

PROTECTION OF PERSONAL DATA OF EMPLOYEES

ABSTRACT: Protection of personal data of employees forms part of the concept of the right to privacy which is becoming increasingly important with the development of various means of monitoring and control by employers, thus creating the need for adopting the legislation that would protect individuals from undesired data processing. The legislation that regulates the field of data protection has created a complex system of their protection. This paper will hence summarise those legal solutions that are relevant to understanding the protection of personal data of employees in the European Union law, but also in the law of the Republic of Serbia. In addition to this, the paper will explore the right to protection of personal data from the perspective of employees, but also from that of employers, by analysing various means of supervision and examples from the practice.

Keywords: *right to privacy, protection of employees' privacy rights, monitoring of employees, employers' responsibility, employees' responsibility, social networks*

1.Introductory considerations

One of the many positive effects brought about by the development of information technologies is its influence on the incredible increase in data on nearly every individual in the world. Due to the speed and ease with which data can be collected and abused, the question of protection of personal data

* Doctoral candidate, The University of Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, secretary of the Faculty of Pharmacy, Novi Sad, e-mail: vasiljkovicjovana5@gmail.com

becomes one of the most relevant issues of the XXI century.¹ Protection of personal data within the right to privacy includes the aspect of protection of the right to confidentiality of personal data. In the field of work and employment, this right is relevant both for protecting the interests of employees and protecting the interests of employers. On the one hand, employers are obliged to provide protection of confidentiality of employees' data, while, on the other hand, employees are obliged to provide protection of any data with which they come into contact when performing their work tasks, concerning other employees, clients or third persons.

Persons employed in the company of an employer become integrated in the employer's sphere of decision-making and influence and cannot avoid it without losing their position. An employer aims to discover many details related to the employees' personality when forming an employment relationship.² It appears that it is very difficult to establish an efficient protection of personal data of an employee, because personal autonomy is in sharp conflict with the needs of modern employment. Namely, in the process of employment, the person seeking a job is in a subordinate position in relation to the potential employer. The reason for this is that the said person is not only unable to significantly influence the content of the employment contract, but is also unable to influence the type and scope of data required as proof that he or she meets the requirements for a particular job. In addition to this, for the duration of the employment contract, the employee, due to a subordinate position in relation to the employer and in fear of dismissal, cannot influence the scope and type of data stored or additionally requested by the employer.³ It is thus necessary that all questions pertaining to protection of private data of employees be regulated by law.

2. Legislation in the European Union

Multiple acts directly or indirectly dealing with protection of personal data have been adopted at the European level since 1950. The first one is the European Convention for the Protection of Human Rights and Fundamental Freedoms, in which Article 8 guarantees the right to respect for one's private

¹ Diligenski, A., Prlja, D., Cerović, D., (2018). *Pravo zaštite podataka*, Belgrade, Institute of Comparative Law, p. 7.

² Halbach, G., et. al., (1994). *Labour Law in Germany: an overview*, Bon, Federal Ministry of Labour and Social Affairs, p. 136.

³ Obradović, G., (2003). *Pravo zaposlenog na zaštitu podataka od značaja za radni odnos*, *Pravni život*, 52, (10), p. 962.

and family life, home and correspondence. The Charter of Fundamental Rights of the European Union⁴ is also of particular importance. The relevance of this Charter lies in the fact that it contains a provision on the protection of personal data, stipulating that data must be processed fairly, for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis stipulated by law. Everyone has the right of access to collected data concerning him or her, and the right to have them rectified.⁵ The European Union has also adopted the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data.⁶ The purpose of this Convention is to secure in the territory of each Party for every individual, whatever their nationality or residence, respect for their rights and fundamental freedoms, and in particular their right to privacy, with regard to automatic processing of personal data related to them.⁷

Another important document passed by the European Union is Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.⁸ Seeing as there were certain doubts regarding the meaning of information, as well as regarding the subjects and fields to which the protection extended, other supporting acts have been passed.⁹ However, Directive 95/46 was a cornerstone in the development of

⁴ This Charter was proclaimed in a joint declaration by the European Parliament, Council of the European Union and European Union Commission at the European Summit, in Nice, on 7th December 2000. See: Đorđević, S. (2011). *Pravni status Povelje o osnovnim pravima Evropske unije. Zbornik radova Pravnog fakulteta u Nišu*, (58), 219-234.

