FACTA UNIVERSITATIS
Series: **Law and Politics** Vol. 11, N°3, 2013, pp. 121 - 133

Review Article

INTERNATIONAL STANDARDS ON THE PROTECTION OF EMPLOYEES' RIGHTS TO PRIVACY *

UDC 349.2(100):342.738

Ivan Barun

Faculty of Economics, University of Niš, Serbia

Abstract. *The author addresses the issues and challenges related to the protection of employees' rights to privacy in the modern information society. The use of information and communication technologies (ICT) in the workplace facilitates the collection, storage and processing of employees and job applicants' personal data, thus contributing to business efficiency, but it also facilitates various violations of privacy of employees and employers alike. In this article, the author analyzes some aspects of employees' right to privacy as envisaged in the international law instruments. The analysis is aimed at examining the methods and instruments for the collection and protection of personal data, as well as the procedure in case of any violation of privacy rights. In that context, the author particularly focuses on the issues pertaining to the supervision of employees' business correspondence, video surveillance in the workplace, monitoring employees through performance tests, etc. The author believes that prospective solutions in the legislation of the Republic of Serbia may be based on and perceived through the most important international sources in the field of protecting employees' privacy rights.*

Key words: *privacy; employees; personal data; supervision; employment.*

1. INTRODUCTION

The Right to Privacy was originally developed as a human right within the framework of the Right to Dignity. Given the fact that employment is one of the most important parts of every person's life, employees' dignity is the cornerstone for developing the social welfare state [1].

Received August 29, 2013/Accepted November 29, 2013
Corresponding author: Ivan Barun, LL.B., PhD Student,
Faculty of Law, Trg kralja Aleksandra 11, 18 000 Niš, Serbia
Tel: +381637792642 • E-mail: barun_barun86@yahoo.com
* This paper is a result of participation in the project "*Protection of Human and Minority Rights within the European Legal Area*", which has been carried out by the Faculty of Law, University of Niš.

The European Convention of the Council of Europe on Human Rights and Fundamental Freedoms of 1950 is one of the first International Law documents which set out the foundations for the Right to Privacy. Article 8 (Right to Respect for Private and Family Life) states that "everyone has the right to respect for one's private and family life, privacy of one's home and correspondence." The definition of the Right to Privacy was framed within the activities of the European Council [2] and it has been accepted by most authors in the field of Labor Law. Under this definition, the Right to Privacy implies the right of individuals to live their own lives with as little external influence as possible, including numerous fields of Privacy Policy.

Employees' Right to Privacy implies a set of personal authorities that guarantee Respect for their Persona, Honor and Reputation [3]. The most important aspect of this issue is what kind of personal data employers are entitled to collect about employees (and prospective job candidates) and how they can process and use the data, whether the collected data may be specified as one of the special employment requirements and whether such data may be used as the grounds for the termination of employment or disciplinary action.

Another area of considerable importance pertains to the possible means of employer's supervision over the employees, both in the workplace (during the working hours) and in employees' free time. The employer's supervision can be organized in many ways, by installing equipment for monitoring and controlling employees' business correspondence. An employee's Privacy Right can be violated if an employee or a job candidate is inadvertently subdued to various tests (aimed at evaluating one's physical, physiological and intellectual abilities).

The procedural aspects governing the issue of Employees' Privacy Protection come into play in case of any violation of the rights guaranteed by labor legislation. The effective protection system is an important prerequisite in achieving good results in the highly sensitive area governing the Protection of Human Rights.

The statutory regulation of this issue is governed by a number of factors which must be taken into consideration when reaching a compromise between the competing interests of employers and employees. While the former tend to expand the scope of data collected in the process of establishing employability and in the course of employment, the latter demand more effective protection of Privacy Rights.

The inspiration for developing the national legislation in this area may be found in numerous International Law documents dealing with Employees' Privacy Rights [4]. The proposed solution should include unambiguous rules, drawing a clear line between the permissible and impermissible practices, whereas the exclusion rules should be formulated in such a manner that they leave very narrow margin for arbitrary interpretation.

