

## EMPLOYEE PROFILING – ETHICAL AND LEGAL BOUNDARIES\*\*

### *Summary*

*Employee profiling emerged from an employer's desire to make the work process as efficient as possible and assign the most optimal work tasks to each person employed. However, with so-called artificial intelligence, algorithms that can process a larger amount of information electronically and, based on that, optimise work or predict employee behaviour, profiling takes on new dimensions. Employers conduct research that far exceeds their legally permitted interests in the private and family lives of employees, collecting their digital footprint, including information related to the most intimate aspects of their lives. Creating medical and psychological profiles thus becomes technically feasible for the employer, but this does not make the activity permissible. The right to personal dignity, as well as the right to privacy, are realised in the work process equally with the right to decent work and the right to a reasonable expectation of privacy at work. The research examines the legal and ethical aspects of employee profiling in the context of modern communications and the mass processing of information from social media, public and non-public databases, cross-referencing them with classical (and still valid) principles of the employer-employee relationship. It highlights the risks and dangers, as well as the benefits of using new digital tools.*

**Keywords:** *Employee Profiling, Algorithmic Predictability, Personal Data Protection, Right to Privacy at Work, Reasonable Expectation of Privacy at Work.*

### 1. INTRODUCTION

Using modern technologies in the work process is not a novelty, but it is increasing every day with a series of new tools that employers can use, or that can be used by employees. Some of them lead to positive effects that are reflected in

\* PhD, Senior Research Fellow, Institute of Comparative Law, Belgrade, e-mail: [m.reljanovic@gmail.com](mailto:m.reljanovic@gmail.com), ORCID: <https://orcid.org/0000-0001-6379-7545>.

\*\* This work is a result of research within the project "Adapting the Legal Framework to Social and Technological Changes with a Special Focus on Artificial Intelligence", carried out in 2025 by the Institute of Comparative Law with financial support from the Ministry of Science, Technological Development and Innovation (contract number 451-03-136/2025-03/200049).

higher productivity while reducing working hours or improving working conditions. Some are predominantly negative, such as the excessive use of employee monitoring tools that far exceed the rational needs of the employer or using technology to circumvent labour rights legal provisions (so-called “hacking labour law”<sup>1</sup>). Precisely because of the emerging of a number of new opportunities for misuse of digital technology at work, the principle that the digitalization of work processes cannot undermine labour rights was adopted at the EU level, contained in Directive 2019/1152 on transparent and predictable working conditions.<sup>2</sup> Most of these tools are, however, of an indefinite nature – they can lead to good or bad outcomes for the employer or employees, depending on how they are used. One such example is employee profiling, i.e. the systematic use of available data about an employee in order to create a complex profile that serves certain needs of the employer. With introducing algorithms for automatic research and processing of large amounts of data, called “artificial intelligence”, employee profiling is not only becoming easier and more efficient, but is also gaining previously unimagined purposes.

Employers use classic employees profiling to improve their efficiency and productivity, to make it easier to cope with the tasks they perform, or to hire an individual for certain tasks who would (in theory) perform them best. This profiling is limited by the right to privacy of employees, as well as the right to protecting personal data. There is also a prohibition on the employer collecting any data that was not related to employee’s expertise, his work results or other information directly linked to the work process. The employers’ access to data cannot create a broader picture of the employees outside their workplaces.

In such circumstances, the theory of reasonable expectation of privacy at work was created. It is based on the notion that the right to privacy of a person is inalienable and cannot be suspended entirely in the work process. It will be reduced in certain aspects that are important for the smooth running of the work process and application of the occupational safety measures, but apart from that every employee retains most of the right to privacy, which includes (but is not limited to) the right to privacy of correspondence, the right to private and family life, the protection of personal data, including particularly sensitive medical data. This theory, developed in detail in the case law of the European Court of Human Rights, is an essential element in limiting employer actions that could lead to violations of the right to privacy, including the collection of data used for profiling.