⁵ Article 8 of the Charter of Fundamental Rights of the European Union. (2019, October 15). Retrieved from <https://en.uts.org.rs/index.php/association/about-uts/work-reports/11-dokumenti/dokumenti/798-796>

⁶ This convention was opened for signature on 28th January 1981 (Convention of the Council of Europe ETS no. 108). FR Yugoslavia ratified it in 1992 (Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka, *Službeni list SRJ – Međunarodni ugovori*, br. 1/92, *Službeni list SCG – Međunarodni ugovori*, br. 11/2005 – dr. zakon i *Službeni glasnik RS – Međunarodni ugovori*, br. 98/2008 – dr. zakon i 12/2010).

⁷ Article 1, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Ibid*.

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, number L, 281, 31-50. Retrieved from <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>

⁹ Some of these acts are: Directive on privacy and electronic communications (Directive 2002/58 EC), Standard contractual clauses for the transfer of personal data to third countries (no. 2004/915 EC), Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (no. 45/2001 EC). Diligenski, A., Prlja, D., Cerović, D., (2018). *op. cit.*, pp. 9-10.

further EU legislation on the protection of data and right to privacy.¹⁰ One of the reasons for this was also the fact that case law was for a long time based on this Directive. The legal system of data protection in Europe that was based on the Directive 95/46 was not adequate enough to accommodate for the accelerated advancement of technology and various means of inadequate collection and processing of personal data. This is why after many years in preparation,¹¹ General Data Protection Regulation¹² was adopted in April 2016 and came into force on 25th May 2018. This Regulation constitutes a new legal framework prescribing the use of personal data of citizens of the European Union. It follows from the above that any organisation that in any manner processes the data of citizens of the European Union will be required to adhere to the new rules on personal data protection, even if its seat is outside the territory of the European Union, as is the case with the Republic of Serbia.¹³ The primary purpose of the General Data Protection Regulation is to secure respect of all the fundamental rights and freedoms, in particular the respect for private and family life, communication, the protection of personal data, freedom of religion, thought, freedom of expression and information, freedom to conduct a business, the right to cultural, religious and linguistic diversity, as well as the right to an effective remedy and a fair trial. This Regulation also aims to provide legal transparency and security; the same level of rights, obligations and responsibilities of individuals and institutions

¹⁰ Directive no. 95/46 primarily protected the fundamental rights and freedoms of individuals. The protection also extended to unborn children, deceased persons and, to a certain extent, legal entities – through directors and other responsible persons in companies. It also concerned employees, seeing as the Commission of the European Community concluded that this type of intervention is very important in the field of labour law, and that employers and third parties must be controlled when it comes to use of personal data for employment purposes. Jašarević, S. (2008). Zaštita ličnih podataka zaposlenih u srpskom i evropskom pravu. *Pravni život*, 57 (12), pp. 464-465.

¹¹ The legislative procedure for adopting a regulation that would comprehensively regulate the issues related to the data protection right began in 2012. Following the adjustment of numerous proposals and after a lengthy public discussion and consideration of over 4,000 amendments, the final text of the General Data Protection Regulation was adopted in April 2016. Due to its complexity and the adaptation required by the institutions that needed to implement it, it was agreed that the Regulation would come into force after a period of two years. Diligenski, A., Prlja, D., Cerović, D., (2018). *op. cit.*, p. 11.

¹² 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. *Official Journal of the European Union* (OJ), 59(1-88), 294.

¹³ Milosavljević, M., (2018). GDPR u Srbiji, (2019, 22th October). Retrieved from: <https://www.securitysee.com/2019/08/gdpr-u-srbiji/>

that engage in processing personal data, as well as equivalent sanctions in all European Union member states.¹⁴

3. Legislation in Serbia

In Serbia, it is the constitution of the Republic of Serbia¹⁵ that guarantees the protection of personal data, leaving further regulation of this field to laws. More precisely, a provision of the Article 42 of the Constitution provides a guaranteed protection of personal data, while collection, storing, processing and use of such data are regulated by law. In the very same article, the legislator stipulates that the use of personal data beyond the purpose for which they were collected in accordance with the law is prohibited and punishable, except for the conduct of criminal proceedings or the protection of security of the Republic of Serbia in the manner prescribed by law. Additionally, everyone has the right to be informed of their personal data collected in accordance with the law and everyone has the right to judicial protection in cases of their misuse. As with other human and minority rights, according to the provision of Article 202 of the Constitution, derogation from the aforementioned may be made only in a state of emergency and to the extent necessary.

