PROTECTION OF EMPLOYEES' PERSONAL DATA IN THE PUBLIC AND PRIVATE SECTOR, IN THE CONTEXT OF THE NEW IT TECHONOLOGIES

Ancuța Gianina OPRE*
Simona ȘANDRU**

Abstract

The basic relations between employers and employees are regulated, traditionally, by the Labour Code and the related legislation. As regards the public sector, specific rules regarding the status of the employee as a public servant create a separate legal regime of the working conditions of this kind of staff, which is also completed by the general labour norms. However, nowadays, new problematic topics arise in the context of an working environment "under surveillance", where the employer chooses to make use of the latest technologies on the market in order to monitor the performance or the behaviour of their employees, whether in the private or public sector. According to the general principles set in the Romanian Labour Code, the employees' dignity and protection of personal data are to be respected. Therefore, any employer, either a public institution or a private company, has to comply as well with the obligations arising out of the legislation on data protection, especially whenever electronic devices are installed to survey the people or the equipment "at work". In the present paper we shall examine the IT technologies most used at the workplace from the perspective of the legal rights of an employee, on the one hand, and the legal duties of an employer, on the other hand, as established by the European and Romanian legislation on personal data protection, taking also into account a number of guidelines derived from the jurisprudence of the European Court of Human Rights and the European Court of Justice of the European Union

Key words: *Rights to privacy and personal data protection, Labour Code, surveillance techniques, relevant case law*

JEL Classification: [K10]

1. Introduction

The basic relations between employers and employees are regulated, traditionally, by the Labour Code and the related legislation. However, as regards the public sector, specific rules regarding the status of the employee as a public servant create a separate legal regime of the working conditions of this kind of staff, which is also completed by the general labour norms.

Nowadays, new problematic topics arise in the context of an working environment "under surveillance", where the employer chooses to make use of the latest technologies on the market in order to monitor the performance or the

* Mrs. Ancuța Gianina Opre is an Associate Professor (Conf. univ. dr.) at the Faculty of Legal and Administrative Sciences, "Dimitrie Cantemir" Christian University Bucharest.

** Ms. Simona Șandru holds a PhD from the Faculty of Law, Bucharest University.

behaviour of their employees, whether in the private or public sector.

The processing of employees' personal data is ordinary legal practice for any employer, as regards, for instance, the staff selection process, the job interviews or contests, keeping the professional file, filing in the register of employees (the so-called "REVISAL"), the payment of the salaries, reporting the social and public health contributions, retaining the income tax, appraisal of the individual performance, disciplinary proceedings, continuous professional training.

This sort of classical human resources activity is usually carried out in order to comply with the legal obligations, so there are no specific issues regarding data protection. Nevertheless, whenever automatic means of processing personal data are being put in place (for small or large databases), using inside, outside or shared resources (for instance, in multinational companies), an employer should be aware of the importance of taking the necessary measures to avoid illegal or unauthorized access to the employees' data. In fact, these obligations are incumbent on an employer not only according to data protection regulations, but also as a result of the obligation of maintaining the confidentiality as set out by the general labour law[1] or by the sectoral law on public servants[2].

Besides the classical ways of processing data mentioned above, there appears a different kind of situation whenever the employers use IT technologies in order to monitor the level of their employees' performance, so whenever an employer choses other purposes or means, than those legally imposed.

In the present study, we shall restrict our research to the latter case and shall examine two categories of means used by the employers in order to monitor, on the one hand, the external behaviour of their employees, related to the work, and to monitor the access to the electronic equipment/devices put at their disposal, in relation with their work, on the other hand[3]. As all employers are also data controllers for their employees' personal data, they have to obey data protection rules, which could be more specific in the employment context.

---

[1] In accordance with art. 40 (2) i) of the Romanian Labour Code (Law no. 53/2003 – Labour Code, republished in the OJ, Part I, no. 345 of 18.05.2011, amended and supplemented), the employer has the obligation to ensure the confidentiality of their employees' personal data. There are also some other provisions in the Code, concerning the obligation to keep confidential the salary, the special clauses of confidentiality or a separate contract on confidentiality to be concluded- these last two mentioned being optional for the parties (employer/employee).

