the abuse of company PCs is fully applicable. Pursuant to Section 316 (1) LC,

98 Judgment of the European Court of Human Rights of 22 February 2018 on the case Libert v. France, application No. 588/13.

99 WP 29 Opinion No. 2/2017.

100 *Ibidem*; see also E. Škorničková, Důvěřuj, ale prověřuj? GDPR zpřísňuje monitoring zaměstnanců, "GDPR.cz", 6.03.2018, https://www.gdpr.cz/blog/monitoring-zamestnancu/ (accessed 31.10.2018); M. Nulíček, K. Kovaříková, J. Tomíšek, O. Švolík, GDPR v otázkách a odpovědích, "Buletin Advokacie", 3.11.2017, http://www.bulletin-advokacie.cz/gdpr-v-otazkach-a-odpovedich (accessed 31.10.2018).

101 The UOOU warns that the recording of such a call and other related work with it is always the processing of the personal data of the employees of the call center and if the caller can be identified, then also of the company's client. It acknowledges that such processing may have a legitimate purpose consisitng in performance or change of contract, improvement of customer service etc. See UOOU Opinion No. 5/2013.

the employer is authorized to check the numbers dialed and the time spent handling out-of-work calls. As long as he does not try to detect the contents of the calls, there is no interference with the privacy of employees.[102] An employee's consent to the monitoring of his telephone activities is legally irrelevant. Preliminary information to employees that compliance with the ban on use of company phones for private purposes can be checked, is unanimously recommended by the literature since any case of more extensive and systematic monitoring of phone calls may fall under both Section 316 (2) LC and personal data protection.

The use of spyware, keyloggers and other high-tech means in the workplace would be, for reasons that have now been repeated several times, mostly very inappropriate and therefore unlawful. These high-tech means represent a far more systematic and less controllable invasion into employee privacy and their personal data than most of the above-mentioned methods and devices.[103] However, even here, the legal literature does not exclude exceptional cases where the protection of extraordinary know-how, the prevention of increased health and safety risks (i.e. access and work with a sensitive database, access and use of a particularly hazardous equipment) may justify protection against unauthorized entry and dangerous manipulation by an instantaneous identification of users and their following of a standard operating procedure. Preventive measures focusing on the employer's assets, not on the employees at work, should always be preferred and all deployed measures should be communicated to all the employees concerned.[104]

10. Conclusion

Czech law on the protection of privacy of employees in the workplace, as well as the authorities applying it, are principally in line with generally accepted European standards. There is no doubt that the employee in the workplace has the right to privacy and that the content, extent and degree of protection of this fundamental right are understood and protected in the Czech Republic in accordance with the ECtHR. However, this basic consensus on values, and their substantive and procedural legal safeguards, does not mean that Czech law currently answers all questions and leads employers safely outside the restricted zone of prohibited ways of employee monitoring.

Possible ways of using high-tech devices in the control and monitoring of employees are regulated in the Czech Republic, in particular, by a general regulation

102 Judgment of the Supreme Court on the case 21 Cdo 747/2013 (7.08.2014).

103 P. Mališ, Právní aspekty používání keyloggerů, "PrávoIT.Cz", 9.12.2008, http://www.pravoit.cz/novinka/pravni-aspekty-pouzivani-keyloggeru (accessed 31.10.2018).

104 See for instance M. Štefko, K problému sledování vlastních zaměstnanců, "Právo a zaměstnání" 2005, No. 1.

of labor law. The privacy in the workplace issue enjoys the vivid attention of commentators and the case law of the highest judicial courts is also growing year after year. In general, however, the statutory provisions remain rather unclear, legal advisors sometimes contradict each other and even state authorities do not always provide entirely consistent guidance. Overall, an employer without legal education may find it difficult to stay on the safe side when he gets into more sophisticated monitoring of his employees.

The analysis has shown the main causes of these uncertainties. In addition to the duality of legal regulations affecting workplace monitoring – the Labor Code and the data protection rules – it is primarily the wording of the key Section 316 LC. Certain tracking measures will interfere with the privacy of employees, but not always with the processing of their personal data and vice versa; employee data can be retrieved and processed without interfering with their privacy – which does not mean that those data are not protected. Adoption of one common *lex specialis* defining the employer's duties in the field of employee monitoring and data collection is no longer possible because its application would have directly replaced the existing GDPR, i.e. a directly applicable piece of EU legislation enjoying precedence over any national rule.