The Serbian legislation does not specifically regulate employee privacy as such, but rather applies the general rules on the right to privacy and the protection of personal data to employees, which further complicates this issue within the Labour Law framework. The Labour Law¹⁶ did not regulate the issues of privacy rights in more detail, but only touched on this issue in several provisions. Thus, a provision of the Article 83 introduced the principle of protection of personal data,¹⁷ prescribing the rules pertaining to protection of employees' personal data. More specifically, by this provision the legislator stipulates that an employee has the right to inspect documents containing his or her personal data stored with the employer, the right to request the deletion of data that are not of direct relevance to the job he or she performs, as well as to rectify information that is incorrect. The legislator also stipulates that personal data relating to an employee may not be made accessible to a third party, except in the cases and under the conditions provided for by law or if necessary to prove the rights and obligations arising from employment or

¹⁴ See: Prlja, S. (2018). Pravo na zaštitu ličnih podataka u EU. *Strani pravni život*, (1), 89-99.

¹⁵ Ustav Republike Srbije, *Službeni glasnik RS*, br 98/06.

¹⁶ Zakon o radu, *Službeni glasnik RS*, br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – odluka US, 113/2017 i 95/2018 – autentično tumačenje.

¹⁷ This principle was introduced into the Labour Law of the Republic of Serbia in 2005.

in connection with work. The personal data of employees may be collected, processed, used and provided to third parties exclusively by an employee authorized by the manager. It follows from the abovementioned provisions that an employer needs to be mindful of how he treats employees' personal data, as well as of persons permitted to collect, use, process and provide those data to the third parties.¹⁸

The provision of Article 26 of the Labour Law stipulates that an employer may not request from the candidate information relating to family, i.e. marital status and family planning, i.e. submission of legal instruments and other evidence which are of no direct importance for the performance of tasks the employment relationship is established for. In addition to the aforementioned, an employer may not condition the establishment of an employment relationship on a pregnancy test, unless the relevant tasks involve considerable risk for the health of the woman and child, as determined by a competent health-care agency. An employer may not condition the establishment of an employment relationship on the candidate giving a prior statement on the cancellation of employment contract. Danilović¹⁹ is of the opinion that these rules are more principles than precise practical guidelines, which is why most privacy-related dilemmas remain outside the scope of Labour Law.

The primary law in the Republic of Serbia regulating the protection of personal data of employees is the Law on Personal Data Protection, which came into force in August 2019.²⁰ This law is identical to the General Data Protection Regulation, which means that all rules regarding the protection of personal data that apply to the members of the European Union, also apply to Serbia.²¹ A relevant component here is the alignment of privacy policy with the General Data Protection Regulation. In this regard, it is essential that companies that use personal data for business purposes focus on how to obtain consent from their employees for using their data, and also that they explain to them to what purpose the data will be used.

¹⁸ Kulić, Ž., Škorić, S., (2016). *Radno pravo*. Novi Sad, Faculty of Law for Commerce and Judiciary, p. 225.

¹⁹ Danilović, J., (2017). *Pravo na privatnost zaposlenih. Anali Pravnog fakulteta u Beogradu*, 65 (2), p. 170.

²⁰ *Official Gazette of RS*, no. 87/18.

²¹ By signing the Stabilization and Association Agreement, the Republic of Serbia committed to aligning national legislation in the field of personal data protection with the *acquis communautaire*. This issue is the subject of the negotiation chapters 23 – Judiciary and fundamental rights and 24 – Justice, freedom and security. (Milosavljević, M., *op. cit.*).