Development of new technologies and internet usage trends means that all kind of data about employees can be found online – primarily on their social media profiles, but also in other public online databases. This has influenced the

---

<sup>1</sup> C. Alexander, E. Tippet, “The Hacking of Employment Law”, *Georgia State University College of Law, Legal Studies Research Paper No. 2018-09*, 2018. Cited according to: M. Reljanović, J. Misailović, „Radnopravni položaj digitalnih radnika”, *Strani pravni život* 3/2021, 424.

<sup>2</sup> M. Reljanović, „Informacione tehnologije i izazovi u reformi radnog prava“, *Zbornik Pravnog fakulteta u Novom Sadu* 2/2020, 774.

expansion of profiling, which nowadays extends far beyond the determining an individual's work capacity, and penetrates far into both his private sphere and into details that cannot be directly related to the work process, or the tasks employee performs. So-called "models of prediction of employees' behaviour" are emerging, which are created based on the processing of all available (public and non-public) data about that person. They are created by processing the "digital fingerprints" a person voluntarily leaves (on social networks or sites where they comment or react) and through the digitalisation of state administration and public service databases (information available, for example, to the police or mandatory social security institutions).

The research follows the contemporary concept of profiling, its elements and potential uses. The basic hypothesis is that profiling, which goes deeper than the traditional processing of employee data, most often cannot be justified by the employer's rational and objective business interest, and therefore violates the moral and ethical codes of employer-employee relations, as well as the legal restrictions that are clearly set when it comes to the employer's impact on employee's private life. In accordance with the direction and content of the research, the normative method is dominantly used.

## 2. THE RIGHT TO THE REASONABLE EXPECTATION OF PRIVACY

The theory of reasonable expectation of privacy is based on the principle that each person must adapt their privacy standards to the location they are in and the social role they are engaged in at that moment.<sup>3</sup> Thus, an employee does not waive her/his right to privacy at work. It still exists, although it has been modified to meet the objective needs of the employer. "Workers have an interest in autonomy and an interest in privacy. Employers, on the other hand, have an interest in control over the disposition of their assets for efficiency, productivity, and risk reduction."<sup>4</sup>

This theory is not of recent origin; it dates back to a time long before modern communication technologies emerged. One of the first cases of this kind before the European Court of Human Rights was *Halford v. United Kingdom*,<sup>5</sup> where the Court found that employees retain the right to privacy of communication even when using the employer's communication tools. Later, in the case of *Libert v. France*,<sup>6</sup> the Court emphasised that data that can be considered private is still protected from employer access, even when it is located on an employer's com-

<sup>3</sup> D. Golubović, M. Galetin, „Pregled prakse Evropskog suda za ljudska prava od značaja za obradu podataka o ličnosti putem video-nadzora“, *Strani pravni život* 1/2024, 69.

<sup>4</sup> R. Bortnick, "Restoring Reasonable Expectations to Privacy at Work in the Face of Modern Electronic Monitoring Practices", *UC Law Journal* 5/2024, 1488.

<sup>5</sup> European Court of Human Rights, *Halford v. the United Kingdom*, Application no. 20605/92, Judgment of 25.6.1997.

<sup>6</sup> European Court of Human Rights, *Libert v. France*, Application no. 588/13, Judgment of 22. 2. 2018.

puter. “Respect for private life and the privacy of correspondence continues to exist, even if they can be limited to the extent necessary.”<sup>7</sup> Privacy is of course not absolute, which the Court found it necessary to emphasise in the case of *Barbulescu v. Romania*,<sup>8</sup> when it sided with the employer who had reviewed his employee’s emails on the work address. Therefore, the privacy of individuals is maintained but is limited by certain boundaries that are necessarily needed in specific (working) circumstances. Modern means of communication only contributed to practical modifications in preserving this right, leading for example to the creation of the so-called “right to disconnect”<sup>9</sup>