On the contrary, the refinement of Section 316 LC would be desirable and is entirely within the purview of the Czech legislator. To emphasize the difference between paragraph 1 and paragraphs 2-3, not to repeat the same terms referring to the employer's control, to underline that acting consistently within the limits of Section 316 (1) LC does not imply an interference with employee privacy (and thus no encroachment upon fundamental rights), whereas falling under Section 316 (2-3) LC already means interference, as well as to determine more clearly whether covert monitoring is possible and when advanced information about employee control is strictly required; all these amendments would remove a great deal of uncertainty on the part of employers. However, even the most sophisticated law cannot precisely set the limits of proportionality once and for all, cannot list all grounds justifying employee monitoring, etc. There would always be the necessity to await judgments in cases that are not factually exclusive and permit to formulate general standards and set more precisely the boundaries between legal and illegal monitoring.

Czech courts have already provided such practical guidelines for cases of monitoring employees' work on PCs, their e-mail communications and telephone calls. Courts took a clearly negative stance in several of the above-cited cases towards deployment of cameras that tracked employees for the whole or most of their working hours. Along with this jurisprudence, as well as with decisions of the ECtHR, the Czech administrative authorities (UOOU and SUIP) and Czech commentary literature, outlined some boundaries between prohibited and conditionally allowed acts of employers. However, the examples given in soft law and Czech lawyers' articles naturally point to cases of obviously exaggerated and therefore forbidden monitoring,

or on the contrary to well-justified cases of employee control which would be logically and legally difficult to challenge. For employers in the field, which is not exceptional by extraordinary risks, by unique know-how or, at least, by numerous operations with high financial amounts, the boundary of conditionally permitted monitoring still remains - a bit unclear.

Czech employers may thus lament that there is still a lack of clarity and perhaps legal certainty on the issue, nevertheless, certain recommendations they should follow are sufficiently obvious. They can also be considered as a brief summary of the case law and the opinions of administrative bodies analyzed above.

Interference with employee privacy can never be justified by the protection of employer's property in general, under any circumstances, or by the need to monitor and evaluate the performance of employees. Certain restrictions on the fundamental right to privacy are permissible only if justified by the need for a higher level of protection (or higher risk of threat) of other legally protected rights and interests. Clear prohibitions and preventive measures to avoid breaching the rules of the workplace (by restricting employee access to certain devices, websites, etc.) are always more appropriate than monitoring what the employees actually do with particular devices or equipment.

Targeted, time-limited tracking, justified by the employer's previous negative experiences or reasoned suspicion, is always more appropriate than a comprehensive, long-term, and only prevention-focused monitoring of employees at work. To focus the tracking device on an equipment, car, cash desk etc. is generally more acceptable than targeting the employees in person and their movement at the workplace. Preliminary information that monitoring can be used, how it will be handled and controlled and who will be responsible for it, is always a more appropriate and secure way of proceeding than any employer's attempt to acquire information about employee's behavior secretly.

Finally, yet importantly, even measures that meet the stated recommendations must pass the proportionality test, i.e. to demonstrate their suitability and necessity to achieve legitimate purpose and compatibility with maintaining of the minimum necessary employee privacy in the workplace. Although grossly disproportionate measures are apparent from the above-mentioned recommendations quite clearly, where precisely the boundary between proportional and non-proportional is situated in a specific case, will always remain difficult to tell in advance.

BIBLIOGRAPHY

Bednář S., Metelka J., GPS monitoring zaměstnanců podruhé. "EPRAVO.CZ" 18. 7. 2017, https://www.epravo.cz/top/clanky/gps-monitoring-zamestnancu-podruhe-106141.html (accessed 31.10.2018).

Beneš O., Za jakých podmínek je možné kontrolovat e-maily zaměstnance?, "EPRAVO.CZ", 16.03.2018, https://www.epravo.cz/top/clanky/za-jakych-podminek-je-mozne-kontrolovat-e-maily-zamestnance-107090.html (accessed 31.10.2018).