[2] The only express obligation in this area is provided by the art. 26 (4) of the Law no. 188/1999 on the Statute of the public servants (republished in the OJ, Part I, no. 365 of 29.05.2007, amended and supplemented): "The persons who have access to the data in the national record of the public functions and public servants, and to the professional file of the public servant have to comply with the obligation of keeping confidential the personal data, according to the law."

[3] As for different types of monitoring, see also A. Sakrouge, K. Minett, D. Preiskel and J. Saras, *Monitoring Employee Communications: Data Protection and Privacy Issues*, in "Computer and Telecommunications Law Review", Issue 8, 2011, p. 213.

2. External behaviour of the employees under surveillance

Three kinds of means are mostly used in order to monitor the employees externally: electronic cards, video surveillance, and biometric data. These means may be used for one or more purposes: to monitor and control the access to the premises (devices are being installed at the entries/exits of a building, in the lobbies, at the office doors, etc.), to monitor and control the process of production or the work performance (devices are installed inside the workplace, such as closed or open spaces, halls of production, warehouses, cash desks, shops, etc.), to monitor and control the working time[4] (in this case, devices are usually being installed at the main entrances/exits of a building or of the actual workplace).

These systems of monitoring vary, whereas some employers may choose only one of them (cards/video surveillance/biometrics), and others, the whole area of means. There is also a third category, where these new IT devices are being used alongside other traditional means: a paper register for controlling the access and for checking the working hours, and people hired to perform this duty. In a fictitious example, we may imagine a workplace - a big shoe factory - where all the employers are being monitored and checked by video cameras and by using the e-cards and biometric access devices installed at the entrances/exits and by a few people having to perform such duty in the same areas; then, some other video cameras and line managers are monitoring the activity of the workers in the halls of production, even during their lunch time; other video cameras are on any passages in the premises; biometric devices are being installed at the door of every office of the administrative staff, and there are also video cameras capturing images all around inside these offices; in order to have access to the computer assigned for the daily job, this staff have to use again the e-card and a biometrics reading device.

3. Internal behaviour of the employees under surveillance

This kind of surveillance is mostly specific to workplaces where using IT equipment is part of the job. Many employers put IT resources at their employees' disposal in order to achieve their professional duties better: Internet access, electronic accounts, digital signature, electronic devices for location, etc. In the example previously provided, the administrative staff might be the beneficiaries of the first three resources; as for the location devices, these could be used, for instance, on the

[4] The Court of Justice of the European Union (CJEU) considered that a record of working time which indicates, in relation to each worker, the times when working hours begin and end, as well as the corresponding breaks and intervals, is covered by the concept of "personal data" - Order of the Court (Eighth Chamber) of 19 June 2014, *Pharmacontinente - Saúde e Higiene SA and Others v Autoridade Para As Condições do Trabalho (ACT)*, Case C-683/13 (ECLI:EU:C:2014:2028), Judgment of the Court (Third Chamber) of 30 May 2013, *Worten - Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)*, Case C-342/12 (ECLI:EU:C:2013:355).

mobile phones and/or cars of the drivers who are entitled to deliver the merchandise the shoe factory produces, in order to prevent/sanction some illegal or unfair conduct.

By specific software, the employers may monitor (in a broad, nearly anonymous or in a very insidious way) the time their employees spend on the Internet, by accessing websites or using their e-mail accounts in order to strictly do their job (get professional contacts, searching for better offers of goods and services, etc.), to have fun (chatting on a social network, playing online, etc.), or to do some other personal businesses (making doctor appointments, purchasing personal items, etc.). Also, the employers could monitor their staff use of IT equipment in order to ensure the proper functioning and security of the network and communications.

4. Data protection rules in the context of monitoring external and internal behaviour of the employees

Some people might argue that there is no private life at the workplace, which is an open or a public place, as this concept is only applicable in a close environment, specific to home and family[5]. According to this thinking, an employer would be free to survey the activity of its employees, without any restrictions.