2. INTERNATIONAL STANDARDS

The contemporary Labor Law is facing another challenge in regulating the issues pertaining to the Protection of Employees' Privacy Rights in the workplace. The development of information technologies and technical means of controlling space and people, easier collection and storage of personal data and the development of biometric and genetic testing, as well as testing on certain illegal drugs, have given rise to the need to adopt legislation which would provide relevant protection for both employees and employers.

The degree and the manner of exercising of Employees' Privacy Protection Rights show no uniformity of practice even in the developed countries founded on the liberal legal tradition. However, the differences are more dramatic when the developed countries are compared with the transition countries, for example.

The United States, as a typical proponent of the liberal legal thought, developed a market-based approach to employment policy. In regulating the competing interests concerning the requirements for the Protection of Employer's Property or the need to respect the Employees' Privacy Rights, the USA favors the interests of the employer and puts them in a privileged position when adopting regulations in this area.

The EU Member States (except for the United Kingdom) have a different approach which favors the requirements for the Protection of Human Dignity and Autonomy. As a result, there is more restrictive legislation on the employer's right to supervise the employees. A comparative study of the legal systems of the European-Continental and the common law systems [5] has shown that the degree of Employees' Privacy Protection is much higher in the civil law countries (especially in the EU countries) whereas the US legislation contains some legal provisions recognizing a certain degree of employer's intrusion into the employee's privacy; on the other hand, in the countries such as Australia and the United Kingdom, there are no statutory provisions prohibiting such conduct of the employer.

2.1. General overview of foreign legislations

There are numerous International Law documents related to Privacy Issues in the workplace which clearly reflect the development and the scope of Privacy Right Protection. Although there is a fair degree of similarity in the legal solutions found in the documents adopted at the regional and universal level, there are also some discrepancies, particularly in terms of the obligations envisaged in these documents and the standardization of personal data from the private life of an employee who is being protected.

The European Convention of the Council of Europe on Human Rights and Fundamental Freedoms of 1950, which was signed by all EU states, states in Article 8 (Right to Respect for Private and Family Life) that "... everyone has the right to respect for private and family life, privacy of their home and their correspondence". In the case *Niemitz v. Germany*, the European Court of Human Rights concludes that the Right to Respect Privacy also extends to "professional and business activities." [6] The Court also found that the inviolability of correspondence was also related to telephone communication, both private and business, and that the use of the Internet and email should be subject to Protection as well [7].

The Charter of Fundamental Rights of the European Union (Article 7) refers to the provision included in the European Convention of the Council of Europe (Art. 8), which stipulates the Right to Privacy as one of the fundamental social rights which has been protected in the EU legislation since 1950. Although the field of Privacy Rights largely remains the responsibility of the EU Member States, there are certain instruments at the EU level, such as the Directive on the Protection of Individuals with regards to the processing of personal data and the free movement of these data [8], as well as the Directive concerning the Processing of Personal Data and the Protection of Privacy in the sector of telecommunications [9].

It may come as a surprise that the concept of Right to Privacy was not explicitly mentioned in the original text of the US Constitution. However, the Fourth Amendment of the US Constitution guarantees the Right to Privacy of an individual in terms of the obligation of public authorities to provide for the respect of one's private life and security in one's homes, business papers and effects. Be as it may, neither the Constitution nor its Amendments refer to employees' privacy protection issues, particularly in light of new technological developments.

Unlike European countries which constantly endeavor to regulate newly emerging threats to privacy both at the national and at the EU level, in the United States there is no legislation in this area and the regulation of these issues largely depends on the case law (judicial precedents).

These differences in the approach to addressing the issue of Employees' Privacy Rights Protection arise from the fact that EU Member States basically tend to get involved in resolving the conflict between the employer's desire to increase surveillance and the employees' aspirations to reduce the level of supervision. On the other hand, the social partners in the USA assert that the State (i.e. the Government) should interfere as little as possible in resolving their mutual employment-related issues, including Employees' Privacy in the workplace [10].

At the international level, the most important legal documents have been adopted within the activities of the International Labour Organization (ILO) and the Organization for Economic Cooperation and Development (OECD) [11]. The main feature and probably the major disadvantage of these instruments is that they are not binding for the State Parties, even though they may have a significant impact on the legislation of States which have signed these international documents.