Borovec D., Prohlížeí internetu v pravoní době, aneb Nejvyšší soud ČR se vyjádřil k ochraně majetkových zájmů zaměstnavatele a soukromí zaměstnance, "EPRAVO.CZ", 28.08.2012, https://www.epravo.cz/top/clanky/prohlizeni-internetu-v-pracovni-dobe-aneb-nejvyssi-soud-cr-se-vyjadril-k-ochrane-majetkovych-zajmu-zamestnavatele-a-soukromi-zamestnance-85199.html (accessed 31.10.2018).

Červínek Z., Standardy přezkumu ústavnosti v judikatuře Ústavního soudu, "Jurisprudence" 2015, No. 4.

Doležílek J., Přehled judikatury ve věcech ochrany osobnosti, Wolters Kluwer, Praha 2016.

Dostál D., GDPR ovlivní také kamerové systémy ve firmách. Na co si podniky musí dát pozor?, "BusinessInfo.cz", 9.01.2018, http://www.businessinfo.cz/cs/clanky/gdpr-ovlivni-take-kamerove-systemy-ve-firmach-na-co-si-podniky-musi-dat-pozor-99784.html (accessed 31.10.2018).

ECHR, Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence, Council of Europe/European Court of Human Rights 2018, https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (accessed 31.10.2018).

Grasser U., Law, Privacy & Technology. Commentary series, "Harvard Law Review Forum" 2016, vol. 130(2).

Hromanda M., Ochrana osobnosti zaměstnance při elektronické komunikaci, (in:) H. Barancová, A. Olšovská (eds.), "Pracovné parvo v digitálnej dobe", Leges, Praha 2017.

Hromanda M., Ochrana osobnosti zaměstnanců v soudní praxi, "Acta Universitatis Brunensis Iuridica" 2018, vol. 604.

Janečková E., Bartík V., Ochrana osobních údajů v pracovním právu (Otázky a odpovědi), Wolters Kluwer, Praha 2016.

Jarošová B., Co je a není protiprávní, když vás šéf sleduje nejen kamerou, "Idnes.cz", 5.05.2017, https://finance.idnes.cz/legislativa-kamery-na-pracovisti-kontrola-aut-e-mailu-a-telefonu-phf-/podnikani.aspx?c=A170427_2321709_podnikani_kho (accessed 31.10.2018).

Jouza L., Ochrana osobnosti zaměstnance v pracovněprávních vztazích, "EPRAVO.CZ", 9.10.2017, https://www.epravo.cz/top/clanky/ochrana-osobnosti-zamestnance-v-pracovnepravnich-vztazich-106434.html (accessed 31.10.2018).

Kadlecová T., Monitoring zaměstnanců, "Praktická personalistika" 2015, No. 11-12.

Kalvoda A., Ochrana majetkových zájmů zaměstnavatele, ochrana osobních práv zaměstnance a inspekce práce, "Práce a mzda" 2018, No. 6.

Kolářová K., Většina stížností na nepřiměřené sledování v práci je oprávněná, "Česká pozice", 8.12.2017.

Kosař D., Antoš M., Kühn Z., Vyhnánek L., Ústavní právo. Casebook, Wolters Kluwer, Praha 2014.

Kubíčková A., Patáková V., Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z, "Práce a mzda" 2017, No. 11.

Matzner J., Může zaměstnavatel kontrolovat e-maily a sledovat online aktivitu zaměstnanců?, "Podnikatel.cz", 22.06.2017, https://www.podnikatel.cz/clanky/muze-zamestnavatel-kontrolovat-e-maily-a-sledovat-online-aktivitu-zamestnancu/ (accessed 31.10.2018).

Metelka J., GPS na pranýři aneb sledování zaměstnanců, "Právní prostor", 15.04.2014, https://www.pravniprostor.cz/clanky/pracovni-pravo/gps-na-pranyri-aneb-sledovani-zamestnancu (accessed 31.10.2018).

Mikulecký J., Monitorování zaměstnanců je legální!, "DSM" 2010, No. 3.