This sort of judgment is contradicted by the European Court of Human Rights (ECHR) which stated that "There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature"[6]. The Article 29 Working Group (comprised of the representatives of the European Union data protection authorities) also retained that "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace. They do have a legitimate expectation of a certain degree of privacy in the workplace as they develop a significant part of their relationships with other human beings within the workplace.[7]"

No one can deny the legitimate interest of an employer to monitor performance of contractual duties by their employees and the achievement of performance goals set. On the other hand, every employer has to bear in mind that the employees still have individual rights, as privacy, even in a diminished proportion. This is why the decision to install and use new IT technologies in order to accomplish the above said purposes has to be the result of a fair balancing of the legitimate interest of the employer and the fundamental rights of the employees.

These general ideas are also applicable when speaking of the monitoring of employees' external or "internal" behaviour at the workplace we referred to in the

---

[5] For opinions on conceptualizing "privacy", see: D. J. Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, in "San Diego Law Review", Vol. 44, 2007, p. 745-772; L. A. Bygrave, *Privacy and Data Protection in an International Perspective*, Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010, p. 167.

[6] Judgment of 16.12.1992, case *Niemietz vs Germania* (no. 13710/88), para. 29.

[7] "Working document on the surveillance of electronic communications in the workplace", WP 55, 29.05.2002, p.4.

previous sections.

There is no doubt that by using IT means in order to monitor the employees an intrusion into their right to privacy occurs, as they would feel under scrutiny and therefore, they change or censor their usual conduct, habits, preferences; in case biometrics are used, some people could even think their dignity is under question, as collecting and storing the individual's fingerprints are usually associated with a criminal behaviour.

An interference with the right to privacy could be permitted only in accordance with the criteria established by art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms[8] and by the jurisprudence of the ECHR on the matter.

When we balance the employer's interest and the employees' right to privacy, three answers could be given, on a case by case basis: the surveillance is not allowed in any circumstances; some sort of surveillance might be permitted under specific circumstances; a combined area of surveillance means is allowed under specific, strict conditions.

Data protection rules are the key in order to make a proper analysis for getting the right answer.

First of all, any employer should make a (minimal) impact assessment, before taking the decision to have recourse to means which could prejudice the human dignity or privacy; so, only if it is absolutely necessary to achieve a specific purpose and some other non-invasive means previously used had actually failed, then the decision to use IT technologies with monitoring functions could be taken[9].

At this stage, an opinion from the national data protection authority is advisable. However, instead of monitoring personal data, an employer could give preference to preventive measures – for instance, using filters blocking the access to specific operations on the Internet.

Once the new data protection rules are adopted in the Member States of the European Union[10], data controllers shall have to make[11] an impact assessment and to

---

[8] "Art. 8 Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[9] The Article 29 Working Party in the above mentioned document (WP 55, 29.05.2002) considered that "It would only be in exceptional circumstances that the monitoring of a workers mail or Internet use would be considered necessary. For instance, monitoring of a worker's e-mail may become necessary in order to obtain confirmation or proof of certain actions on his part. Such actions would include criminal activity on the part of the worker insofar as it is necessary for the employer to defend his own interests, for example, where he is vicariously liable for the actions of the worker. These activities would also include detection of viruses and in general terms any activity carried out by the employer to guarantee the security of the system" (p. 13-14).

[10] The European Commission proposed the replacement of the current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with

consult the data protection authority prior to the processing of personal data, in certain cases.

Apart from assessing the necessity of a certain system of surveillance, an important question should be asked, namely, whether the intended processing is legitimate or not. The usual monitoring of employees' performance of the professional duties or ensuring the system security could be considered as legitimate. As a matter of principle, "the introduction and use of information systems and technologies for the direct and principal purpose[12] of monitoring employees' activity and behaviour should not be permitted"[13].

The main rule for legitimising a personal data processing regards the free and unambiguous consent of the data subject. However, in the employment context, a controller could hardly rely on the consent, given the lack of a fair balance between the employer and the employee. The Article 29 Working Party considered that "reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment."[14]

In the second stage, once established the necessity, the principle of proportionality[15] must be taken into account, by choosing those means of processing which respond to the employer's interest/purpose, but are less likely to affect individuals' privacy. In this context, a correlation should be made with the "privacy by design and by default" principle, enshrined in the future EU regulation (art 23).