2.2. The US regulation on employees' right to privacy

In order to fully understand the current legal framework of Employees' Right to Privacy in the United States, we shall look into the attitude of numerous authors on the approach to regulating Employment and Labor Law in the United States in general. Many authors point out that the economic theory of *laissez-faire* and the private-entities-oriented approach to understanding the Employment Contract are deeply embedded in the approach and principles governing labor relations in the United States. Considering the legal nature of contractual relationship in Private Law as well as the rights and obligations arising from employment, they insist that employment should only be regulated by employees and employers alone, with minimal interference from the state, either through legislation or by means of collective bargaining agreements and internal codes of practice [12].

It can be said that the USA has made no efforts to standardize the newly emerging circumstances resulting from the IT development into a single legal act regulating privacy in the workplace. Instead, the US has resorted to enacting a number of documents which only partially regulate this area (such as: the "Constitutional Guarantees", statutes, case law) or resolving these issues in individual employment contracts.

Individual Privacy Protection is envisaged in the Fourth Amendment of the U.S. Constitution, which states that "... everyone has the right to enjoy the security of their home, their letters and personality "and that this amendment provides protection when there is a "reasonable expectation of privacy". As previously stated, such a wording can be the basis

for the Protection of Employees' Privacy Rights only in the public sector but the courts are reluctant to grant protection to employees even in cases of violation of privacy by the state as an employer. [13].

Taking into consideration the growing number of court proceedings related to alleged violations of the Employees' Privacy Right and the existing legislation on Employees' Protection in the workplace, the US Congress adopted the Electronic Communications Privacy Act [14] in 1986. In order to reduce the apparent discrepancy between the existing legislation and the judicial practice, this Act prohibits unauthorized monitoring of electronic mail and other communications by phone or the Internet.

Yet, the Act provides three exceptions when the prohibition does not apply. Hence, the Act shall not apply: when the interception of communication channels enables communication in order to improve the quality of the communication service; when consent is given by the person whose communications are monitored; and when activities of interception and eavesdropping are carried out "in the ordinary course of business."

In practice, the provision allowing the employers to monitor the employees' activities "in the ordinary course of business" as well as the consequences stemming from the application of this Act and the Fourth Amendment of the US Constitution clearly indicate that employers are favoured and that they are left a wide leeway in the interpretation of this legal standard. All the constitutions of individual American states also contain provisions similar to the one contained in the Fourth Amendment; however, all these provisions envisage the protection of Employees' Right to Privacy only in the public sector. The only exception is the State of California where the courts have interpreted this provision in such a way as to afford protection to employees in the private sector as well [15].

Despite the apparent favoring of the employer's position, the number of private lawsuits filed by employees is on the rise. The employees mainly complain about the employer's violation of their privacy rights.

Case law shows that it is not impossible to win this kind of lawsuit and claim damages. But, for that to happen, the the plaintiff must prove that there was a significant invasion of privacy, and that such interference has given rise to some consequences that have further resulted in damage to the employee [16]. The implementation of various tests conducted by employers in the workplace is an interesting area where case law protects the Employees' Rights to Privacy. The Supreme Court of West Virginia found [17] that drug testing of employees is an unauthorized invasion of Employees' Privacy unless there is a "... reasonable and objective suspicion that the employee has abused narcotics ...", even though there is no clear interpretation of the standard of "reasonable and objective suspicion" and whether "...the employee works on jobs related to public safety or the safety of others." In the process of negotiating an employment, the Court considers that in cases involving drug testing privacy also deserves protection but to a lesser extent than in cases where the working relationship already exists [18]. Generally, polygraph testing is prohibited by the US Employees' Polygraph Protection Act [19] of 1988. Employees cannot be subjected to a polygraph testing against their will, except when they have jobs related to automobile safety, operations and maintenance of alarm systems and safety matters related to the manufacture, distribution, disposal and destruction of pharmaceutical materials.

2.3. The European Union standards

In regulating the issues related to Employees' Privacy, the states of the Continental European legal system opted for a fairly comprehensive, systematic and, above all, progressive approach. The Employees' Privacy issue is, for the most part, still under the jurisdiction of the EU Member States even though there are important documents at the EU level pertaining to these powers. By analyzing some national legislation and other regulations on Privacy in general, including Privacy in the Workplace, one can conclude that they are based on some common principles, which set out further guidelines for defining the concept of protection.