Molek P., Základní práva, Wolters Kluwer, Praha 2017.

Morávek J., Kontrola a sledování zaměstnanců, "Právní rozhledy" 2017, no. 12.

Nulíček M., Nové stanovisko WP29 ke zpravování osobních údajů zaměstnanců, "Právní rádce", 8.09.2017.

Pravdová M., Sociální media na pracovišti, "Právní prostor", 21.05.2018, https://www.pravniprostor.cz/clanky/pracovni-pravo/socialni-media-na-pracovisti (accessed 31.10.2018).

Procházková E., Několik poznámek k monitoringu zaměstnanců, "EPRAVO.CZ", 11.10.2017, https://www.epravo.cz/top/clanky/nekolik-poznamek-k-monitoringu-zamestnancu-106512.html (accessed 31.10.2018).

Řezníček D., Černický T., Problematika kamerového systému na pracovišti, "EPRAVO.CZ", 27.07.2018, https://www.epravo.cz/top/clanky/problematika-kameroveho-systemu-na-pracovisti-107905.html (accessed 31.10.2018).

Škorničková E., Důvěřuj, ale prověřuj? GDPR zpřísňuje monitoring zaměstnanců, "GDPR.cz", 6.03.2018, https://www.gdpr.cz/blog/monitoring-zamestnancu/ (accessed 31.10.2018).

Štefko M., K problému sledování vlastních zaměstnanců, "Právo a zaměstnání" 2005, No. 1.

Štefko M., Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod, "Jurisprudence" 2012, No. 7.

Štefko M., Soukromí zaměstnanců pod ochranou inspelce práce, "Acta Universitatis Brunensis Iuridica" 2018, vol. 604.

Ticháčková L., Vlastnictví zaměstnavatele versus soukromí zaměstnance, "EPRAVO.CZ magazine" 2016, No. 1.

Tomšej J., Metelka J., Ochana soukromí nad zlato?, "EPRAVO.CZ", 16.09.2013, https://www.epravo.cz/top/clanky/ochrana-soukromi-nad-zlato-92358.html (accessed 31.10.2018).

Valentová K., Jak legálně sledovat zaměstnance, "Právní rádce", 8.07.2016, http://www.vilmkovadudak.cz/Media.aspx?id=534 (accessed 31.10.2018).

Vejvodová A., Šéf není velký bratr. Za šmírování zaměstnanců hrozí firmám nově milionová pokuta, "Právní rádce", 4.10.2017, https://pravniradce.ihned.cz/c1-65902400-sef-neni-velky-bratr-za-smirovani-zamestnancu-hrozi-firmam-nove-milionova-pokuta (accessed 31.10.2018).

Veselý P., Jaké jsou možnosti zaměstnavatele při kontrole zaměstnanců a jak je to s instalací kamer se záznamem?, "EPRAVO.CZ", 14.07.2017, https://www.epravo.cz/top/clanky/jake-jsou-

moznosti-zamestnavatele-pri-kontrole-zamestnancu-a-jak-je-to-s-instalaci-kamer-se-zaznamem-106015.html?mail (accessed 31.10.2018).

Vobořil J., Nejvyšší soud k možnostem utajeného sledování zaměstnanců, "Zpravodaj Gender Studies" 2012, No. 12, 30.10.2012, http://zpravodaj.genderstudies.cz/cz/clanek/nejvyssi-soud-k-moznostem-utajeneho-sledovani-zamestnancu (accessed 31.10.2018).

Vych J., Navrhovaná změna v oblasti ochrany soukromí zaměstnanců, "EPRAVO.CZ", 4.09. 2015, https://www.epravo.cz/top/clanky/navrhovana-zmena-v-oblasti-ochrany-soukromi-zamestnancu-98803.html (accessed 31.10.2018).

Zahradníček J., Sledování elektronických komunikací na pracovišti, "Právní rádce" 2016, No. 11.

Zemanová Šimonová H., Právní prostředky ochrany osobnosti zaměstnance, "Buletin advokacie", 31.10.2016, http://www.bulletin-advokacie.cz/pravni-prostredky-ochrany-osobnosti-zamestnance?browser=mobi (accessed 31.10.2018).