4. The right to protection of personal data of employees in modern law

In modern law, the right to privacy refers to the right of restricted access to an individual and the right of non-disclosure of certain personal information to other parties. There are novelties in the work process related to an increasing use of information and communication technologies, which creates countless possibilities, but also room for abuse. Personal data of employees and job applicants²² are necessarily stored by the employer and there is a question of what he or she will choose to do with them, i.e. if they will be used in the best interest of employees or to their detriment.²³ Nikolić²⁴ states that an employer is not obliged to ask for employees' consent to keep and process records on them, but it is necessary to ensure that employees are aware of the purposes for which these data will be used.²⁵ As a rule, employers should collect all personal data only from those persons to which the data refer. And if data collection by third parties is required, the employee in question should be informed of this in order to be able to give explicit consent. When obtaining consent, employers should indicate the purpose of the processing, the sources and methods used, the type of data they intend to collect, as well as the consequences if the employee refuses to consent, if any. On the other hand, employees should also be informed of the consequences of violating the right to confidentiality of other persons' personal data. The labour law consequences of violation of the mentioned obligation are more precisely regulated by autonomous legal acts, i.e. codes of professional and ethical conduct at work or collective agreements.²⁶ The decision of the Court of Appeal

²² These data are diverse and numerous and can include first name, last name, unique identification number, age, qualification, place of residence, marital status, etc. (Brković, R. Antić, A., (2016), *Zaštita prava na privatnost zaposlenih* in: Marija Krvavac (editor) *Human Rights: Ideals and Challenges – a scientific conference*, Kosovska Mitrovica, Faculty of Law, p. 718). According to the provision of Article 4, paragraph 1 of the Law on Personal Data Protection (*Zakon o zaštiti ličnih podataka*, Službeni glasnik RS, br. 87/2018), the Serbian legislator defines "personal data" as "any data relating to an individual whose identity is defined or definable directly or indirectly, especially on the basis of identity markers, such as his or her name and identification number, location data, identifiers in electronic communication networks or one or more features of his or her physical, physiological, genetic, mental, economic, cultural and social identity".

²³ Brković, R. Antić, A., op. cit. p. 718.

²⁴ Nikolić, V., (2014). *Zaštita privatnosti na radnom mestu*, *Izbor sudske prakse*, 22 (3), p. 13.

²⁵ Thus, the legislation prescribes, in Article 5 of the Law on Protection of Personal Data, the principles of processing, which precisely define the way in which personal data must be collected, stored and processed, as well as who is responsible for processing them.

²⁶ Stojković-Zlatanović, S., Lazarević, B. (2017). *Poverljivost podataka o ličnosti – implikacije na položaj zaposlenih sa stanovišta sudske prakse*. *Pravo i privreda*, 55 (4-6), p. 711.

in Belgrade is cited as an example of violation of the right to confidentiality and as an example of consequences of such violation on an employee's legal status.²⁷ This decision rejected the claimant's appeal against the decision of the trial court, as it upheld the ruling rendered in the disciplinary proceedings and the claimant was found guilty of a serious breach of duty. She was also given a disciplinary measure and a fine.²⁸

Literature accounts for three types of privacy: physical privacy, decision privacy, and data privacy.²⁹ Physical privacy in the field of labour and employment refers to the interest of the employer for the medical condition of the employee.³⁰ Namely, an employee is required to have a certain degree of medical fitness, which represents a condition for establishing a work relationship, depending on the nature of the work activities and the conditions in which these activities are performed.³¹ Compliance with the medical requirements is proven by a medical certificate. From the aspect of data protection in relation to the employee's personality and their privacy, how far an employer can go when gathering the data on an employee's or a potential employee's medical condition is a matter of great importance. It can be argued that the employer takes great interest in the medical condition of the employee in order to avoid payments. On the other hand, an employer taking too much interest in the employee's medical condition is an invasion of privacy, even when requested by the company doctor.³²

²⁷ Decision of the Court of Appeal in Belgrade, no. 1360/2014 dated 21.05.2014 (2019, 24th October). Retrieved from: <http://www.bg.ap.sud.rs/cr/articles/sudska-praksa/pregled-sudske-prakse-apelacionog-suda-u-beogradu/odeljenje-radnih-sporova/gz1-1360-2014.html>

²⁸ The claimant was employed by a preschool institution and she provided (without the permission of the principal) information on mothers who gave birth out of wedlock and who used the services of this institution to a scientific research institution for the purpose of scientific research work, i.e. the preparation of a doctoral dissertation. The court found that there had been a violation of Article 141, paragraph 1 of the Law on Foundations of Educational System (Zakon o osnovama sistema obrazovanja i vaspitanja, Službeni glasnik RS, br. 88/2017, 27/2018 – dr. zakon, 10/2019 i 27/2018 – dr. zakon), which means that the claimant had carelessly and negligently performed the duties entrusted to her. The current Labour Law does not contain provisions on the consequences of a violation of the right to confidentiality of information, in terms of the status of an employee who acted without authorization. In this regard, one can ask whether disclosure of personal data of service users or clients to third parties without the approval of a superior constitutes careless and negligent performance of duties (Navedeno prema: Stojković-Zlatanović, S., Lazarević, B. (2017). op. cit., p. 712).