- *The Principle of Relevance* (i.e. the principle of cause) concerns the objective justification for the employer's intrusion into the employee's privacy, especially in terms of electronic communication channels. Thus, an employer may be allowed to monitor an employee's communications via the Internet and e-mail only if it is necessary and directly related to the employee's status and job responsibilities.
- *The Principle of Proportionality* implies that the monitoring of employees must be necessary, relevant and proportionate to the objectives that the employer is trying to achieve. The manner and the extent of surveillance must reflect a compromise between the competing interests of employees and employers.
- *The Principle of Transparency* is specifically reflected in the employer's obligation to notify the employee representatives about the intention to set up a monitoring system or to start tracking the official correspondence channels. In that context, the employer should carry out the necessary consultations with employees to make them aware of the fact that their privacy will be limited by the employer, in accordance with the law.
- *The Principle of Non-discrimination* implies that all employees must be subject to the same supervision measures and that there will be no discrimination among workers or groups of workers. Hence, supervision must be applied to all employees, regardless of their position in the organizational structure [20].

In the European Legal Area, the sources of law pertaining to employers' privacy include the sources stemming from the activities of the European Council and the sources of the EU Law (*acquis communautaire).* It is worth noting here that these sources are not substantially different and, in many cases, they even refer to each other in terms of their application.

The first instance in the development of the Right to Privacy is the European Convention of the Council of Europe on Human Rights and Fundamental Freedoms (1950), which guarantees the right to respect for private and family life (Article 8), which is interpreted as being related to both professional and business activities and communications of the employees, including e-mail and the use of the Internet. This provision of the European Convention is reaffirmed in the EU Charter of Fundamental Rights (2002), where the Employees' Right to Privacy is given the status of a basic social right in the EU.

The Council of Europe has been working on the promotion of the Right to Privacy as a Fundamental Human Right. As a result, in 1981, the Council of Europe adopted the Convention on the Protection of Individuals with regards to Automatic Processing of Personal Data, which was signed by all EU Member States and Norway. In line with the Convention objectives concerning the matters of Employment and Contractual Obligations, the Committee of Ministers of the European Council adopted the 1989 Recommen-

dation (R(89)2) on the Protection of Personal Data used for employment purposes, with regard to automatic processing of personal data. As the use of information technologies significantly advances in employer-employees relations, this Recommendation is to reduce the risk of invasion of privacy, which is inevitable due to such tendencies.

The most important document in the EU legislation in this area is certainly the Directive (95/46/EC) on the Protection of an Individual regarding the processing of personal data and on the free movement thereof, jointly adopted by the European Parliament and the European Council. The aim of this Directive is "... to protect the rights and freedoms of individuals, notably the Right to Privacy with regard to the processing of personal data in the EU Member States." It also specifies that "... Member States shall not restrict or prohibit the free flow of personal data between Member States for reasons connected with the protection which the Directive provides." The provisions of this Directive are legally binding for EU Member States, which were instructed to implement this document in their National Legislations by October 1998 [21].

As for the Protection of Personal Data, the Directive includes standards relating to data collection, as well as to the volume of data that can be collected in connection with employment. For instance, Article 6 of the Directive states that data must be:

- processed fairly and lawfully;
- collected for explicitly specified and legitimate purposes, and shall not be further processed in a way which is incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected, and shall not intrude into the privacy more than it is necessary;
- accurate and, where necessary, even updated in order to ensure that inaccurate or incomplete date are erased or rectified;
- stored in a form that allows for the identification and use of such data in a manner that allows its use only for no longer than it is necessary for specific purposes.

Article 7 of the Directive pertains to cases where the collection of employees' personal data shall be considered legitimate and legal. Thus, personal data may be collected and processed only if:

- a person whose data are collected has given his/her unambiguous consent, or
- the data processing is necessary for the performance of obligations assumed under the employment contract, where one of the Contracting Parties is the person whose data is being collected, or if it is necessary for entering into an employment contract, or
- the data processing is important to the person who collects the data in order to fulfill their legal obligation to collect such data, or
- the data processing is necessary in order to protect the interests of the person whose data are being collected, or
- the data processing is conducted in the public interest or in the exercise of an official authority of the person vested with the power to collect data, or if such powers are vested in a third party, or
- the data processing is necessary to pursue the legitimate interests of the person who has the authority to collect such data, or a third party authorized by the original holder of the authority to collect the data, except in cases where such data collection would be regarded as a violation of the fundamental rights and freedoms of persons whose data have been collected.