---

regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31-50), with a regulation („Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"), expected to be adopted during 2016.

[11] Art. 33 (1) of the proposal: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

Art. 34 (2) of the proposal: "The controller shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk."

[12] Personal data should be collected for specific, explicit and legitimate purposes - art. 4 (1) b) of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ, Part I, no. 790 of 12.12.2001).

[13] Para. 15.5 of the Part II from the Appendix to the "Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment", adopted by the Committee of Ministers of the Council of Europe on 1 April 2015.

[14] Opinion 8/2001 on the processing of personal data in the employment context, WP 48 of 13.09.2001, p. 3.

[15] In the above mentioned WP 55/2002, the Article 29 Working Party stated that, as for the Internet and e-mails monitoring, "The proportionality principle therefore rules out blanket monitoring of individual e-mails and Internet use of all staff other than where necessary for the purpose of ensuring the security of the system" (p. 17).

Special techniques such as anonymisation, pseudonymisation and minimisation[16] of personal data to be collected and further processed may be put in place. Excessive ways of processing are prohibited[17]. For instance, "the monitoring of e-mails should, if possible, be limited to traffic data on the participants and time of a communication rather than the contents of communications if this would suffice to allay the employers concerns"[18].

Transparency is another obligation derived from data protection legislation. The employer has to inform[19] the employees, before implementing the decision of monitoring the workplace, directly or by their representatives, about each purpose of processing personal data, the categories of information to be processed, the recipients to which data might be disclosed, the rights as data subjects[20] and the conditions for the exercise of these rights. This obligation is also derived from the provisions of the Labour Code, which defend the dignity of the employees and their correct information about the working conditions, health and security.

After putting into place monitoring systems, transparency tools have to be present all the time and be adapted to the specific circumstances: representative images for video surveillance[21], regular information provided by Intranet or other visible alerts posted on the IT devices of the workers under surveillance.

All the conditions (concerning the ways of monitoring, the concrete means used for this goal, each purpose for each type of processing operations derived from it, the

---

[16] According to the art. 4 (1) c) of the Law no. 677/2001 the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

[17] The National Supervisory Authority for Personal Data Processing (NSAPDP) has not allowed the installation of video cameras inside bureaus where the employees are working, unless there are legal provisions stating otherwise (art. 8 (3) of NSAPDP Decision no. 52/2012 on the personal data processing by using means of video surveillance (OJ, Part I, no. 389 din 11.06.2012). The same act prohibits video cameras which are hidden or in very intimate spaces such as: fitting rooms, locker rooms, shower stalls, toilets.

[18] WP 55/2002, the Article 29 Working Party, p. 17.

[19] Art. 12 of the Law no. 677/2001 provides the details of the data controller's obligation to inform data subjects.

[20] In the context of data protection legislation, the most important rights to be actively exercised by a data subject are the right of access to data, the right to rectification, the right to object, and the right not to be subject to automated individual decisions (art. 13-17 of the Law no. 677/2001).

[21] As regards the video surveillance systems, the NSAPDP Decision no. 52/2012 (art. 11) provides the following:

"(1) Data controllers that process personal data using video surveillance are under the obligation to provide the information provide by art. 12 para. (1) of Law no. 677/2001, as subsequently amended and supplemented, including with regard to: a)the existence of the video surveillance system and the purpose of the processing using such means; b)the data controller's identity; c)whether the images are recorded and the categories of recipients; d)the data subjects' rights and the way in which they may be exercised.

(2)The information provided in paragraph (1) must be brought to the data subjects' attention clearly and permanently. The existence of the video surveillance system will be signalled using a representative image, sufficiently visible and positioned at a reasonable distance from the places where the video surveillance equipment is installed."

storage period, the rights of the data subjects and conditions for their exercise, measures for ensuring security and confidentiality, who has access to the records and for what purpose) have to be inserted in written documents like internal regulations or strategic policy[22].

These documents should also include, as Article 29 Working Party justly said in WP 55/2002, "details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them".

The personal data processed by means of monitoring the employees should be stored only for limited periods[23] as long as they are necessary for achieving a certain purpose, and not be further used for a purpose incompatible with the first one. After the expiration of the referred period of storage, the information shall be anonymised or destroyed/deleted.