²⁹ Moskop, J. C., et. al. (2005). From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine—part I: conceptual, moral, and legal foundations. *Annals of emergency medicine*, 45(1), p. 54.

³⁰ Ibid.

³¹ Šunderić, B., (1986). Uslovi za zasnivanje radnog odnosa radnika, Belgrade, Naučna knjiga, p. 120.

³² Obradović, G., (2003). op. cit. p. 963.

The decision privacy in the field of labour means non-interference of the employer in the decision making process of the employees regarding their activities which are not related to their work activities or assignments. Data privacy refers to the protection from the disclosure of the employees' personal data.³³ In the European practice the reference point is the idea of privacy as a human right guaranteed by the international conventions and national legislatures.³⁴ By concluding the employment contract this principle is regarded as a form of human dignity and freedom. Therefore the employees who are constantly and absolutely controlled by the employer and not allowed to display any form of private life, thus being reduced to work resources only, cannot be considered to be free and independent individuals and their human dignity is threatened.³⁵ For the purpose of obtaining a comprehensive view of the aforementioned form of privacy it is important to consider the decisions of the European Court of Justice which dealt with the issue of privacy of the employees in the work place. One of the more prominent cases is *Copland v United Kingdom*.³⁶ In this case, the employer monitored the employee's email, phone conversations and internet searches, without the employee's knowledge. The employer based his defense on the claim that this form of collecting information is justified when it comes to protecting property interests. Nevertheless the European Court held that phone conversations, email communication and internet usage were *prima facie* – private life and that the employee had reasonable expectations regarding privacy.

Accordingly, it follows that the rapid technological development has given rise to the usage of various methods and means in the field of employee monitoring. Hence the rest of this paper will be looking into different forms of employee monitoring.

5. Monitoring of employees in the workplace

The interest in electronic monitoring in the workplace started in the 80s when the US Office of Technology Assessment commissioned one of the first analyses of electronic monitoring in the workplace. Since then electronic monitoring has evolved to such extent that today there is no work-related segment

³³ Moskop, J. C., op. cit., p. 54.

³⁴ See Universal Declaration on Human Rights, article 12, Constitution of the RS article 60.

³⁵ Danilović, J. op. cit., p. 174.

³⁶ *Copland v United Kingdom*, Petition no. 62617/00, (2019, October 24), Retrieved from: <http://reforma.bezbednost.org/slucaj-kopland-protiv-ujedinjenog-kraljevstva/>

which cannot be seen by the monitoring technology.³⁷ Therefore it can be said that the information and communications technologies today are used for monitoring space, communication, and body. Namely, an employer monitoring and collecting information on the employees by means of technology does not constitute an illegal action. On the other hand, from the aspect of privacy invasion this is a very delicate activity. Apparently, the employer, being the owner of the work equipment and the business information is responsible for security, legality, work protection, and quality and effective performing of business activities. For those reasons they have the right, and the obligation to take reasonable and legal measures in order to pursue legitimate interests. The situation gets increasingly more complex when considered that for the employee, but also for the employer, it is impossible to separate the business and private spheres.³⁸ Therefore the employer must use the monitoring moderately, since their interest is confronted with the civil rights of the employees, including the right to privacy among other things.

The list of technical controls, which are available and most often used are: video surveillance, electronic or bibliometric room access control, use of official electronic mail, use of official phones, use of the internet in the workplace, GPS control of vehicle fleet use, social network activity, official computer content control, polygraph testing, etc.

With the usage of video surveillance of the employees the employer achieves two goals. The first goal concerns the completion of work obligations and work discipline of the employees, i.e. the employee is being monitored during work process and during working hours. This way the employer establishes whether the employee meets their working requirements and respects their work discipline. The second goal refers directly to the work process, which implies monitoring employees' behaviour and determining important facts regarding certain events, such as work-related injuries, confrontations between the employees etc.³⁹ It is necessary for the employer to restrict the video surveillance to the premises which are directly connected with the work process, which means it should not be used in the private premises of the employees such as dormitories, offices, bathrooms etc.