The Directive applies to the employees' most sensitive personal data whose processing is strictly prohibited. The sensitive data refer to racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership and/or data concerning health or sexual orientation. The processing of data related to penalties, criminal sanctions or security measures imposed in court proceedings, which are also considered particularly sensitive, is permitted only under the supervision of and in cooperation with the competent authorities. Exceptions to these rules may apply to investigative journalism or artistic and literary study purposes [22].

A person whose data are collected and processed must be timely informed, and he/she must have access to the collected data. A person is entitled to challenge the processing of such data for legitimate reasons and may request corrections if the data is incorrect or not updated. The person who is responsible for the processing of such data must ensure their safe-keeping and storage, which implies that no unauthorized person may have access to such data.

The Directive (97/66/ES), related to the Processing of Personal Data and the Protection of Privacy in the telecommunications sector, was adopted in 1997 as a response to the introduction of advanced information technology in the operation of public telecommunication networks. In July 2002, this Directive was made ineffective due to the adoption of the Directive (2002/58/ES) related to the Processing of Personal Data and the Protection of Privacy in the electronic communications sector. The fact that one Directive was replaced by another in such a brief period of five years indicates the tendency of the EU leaders to monitor the rapid development of information technology and provide relevant legal framework in Employees' Privacy Rights Protection.

At the beginning of the new millennium, the European Commission conducted several rounds of consultations with social partners, trade union representatives and employers' associations at the European level in order to lay grounds for a further development of legislation in this area. In the first round, in 2001, the consultation were held on whether the European Union should take part in the regulation of privacy issues in the field of collecting data on the employees' health status, testing the employees in the workplace for the presence of opiates and alcohol, as well as in the field of video and audio surveillance in the workplace.

The employers took a clear position that the EU should not expand the legislation in this area, considering that the Directive (95/46/EC) regulates this area in a sufficient and suitable manner; on the other hand, the employees' unions considered that new rules should be adopted, with clear instructions on handling the processing of personal data.

The second round of consultations was expected to result in more specific conclusions, aimed at formulating a draft of a new document on this issue. However, as the representatives of the social partners could not agree on the key points, the European Commission started drafting a new Directive without the involvement of the social partners. The new directive has not been adopted yet.

2.4. Australian legislation

The principle governing the Employees' Right to Privacy in Australia may be said to be more similar to the principle accepted in the United States than to the principle accepted by the states of the European-Continental legal system. The factors giving rise to

considerable difficulty in regulating this issue are the absence of constitutional guarantees on the Right to Privacy as well as rather scanty legislation and case law in this area. In practice, employers enjoy a preferential treatment in cases involving employees' privacy in the workplace.

Many Australian states have a number of legislative acts pertaining to the Privacy of Personal Information, such as: the 2001 Information Privacy Act [23] of the State of Victoria, the 2001 Listening Devices (Miscellaneous) Amendment Act [24] of South Australia, or the 1998 Surveillance Devices Act [25] of Western Australia; however, all of them are partly related to Employees' Privacy in the Workplace). New South Wales is the only state that has an act which exclusively regulates the Privacy of Employees [26].

The 1998 Workplace Video Surveillance Act [27] of New South Wales establishes the procedural requirements which must be met in order to consider the supervision over the employees lawful. Thus, video surveillance will be considered unlawful unless the employees have previously been informed of supervision at least 14 days before the start of surveillance, cameras were installed at prominent locations and information on the rooms where the monitoring is being carried out are clearly marked at their entrance (Article 4).

In 2000, the Government of the Commonwealth adopted the federal Privacy Amendment (Private Sector) Act [28] to the 1988 Privacy Act [29], by means of which the effect of this legislative act has been extended to private sector employees. The Act established the National Privacy Principles (NPPs) governing the collection, use and availability of personal data traffic.

After the adoption of the 2000 Privacy Amendment Act, employers in both the public and the private sector have been obliged to respect the 10 principles formulated in the NPPs, except when they are bound by the Privacy Code approved by the Federal Privacy Commissioner [30].