How does employee profiling fit into such concept of workplace privacy? First, it should be emphasised that the reasonable expectation of privacy extends to activities the employee performs in their free time, outside of working hours, and outside of the employer’s premises. In this case, the employer can still access data that is relevant to the employee’s work, but no further. For example, an employee visiting the doctor is not something an employer should be concerned about, unless it is related to taking sick leave. In that case, the employer will be aware of the medical issues, but it will not be acquainted to the nature of the illness nor any other details related to the treatment process. The same principle applies in a number of situations when employees have to present some circumstances from their family or private lives to employers in order to exercise their relevant employment rights. For example, in the case of the employee’s wife or partner giving birth, the employee will be entitled to a paid leave, but the employer cannot know that this circumstance has occurred until the employee informs it. Furthermore, in this specific case, the employee is required to provide proof of the child’s birth, which will give the employer access to more information that would otherwise be considered private. In this case the employer is not exceeding its limitations, as the information it obtains is necessarily needed to realise the right of the employee. Similar situations will occur in other situations regulated by law or the employer’s internal documents: marriage, illness or death of a family member, household relocation, and similar events. However, outside of situations regulated by law and employers’ internal documents, the employer cannot collect information about the employee.

Considering all the above, it can be concluded that employee profiling will only be permitted if the employer uses exclusively the data about the employee that is available to them by usual means and that relates to their professional engagement. There may be exceptions to this rule, which are part of the theory of reasonable expectation of privacy at work, such as the employer’s interest in conducting a security check, protecting some of its commercial interests, and the like. However,

---

<sup>7</sup> European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*, Updated on 31 August 2024, 35, 151. Cited according to: M. Reljanović, A. Knežević Bojović, *Pravo na privatnost na radu*, Institut za uporedno pravo, Beograd 2025, 95.

<sup>8</sup> European Court of Human Rights, *Bărbulescu v. Romania*, Application no. 61496/08, Judgment of 12.1.2016.

<sup>9</sup> See: J. Rajić Čalić, „Pravo na isključivanje – između porodičnog života i profesionalnih dužnosti”, *Radno i socijalno pravo* 2/2023, 303–319.

in these cases, there are serious limitations which employers themselves are often unaware of, or if they are aware, they try to circumvent them through unethical practices. One of the better examples of such illegal collection of data about an employee (or job candidate) is access to a person's criminal record. Although the employer cannot inspect it, except in rare cases prescribed by law (and only by law, so it cannot be prescribed by the employer's internal acts), employers will sometimes request a certificate of non-conviction as part of the regular documentation when applying for a job. This leads to a situation where, even though the employer cannot obtain these documents, it can acquire them from the person who has that authorisation – the very individual whose criminal history is being investigated.<sup>10</sup> The job candidates can refuse to submit this document, but this will undoubtedly lead to their rejection, potentially resulting in legal action against the employer.

### 3. MODALITIES OF THE EMPLOYEE PROFILING

Profiling is “the use of algorithms or other techniques to create, discover or construct knowledge from huge sets of data”.<sup>11</sup> Profiling in the field of labour is considered the collection of data about an employee that is processed analytically and systematically for purposes necessary for the functioning of the work process. “Automated profiling involves different *technologies* (hardware), such as RFID-tags, biometrics, sensors and computers as well as *techniques* (software), such as data cleansing, data aggregation and data mining.”<sup>12</sup> Analysis of the gathered data is usually automatic, so “conclusions” are drawn without human role or input.

For job applicants, the purpose of processing is to decide whether the individual meets the requirements for employment and whether they are the highest quality among the candidates available to the employer. For employees, profiling can be done to assess work quality, for potential employee promotion, and for optimising work processes (assigning employees the tasks where they have proven to be the most productive<sup>13</sup>). In this sense, profiling assumes the collection and analysis of data related to the employee's professional life.

However, some employers are using the fact that a large amount of online information is available about each of us to create profiles that not only focus on data about expertise and work results but potentially delve deeply into the private and family lives of employees, as well as their specific psychological characteristics and

---

<sup>10</sup> See: M. Reljanović, A. Knežević Bojović, 48–49.

<sup>11</sup> M. Hildebrandt, “Defining Profiling: A New Type of Knowledge?,” in: *Profiling the European Citizen Cross-Disciplinary Perspectives* (eds. M. Hildebrandt, S. Gutwirth), Springer Science, Business Media B.V., Houston 2008, 17.