However, the matter of technical surveillance in the workplace in the Republic of Serbia is completely unregulated. The system mechanisms of

³⁷ Petrović, D., (2017). Upotreba informaciono-komunikacionih tehnologija u svrhu nadziranja u radnim organizacijama – slučaj Srbije. *Sociološki pregled*, 51(1), p. 90.

³⁸ Nikolić, V., op. cit., p. 13.

³⁹ Žarković, I. (2015). Mere elektronskog nadzora zaposlenih i pravo na privatnost na radnom mestu. *Nauka, bezbednost, policija*, 20(3), p. 168.

control, with the exception of the Commissioner⁴⁰, upon the reporting of incidents practically do not exist. That in turn makes room for abuse or inadvertent invasion of privacy of the employees by the employer and creates an unhealthy atmosphere of mistrust in organizations. Given the fact that the surveillance equipment is available to the employers, the employees are often not able to prove the abuse or mobbing by their superiors.⁴¹

One of the most relevant issues from the perspective of privacy protection law is monitoring the employees' communication. By controlling the communication that the employees have over the phone, email or social media profiles the employer enters the employee's personal sphere. By using this form of monitoring employers obtain relevant information on the behavior and habits of the employees, and on their efficiency and effectiveness while performing certain work tasks, which can jeopardize their right to privacy.⁴² On the other hand Brković and Antić⁴³ consider that employers can monitor employees' communication if the employees are informed of such control and if it refers strictly to the means which are related to the workplace and the work process, and which takes place during working hours.

Given that the use of email and the internet during working hours on the devices of the employer for private purposes has become reality for a large number of companies Bodiroga and Martinović⁴⁴ state that the lost work time has become an issue for the employers, and the question arises whether it should be sanctioned as well as whether the use of the said forms of media for private purposes can stand as ground for dismissal. The answer to this question can be found in the recent case law of the German Federal Labour Court which holds that the use of internet for private purposes is allowed, provided that the said use is not specifically forbidden and that it is short term. In that sense it is set out that a fifteen-minute usage of the internet for private purposes can be considered as breach of work obligations and may be ground for dismissal.

⁴⁰ Pursuant to the provision of article 4, paragraph 1, point 22 of the Data Protection Law, Commissioner for information of public importance and data protection is an independent government body established in accordance with the law and in charge of monitoring the exercising of Data Protection Law.

⁴¹ See: Biuković, S. (2018). Uticaj mobinga na radnu sposobnost zaposlenih, *Pravo – teorija i praksa*, 35(10-12), p. 103-115.

⁴² Snyder, J. L. (2010). E-mail privacy in the workplace: A boundary regulation perspective. *The Journal of Business Communication*, 47(3), p. 268.

⁴³ Brković, R. Antić, A., op. cit., p. 728.

⁴⁴ Bodiroga-Vukobar, N., Martinović, A., (2009). Izazovi novih tehnologija na radnom mjestu, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 30, (1), p. 79.

Regarding the use of social media employers tend to have opposing viewpoints. Namely, some employers completely forbid the use of social media during and after working hours, while some insist on using social media for promoting their company, products or services. Still, a lot of research points to the negative effects of a complete ban on internet use in the workplace. It is thought that a moderate use of the internet and even social media reduces stress at work, creates a positive work environment and increases productivity.⁴⁵ However, despite the fact that a moderate use of internet for private purposes can reflect positively on the employees, it can also stand as ground for disciplinary procedure and employment termination if it is stipulated as breach of work obligation in the internal legal acts of the employer, and pursuant to article 179, paragraph 2 of the Employment law. Therefore, employees' social media profiles more often than not affect their legal and labour status, especially if employees disclose inappropriate information in public damaging the employer's reputation.⁴⁶ In that regard, it is worth mentioning here the case of a teacher who was dismissed for writing on her Facebook profile that the people living in the school neighbourhood seem "arrogant and snobbish" and that she does not look forward to the new school year.⁴⁷

An employer may, by using his authority forbid the employee to post information on social media profile, referring to the article 179, paragraph 3, point 8. The information involved are most often the ones that can damage the employer and employee's reputation. Still, all that can be viewed as a restriction of freedom of the employees since the employees' expressing themselves in public in the said way and the freedom of speech are in direct correlation, rendering such a restriction by the employer an invasion of the employees' privacy. The content and the information on social media are connected to the employees' private life and should not reflect negatively on their legal and labour status.