The personal data shall not be used without one's consent and for purposes other than those they have been collected for. The person in charge of collecting the data must ensure their accuracy, proper storage and preservation. The persons whose data are collected must have access to data and must be given a chance to change outdated and delete incorrect data [31].

The Privacy Act states that the collection of particularly sensitive data, which includes data on ethnic origin, political views, sexual orientation (etc.) will be allowed only upon securing an express consent of the person whose data are collected (provided that there is express statutory authorization), as well as in case that such collection is necessary to prevent a serious and imminent threat to one's life or health (even if the person whose data are collected is unable to give consent).

The main controversy related to this Act is section 7B, pertaining to the "Employee's Record" [32]. The Act allows employers and employees to regulate the issues pertaining to personal data from "Employee's Record" in employment contracts. This solution has been repeatedly criticized both at the federal and the state level, as well as by the Reform Legislation Committee, the Privacy Commissioner, representatives of trade unions and academia. However, the public debate on this issue has not yet resulted in amending this Act.

The current legal regime governing the Protection of Privacy in Australia is in the early stages of its development. Regulatory bodies and authorities responsible for the enforcement of regulations must make significant efforts to respond to the immediate threats posed by the rapid development of new technologies and the need to establish a coherent,

comprehensive and long-term approach to solving the problem of employees' privacy protection [33].

3. CONCLUSION

The use of ICT in the workplace contributes to business efficiency and enables easier collection, storage and processing of personal data of employees and employment candidates. However, it also implies a possibility of various violations of employees and employers' privacy. The issues and challenges related to the Protection of Employees' Rights to Privacy in the modern information society have been tackled by legislators and employment law scholars throughout the world. These issues are primarily related to the collection and protection of personal data and the procedure in case of violation of privacy rights but they also refer to the supervision over the employees in terms of having an insight into the nature of employees' business correspondence, video surveillance in the workplace, monitoring employees through performance tests, etc.

The employers' act of collecting information about their employees is not a problem *per se*, if conducted for legitimate and relevant purposes, because it is the basis of the employer-employee relation stipulated in the employment contract. The employer is entitled to collect relevant data about the employee in the manner and to the extent deemed reasonable and necessary, and to store them for decades (if necessary); for example, such data may include basic personal data about the employed person, the date of birth, information on qualifications and work experience, knowledge/performance tests (e.g. the Bar Exam for those working in the judicial system) or some aptitude tests (e.g. general and detailed medical examination for pilots).

In recent years, the rapid development of modern technology has facilitated the collection of information about the employees, made it faster and cheaper; however, it also enabled the employers to collect personal data without informing the employees about the nature and the prospective use of the collected data. There is a reasonable concern about the possible intrusion or interference into the employee's private sphere. In order to provide for proper protection of the right to privacy as a fundamental human right, it is necessary to draw a clear line between the lawful and unlawful employer behavior which constitutes a violation of employees' privacy.

However, given the fact that the legislative process often results in making different compromises in diverse spheres of interest, rarely can one find legal solutions specifying what kind of data may be collected, what kind of communication channels may be used and what kind of tests may be applied in the employment contexts.

National legislations are more likely to contain general solutions that guarantee a comprehensive protection of the rights to privacy, citing a number of exceptions to this rule, which are commonly subject to different interpretation in practice [34]. Such general clauses may be found in the Serbian legislation as well. In light of the most important international sources on Employees' Privacy and applicable comparative law in this area, we may conclude that the Republic of Serbia meets the standards envisaged in the legislations of neighboring countries and the EU Member States.

Yet, the existing Serbian case law and the prospective assessment which is to be carried out in the process of Serbia's accession to the European Union will inevitably show

whether the applicable legal provisions are fairly well-formulated and appropriately applied in practice, whether they achieve the anticipated goals regarding the scope of privacy protection in the workplace, and whether they contribute to creating an acceptable and productive work environment.