As in the case of any data processing, adequate technical and organizational measures[24] need to be applied in order to protect the data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, notably if the respective processing involves data transmission within a network, as well as against any other form of illegal processing. Special instructions need to be given to the people entrusted with the access to the personal data processed by monitoring, according to their job description.

After the start of the processing, the employees are entitled to exercise their subjective rights in order to obtain, at reasonable intervals and without excessive delay or expenses, confirmation and information about the data and purposes of processing or the methods and techniques used during the processing (right of access[25]); in cases of incorrect or illegal processing, any employee may ask the

---

[22] In the partly dissenting opinion to the ECHR Judgment in Case of *Bărbulescu v. Romania* (application no. 61496/08) of 12.01.2016, the Judge Pinto de Albuquerque considered that "A human-rights centred approach to Internet usage in the workplace warrants a transparent internal regulatory framework, a consistent implementation policy and a proportionate enforcement strategy by employers." (para. 22)

[23] Art. 14 (1) of the Decision NSAPDP no. 52/2012 imposes a time limit of maximum 30 days for the storage of the data obtained through the use of the video surveillance system, except for the cases expressly provided by law or of well grounded cases.

[24] See Order of the Ombudsman no. 52/2002 on approving the minimum safety requirements for personal data processing (OJ, Part I, no. 383 of June 5, 2002).

[25] Art. 13 (1) of the Law no. 677/2001: " Every data subject has the right to obtain from the data controller, upon request, and free of charge, once a year, the confirmation of the fact that the data concerning him/her are or are not being processed by the data controller. The data controller, in case he has processed any personal data concerning the petitioner, is obliged to communicate to the petitioner, along with the confirmation, at least the following: a) information regarding the purposes of the data processing, the categories of data concerned, and the recipients or the categories of recipients to whom the data are to be disclosed; b) communication in an intelligible form of the processed data and of any other available information regarding the source of origin of the respective data; c) information on the technical principles and mechanisms involved in the data processing concerning that data subject; d) information concerning the existence of the right of intervention upon the data, and the right to object, as well as the conditions in which the data subject can exert these rights; e) information on the

deletion, rectification, updating, anonymization of data or blocking of the processing (right of intervention[26]); if a person alleges justified and legitimate reasons linked to his/her particular situation, he/she may object to that processing (right to object[27]); the employee may ask the employer to revoke or annul a decision based solely on automated processing made by means aimed at assessing some aspects of his/her personality, such as professional competence, credibility, behavior or any other similar aspects[28]. The controller is obliged to answer within 15 days to the data subjects' requests. In case of violation of these rights a complaint to the data protection authority may be submitted.

In accordance with Law 677/2001, the processing operations must be notified in advance to the data protection authority unless there are some exceptions applicable. In 2006 NSAPDP[29] provided a general exemption from the duty to notify the processing of personal data of the employees and external co-workers, which is carried out by public and private law entities in order to fulfill their legal obligations.

Presently, there is a number of situations when data controllers could be obliged to notify the processing to NSAPDP, in the context of using IT technologies at the workplace where: the processing takes place by using video surveillance means[30]; biometric or genetic data are being processed[31]; the processing of data allows, directly or indirectly, geolocalization of individuals by means of electronic communication[32]; the processing is made by using electronic means, for the purpose of assessing personality traits, as well as the professional competence, credibility, behaviour[33], or

---

possibility of consulting the Register of personal data processing, stated under Article 24, before submitting a complaint to the supervisory authority, as well as to dispute the data controller's decisions in court, according to the provisions of this law".

[26] Art. 14 (1) of the Law no. 677/2001: " Every data subject has the right to obtain from the data controller, upon request, and free of any charge: a) as the case may be, rectification, updating, blocking or deletion of data whose processing does not comply with the provisions of the present law, notably of incomplete or inaccurate data; b) as the case may be, transforming into anonymous data the data whose processing does not comply with the provisions of the present law; c) notification to a third party to whom the data were disclosed, of any operation performed according to letters a) or b), unless such notification does not prove to be impossible or if it does not involve a disproportionate effort towards the legitimate interest that might thus be violated."