6. Conclusion

The issue of an individual's personal data protection came into focus with the development of information technologies and various means of communication which enable mass information storage, as well as easy and fast information transfer. All of this has had an influence on the development of

⁴⁵ Chang, S. E., Liu, A. Y., Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems*, 115(1), p. 98.

⁴⁶ Brković, R., Antić, A., op. cit., p. 723.

⁴⁷ Sánchez Abril, P., Levin, A., Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal*, 49(1), p. 68.

personal data protection regulation in the European Union, and subsequently in other national legislatures. The need for this type of regulations exists, and it is regulated up to a point in our legislature and not only for the purpose of meeting the requirements for joining the European integrations, but also due to the fact that there are different kinds of individual's privacy and dignity breaches in practice, which are inadmissible and which remain unsanctioned.

The issue of employee's right to personal data protection refers to all the information on the employee that the employer can obtain. The employees in turn should be informed and aware of the nature, scope and reason for which their data is being used in advance. They should also be familiar with the use of technical surveillance equipment. On the other hand the employer needs to make a detailed estimate of the interest they want to obtain and whether a certain form of technical surveillance is in proportion with the desired purpose. In order to achieve this it is necessary to regulate the matter of electronic monitoring in a normative way, and make additional regulations through the internal legal acts of the company. In that regard, it is recommended that the acts contain precise definition of the field to which they are applied, as well as reasons for introducing the monitoring system, subject to the agreement with the employees. Moreover, incomplete labour and legal regulations regarding confidentiality protection in the field of work and employment lead to ambiguities related to rights and obligations of the employees and the issue of their responsibility, leaving this area in need for a more precise regulation in our employment legislation.

Vasiljković Jovana

Doktorand na Pravnom fakultetu za privredu i pravosuđe i sekretar Farmaceutskog fakulteta Univerziteta Privredna akademija u Novom Sadu

ZAŠTITA LIČNIH PODATAKA ZAPOSLENIH

R e z i m e

Zaštita ličnih podataka zaposlenih čini deo koncepta prava na privatnost koji postaje sve značajniji razvojem različitih načina praćenja i kontrole od strane poslodavaca, stvarajući tako potrebu za usvajanjem zakona kojim bi se pojedinci zaštitili od neželjene obrade ličnih podataka. Zakoni koji

regulišu oblast zaštite ličnih podataka omogućili su složen sistem njihove zaštite. Ovaj rad će stoga sažeti ona zakonska rešenja koja su relevantna za razumevanje zaštite ličnih podataka zaposlenih u zakonodavstvu Evropske unije, ali i u zakonodavstvu Republike Srbije. Pored ovoga, rad će istražiti pravo na zaštitu ličnih podataka iz ugla zaposlenih, ali i prava poslodavaca, analizirajući različita sredstva nadzora i primere iz prakse.

Ključne reči: pravo na privatnost, zaštita prava privatnosti zaposlenih, praćenje zaposlenih, odgovornost poslodavca, odgovornost zaposlenih, društvene mreže

Literature

1. Brković, R. Antić, A., (2016), Zaštita prava na privatnost zaposlenih in: Marija Krvavac (editor) *Ljudska prava između ideala i izazova sadašnjosti – academic conference*, Kosovska Mitrovica, Faculty of Law pp. 717-731.
2. Bodiroga-Vukobar, N., Martinović, A., (2009). Izazovi novih tehnologija na radnom mjestu, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 30, (1), pp. 63-89.
3. Biuković, S., (2018). Uticaj mobinga na radnu sposobnost zaposlenih, *Pravo – teorija i praksa*, 35 (10-12), pp. 103-115.
4. Chang, S. E., Liu, A. Y., Lin, S., (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems*, 115(1), pp. 88-106.
5. Danilović, J., (2017). Pravo na privatnost zaposlenih. *Anali Pravnog fakulteta u Beogradu*, 65 (2), pp. 162-182.
6. Diligenski, A., Prlja, D., Cerović, D., (2018). Pravo zaštite podataka, Belgrade, The Institute of Comparative Law.
7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, number L, 281, 31-50. Retrieved from: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>.
8. Đorđević, S., (2011). Pravni status Povelje o osnovnim pravima Evropske unije. *Zbornik radova Pravnog fakulteta u Nišu*, (58), pp. 219-234.
9. Jašarević, S., (2008). Zaštita ličnih podataka zaposlenih u srpskom i evropskom pravu. *Pravni život*, 57 (12), pp. 459-472.