Given the current circumstances in Serbia, there are assertions that the Employees' Rights to Privacy is not a burning social issue, for there are other significant unresolved political and legal issues which have to be addressed more urgently. Although the author may generally agree with such a statement, it is important to note that an employee's privacy right may be violated only if one is employed. Given the fact that employment opportunities have been significantly reduced in the past period and that the employment circumstances are hardly likely to change in the years ahead, the unemployed people are prone to put up with privacy invasion practices just in order to get or to keep a job. Such circumstances give rise to various violations of employees' rights, primarily the right to a minimum wage, pension, disability support and health insurance but also violations of the right to privacy resulting from the collection of personal data on health status, subjecting the employee to various tests whose results are later used as reasons for the termination of employment, pregnancy test for females before signing the employment contract, as well as physical and sexual abuse in the workplace.

Given the fact that such practices increase the scope of violations, that the employment opportunities are significantly reduced and that individuals whose rights have been violated are unable to opt for other jobs due to economic hardship, the state authorities should give due attention to the employees' right to privacy.

Therefore, the development of relevant legislation in this area is inevitable. The rapid development of ICT gives rise to new solutions and opportunities. In such circumstances, law (as a social discipline) can hardly keep up with the ICT developments and it will always be one step behind the new technology. Thus, the risk of abuse is omnipresent [35]. In that context, instead of lagging behind for decades, law-makers should strive to remain just one step behind the technological developments, particularly given the fact that in a modern society a span of a decade is comparable to a distance expressed in light years.

The solution may be found in adopting more flexible regulations, which could be easily changed and adjusted (if necessary). The key solution to the Employees' Privacy issues may be lying in the flexibility of Labor Law. On the one hand, it is necessary to ensure a good team to represent the employees' interests in decision-making processes, to consult them in the process and to abide by the employees' proposals. On the other hand, it is essential to strengthen state institutions which are to supervise the application of these flexible regulations and to ensure an effective system of judicial protection, where the burden of proof will rest on the employer rather than on the employee (as a weaker party), as it is currently the case.

REFERENCES

1. R. Brković, "Prohibition of Competition to the Employer and the Dignity of the Workers," Labor and Social Law-Journal for the Theory and Practice of Labor and Social Rights, Belgrade, No. 1/2008, p. 250.
2. Resolution No. 428 (1970), containing a Declaration on Mass Communication Media and Human Rights, Section C, Article 2.