[27] However, a legal provision imposing a certain processing precludes the right to object (art. 15 (1) of the Law no 677/2001).

[28] Some exceptions are provided by art. 17 (2) of the Law no. 677/2001, concerning the protection of the legitimate interests of the data subjects.

[29] Art. 1 b) of the NSAPDP Decision no. 90/2006 on the situations in which the notification for personal data processing is not required (OJ, Part I, no. 654 of 28.07.2006)

[30] Art. 15 of NSAPDP Decision no. 52/2012

[31] Art. 1 b) of the NSAPDP Decision no. 200/2015 on the situations in which the notification for personal data processing is not required and amending and revoking a number of decisions (OJ, Part I, no. 969 of 28.12.2015)

[32] Art. 1 c) of the NSAPDP Decision no. 200/2015

[33] Many employers or recruiting agencies make an assessment of the profile of a future employee even by surveying the information shared by them on social media like Facebook or LinkedIn (see http://www.wall-street.ro/articol/Companii/165297/ai-grija-ce-postezi-pe-facebook-jumatate-dintre-

other similar aspects[34]; the processing is made by private entities, through electronic means, for the purpose of adopting individual automatic decisions in connection with analysing the solvability, the economic and financial situation, of the facts likely to entail the disciplinary, contravention, or criminal liability of the individuals[35].

All the notifications registered by NSAPDP are publicly available online on its website, so every individual interested may determine whether his/her employer deploys a system of monitoring, for what purposes, which personal information is being processed, for what period of time, and the conditions for exercising his/her rights. After consulting the public registry, any employee may choose to file a formal complaint to the data protection authority in order to have the legality of his/her employer's monitoring system checked.

Any processing of the employees' personal data by using IT technologies which is carried out under illegal conditions may be subject to the control carried out by NSAPDP; according to the findings, the controller could be fined and the processing stopped[36].

5. Conclusions

Based on the legal provisions, corroborated with the practice of the national supervisory authorities in the EU, the case law of the CJEU and ECHR, a few principles may be retained, as regards the processing of the employees' personal data by IT systems of monitoring at the workplace: the workers have a legitimate expectation of privacy at the workplace, which has to be put in balance with the employer's legitimate interest in surveillance measures, by taking into account the necessity, proportionality and legitimacy of these measures, the need to ensure transparency before and during the processing, and to establish mechanisms for a proper exercise of the rights by the employees, the importance of taking adequate confidentiality and security measures. In addition, the previous consultation of the data protection authority may prevent the later sanctioning of the employer for illegitimate processing.

Finally, as to the importance of regulating specific safeguards for the dignity and fundamental rights of the workers when systems of monitoring are in place, the new EU (future) regulation on data protection will have a whole article dedicated to processing in the employment context.

---

angajatori-iti-verifica-profilul-la-angajare.html, last accessed on 14.04.2016).
For a comparative study between American and European systems of monitoring, see S. Wallach, *The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy*, in "The International Journal of Comparative Labour Law and Industrial Relations", Kluwer Law International, 2011, p. 189-219.

[34] Art. 1 e) of the NSAPDP Decision no. 200/2015

[35] Art. 1 f) of the NSAPDP Decision no. 200/2015

[36] In a case, a local tax authority was fined because it had illegally monitored its employees by electronic means aimed at assessing employees' productivity (see http://www.dataprotection .ro/index.jsp?page=DVBLS2&lang=ro, last accessed on 14.04.2016).

Bibliography:

1. L. A. Bygrave, *Privacy and Data Protection in an International Perspective*, Stockholm Institute for Scandinavian Law & Lee A Bygrave, 2010.
2. A. Sakrouge, K. Minett, D. Preiskel and J. Saras, *Monitoring Employee Communications: Data Protection and Privacy Issues*, in "Computer and Telecommunications Law Review", Issue 8, 2011.
3. D. J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, in "San Diego Law Review", Vol. 44, 2007.
4. S. Wallach, *The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy*, in "The International Journal of Comparative Labour Law And Industrial Relations", Kluwer Law International, 2011.