10. Copland v United Kingdom, Petition no. 62617/00, (2019, October 24), Retrieved from: <http://reforma.bezbednost.org/slucaj-kopland-protiv-ujedinjenog-kraljevstva/>.
11. Kulić, Ž., Škorić, S., (2016). Radno pravo. Novi Sad, Faculty of Law for Commerce and Judiciary.
12. Milosavljević, M., (2018). GDPR u Srbiji, (2019, October 22). Retrieved from: <https://www.securitysee.com/2019/08/gdpr-u-srbiji/>.
13. Moskop, J. C., et. al. (2005). From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine—part I: conceptual, moral, and legal foundations. *Annals of emergency medicine*, 45(1), pp. 53-59.
14. Nikolić, V., (2014). Zaštita privatnosti na radnom mestu, *Izbor sudske prakse*, 22 (3), pp. 10-14.
15. Obradović, G., (2003). Pravo zaposlenog na zaštitu podataka od značaja za radni odnos, *Pravni život*, 52, (10), pp. 957-970.
16. The decision of the Court of Appeals in Belgrade, no. 1360/2014 dated May 21, 2014. (2019, October 24). Retrieved from: <http://www.bg.ap.sud.rs/cr/articles/sudska-praksa/pregled-sudske-prakse-apelacionog-suda-u-beogradu/odeljenje-radnih-sporova/gz1-1360-2014.html>.
17. EU Charter of Fundamental Rights, (2019, October 15) Retrieved from: <https://en.uts.org.rs/index.php/association/about-uts/work-reports/11-dokumenti/dokumenti/798-796>.
18. Prlja, S., (2018). Pravo na zaštitu ličnih podataka u EU. *Strani pravni život*, (1), pp. 89-99.
19. Petrović D., (2017). Upotreba informaciono-komunikacionih tehnologija u svrhu nadziranja u radnim organizacijama – slučaj Srbije. *Sociološki pregled*, 51(1), pp. 81-108.
20. 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. *Official Journal of the European Union* (OJ), 59(1-88), 294.
21. Sánchez Abril, P., Levin, A., Del Riego, A., (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal*, 49(1), pp. 63-124.
22. Stojković-Zlatanović, S., Lazarević, B., (2017). Poverljivost podataka o ličnosti – implikacije na položaj zaposlenih sa stanovišta sudske prakse. *Pravo i privreda*, 55 (4-6), pp. 702-714.

23. Snyder, J. L., (2010). E-mail privacy in the workplace: A boundary regulation perspective. *The Journal of Business Communication*, 47(3), pp. 266-294.
24. Šunderić, B., (1986). Uslovi za zasnivanje radnog odnosa radnika, Belgrade, Naučna knjiga.
25. Ustav Republike Srbije, *Službeni glasnik RS*, br 98/06.
26. Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka, *Službeni list SRJ – Međunarodni ugovori*, br. 1/92, *Službeni list SCG – Međunarodni ugovori*, br. 11/2005 – dr. zakon i *Službeni glasnik RS – Međunarodni ugovori*, br. 98/2008 – dr. zakon i 12/2010.
27. Zakon o radu, *Službeni glasnik RS*, br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – odluka US, 113/2017 i 95/2018 – autentično tumačenje.
28. Zakon o osnovama sistema obrazovanja i vaspitanja, *Službeni glasnik RS*, br. 88/2017, 27/2018 – dr. zakon, 10/2019 i 27/2018 – dr. zakon.
29. Zakon o zaštiti ličnih podataka, *Službeni glasnik RS*, br. 87/2018.
30. Žarković, I., (2015). Mere elektronskog nadzora zaposlenih i pravo na privatnost na radnom mestu. *Nauka, bezbednost, policija*, 20(3), pp. 165-182.