3. P. Jovanović, "The Moral Integrity of Employees and their Legal Working Framework," Labor and Social Law -Journal for the Theory and Practice of Labor and Social Rights, Belgrade, 2011, p. 88.
4. The international regulation on of Employees Privacy Protection is quite extensive. Here is a list of the most important documents that meet the international standards: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981; Directive 95/46/EC of the European Parliament and of the Council from October 24th 1995 on Protection of Individuals with regard to the processing of personal data and the free movement of such data. For more information on the communitarian and non-communitarian sources, see in: B. Lubarda, European Labor Law, CID, Podgorica, 2004, p. 268-269; S. Jašarević, "Protection of Personal Data on Employees in the European and Serbian Law," Legal Life No. 12/2008, p. 459-471); International Labor Organization: Protection of workers' personal data. An ILO code of practice, International Labor Office, Geneva 1997; Recommendation R (89) 2 concerning the Protection of Personal Data used for employment purposes (adopted by the Committee of Ministers on 18 January 1989).
5. J.D.R. Craig, Privacy and Employment Law, Oxford/Portland, Oregon: Hart Publishing, 1999, p. 355-356.
6. Niemitz V. Germany, Series A N0 251/B § 30, ECHR December 16th 1992.
7. R. Blanpain and M. van Gestel, Use and Monitoring of E-mail, Internet and Internet Facilities at Work, Kluwer Law International, 2004, p. 150-151; 268-269.
8. 95/46/EC
9. 97/66/EC
10. S. Wallach, "Who's Info is it Anyway? Employees' Rights to Privacy and Protection of Personal Data in the Workplace", International Journal of Comparative Labor Law and Industrial Relations, Kluwer Law International BV, The Netherlands, 2007, Vol. 23 Iss. 2, p. 220.
11. ILO: International Labor Organization, Protection of workers' personal data. An ILO code of practice, International Labor Office, Geneva 1997; Recommendation No. R (89) 2 concerning the protection of personal data used for employment purposes (adopted by the Committee of Ministers on 18th January 1989); OECD: Guidelines on the protection of privacy and Trans-border flow of Personal Data c(80)58 (final).
12. See: M.W. Finkin, Information Technology and Workers' Privacy: A Comparative Study: Part IV: The Comparative Historical and Philosophical Context: Menschenbild: The Conception of the Employee as a Person in Western Law, CLLPJ, Vol. 23, p. 579-580; J.D.R. Craig, opt.cit. p. 41 and more
13. National Working Institute, Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection, 2000, p. 6.
14. Electronic Communication Privacy Act of 1986 (ECPA), Pub. L. No. 99-508.
15. See: K.A. Jenero and L.D. Mapes-Riordan, Electronic Relations Law Journal, Vol. 18, 1992, p. 80; Hill v. National Collegiate Athletic Association, 865 P.2d 633 (Cal. 1994).
16. See: O'Connor v. Ortega, 480 U.S. 709 (1987); Watkins v. United Parcel Service INC, 797 F. Supp. 1349 (1992).
17. Twigg v. Hercules Corporation, 406 S.E.2d 52 (1990).
18. Baughman v. Wal-Mart Stores INC, No. 31312 (2003).
19. Employee Polygraph Protection Act of 1988, USA.
20. C. Delbar, M. Mormont and M. Schots, New technology and respect for privacy at the workplace, Comparative Study, Institut des Sciences du Travail, 2003 (online publication: www.eurofound.europa.eu).
21. A. O'Rourke, A. Pyman and J. Teicher, "The Right to Privacy and the Conceptualisation of the Person in the Workplace: A Comparative Examination of EU, US and Australian Approaches, *The International Journal of Comparative Labor Law and Industrial Relations*, Kluwer Law International BV, The Netherlands, 2007, Vol. 23 Iss. 2, p. 221.
22. C. Delbar, M. Mormont and M. Schots, op.cit.
23. Victoria, Information Privacy Act, No. 98, 2000.
24. South Australia, Listening Devices (Miscellaneous) Amendment Act, No. 15, 2001.
25. Western Australia, Surveillance Devices Act, No.56, 1998.
26. A. O'Rourke, A. Pyman and J. Teicher, op. cit. p. 186.
27. New South Wales, Workplace Video Surveillance Act, No. 52, 1998.
28. Privacy Amendment (Private Sector) Act, No. 155, 2000.
29. Privacy Act, No. 119, 1988.
30. Ibid, ss 6, 18BB, and Sch 3.
31. R. Owens and J. Riley, The Law of Work, *Oxford University Press*, 2007, p. 447.
32. A. O'Rourke, A. Pyman and J. Teicher, op. cit. p. 186.
33. Ibid, p. 186.

34. Lj. Kovačević, „Collection and use of personal data as a labor law issue", Labor and Social Law - Journal for the Theory and Practice of Labor and Social Rights, Belgrade 2011, p. 62.
35. S. Wallach, op. cit. p. 210.

MEĐUNARODNI STANDARDI U OBLASTI ZAŠTITE PRAVA NA PRIVATNOST ZAPOSLENIH

U ovom radu autor se bavi pitanjima i izazovima vezanim za zaštitu prava zaposlenih na privatnost u modernom informatičkom društvu. Upotreba komunikacionih i informacionih tehnologija na radnom mestu omogućava olakšano sakupljanje, skladištenje i obradu podataka o ličnosti zaposlenih, kao i kandidata za zaposlenje, i time doprinosi efikasnosti u procesu poslovanja ali takođe predstavlja i mogućnost za različite povrede privatnosti zaposlenih ali i poslodavaca. Ovom prilikom će biti analizirani određeni aspekti zaštite prava na privatnost zaposlenih, na međunarodnom planu. Analiza je usmerena u smeru načina za prikupljanje i zaštitu podataka o ličnosti kao i postupak u slučaju povrede prava na privatnost, te pitanja nadzora nad zaposlenima u smislu uvida u sadržaj poslovne korespondencije, video nadzora na samom radnom mestu, nadzora putem testiranja zaposlenih, itd. Autor smatra da se kroz prizmu najznačajnijih međunarodnih izvora koji se tiču zaštite privatnosti zaposlenih, mogu sagledati i usmeriti buduća rešenja zakonodavstva Republike Srbije.

Ključne reči: *privatnost; zaposleni; podaci o ličnosti; nadzor; radni odnos*.