<sup>12</sup> *Ibid.*

<sup>13</sup> “Through a fusion of data analytics algorithms and machine learning, our proposed solution will enable the profiling system to identify patterns, correlations, and insights that facilitate optimal employee-to-project assignments. The system's intelligent recommendation engine will consider various project requirements, employee interests, and individual profiles, ensuring the formation of balanced and high-performing project teams.” A. Rafae, M. Erritali, “Using a Profiling System to Recommend Employees to Carry Out a Project”, *Electronics* 12/2023, 2.

preferences regarding various aspects of social life. Thus, profiling can involve two types of data compilation about an employee.

The first method of profiling involves collecting and processing data that is relevant to expertise, education, professional experience, and work results. This data may also include the collection of documentation: school or university diplomas, proof of completed training courses or the acquisition of certain licenses, and similar. In certain situations, they may also involve the collection of specific data, such as proof of health, when this is important for performing particularly demanding and difficult work tasks. Profiling individuals working in security or similar safety and national defence duties can significantly intrude into their private and family lives. However, what is common to every profiling of this type are the following circumstances: profiling is done according to pre-known procedures (it is known how and from whom the data is collected); the person whose profile is being created has been informed in advance about what data will be collected and processed, and has given their (explicit or implicit) consent for this<sup>14</sup>; there is a clearly defined legal basis for collecting and processing data, and the employer's internal regulations only specify and operationalise the employer's powers, which are certain and clearly defined by existing regulations.

The second type of profiling, unlike the first, is carried out through legally questionable and ethically unacceptable activities. This means that in addition to the data available to the employer through public registers of professional competencies, as well as through data and public documents provided by the employees themselves, profiling is done by collecting all available data about a person, without him/her knowing anything about it. In this context availability of data is understood in the broadest sense of the meaning, so it can refer to both data that is publicly available (for example, on social media where the employee has open profiles) and data that should not be publicly available but can be purchased from individuals who engage in their mining (which often boils down to unauthorised and unlawful access to various databases). In the early days of social media, employers engaged in practices that would be unthinkable today, such as collecting passwords for employees' online profiles.<sup>15</sup> Today such a practice doesn't exist, but it's not uncommon for an employee to be subtly or not-so-subtly pressured to include their employer's or direct supervisor's profile in their closest circle of friends on social media.

There was also early confusion about which social media data was private and which was public.<sup>16</sup> This doubt is not realistic, because data is not only divid-

---

<sup>14</sup> "(...) the regulation of automated profiling was seen as a means designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him." European Commission, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, COM(90) 314 final, 29.

<sup>15</sup> See: N. D. Beadle, "A Risk Not Worth the Reward: The Stored Communications Act and Employers' Collection of Employees and Job Applicants' Social Networking Passwords", *American University Business Law Review* 2/2012, 397–412.

<sup>16</sup> D. H. Kluemper, "Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment", *Selection, Social Media in Human Resources Management Advanced Series in Management*, 2013, 5.

ed according to whether it is private or public but also according to whether it is related to the work process and the tasks the employee performs or is applying for, or not. Thus, any information that an employee or job candidate leaves on social media platforms designed to showcase users' competencies and attract potential employers (such as LinkedIn, for example) will be treated as available and relevant to the employer. However, even among such publicly available information, if the employer finds some that should not influence their decision-making and formation of opinions about the person being profiled, e.g. such as information about family members, it must not be used for any purpose – because the employer is already prohibited from using it in advance based on irrelevance, not public availability.

Gathered information can include data related to the employee's health and financial status, as well as information about their union activities, political preferences, and even details about their intimate life and sexual preferences. It is clear that most of this data cannot be collected legally, and even when it is compiled out of information that is somewhat available in the online world, it cannot be said that the employer has any right to collect and further process it, for any legal purpose.

A special subtype of profiling exists when an employer collects data that the individuals submit themselves but does so for fraudulent purposes. This happens with the advertising of so-called “ghost jobs”, positions that don't actually exist at that employer (or exist but there are no new openings for employment), and the sole purpose of the process is to create a database of potential candidates in case a vacant position opens up in those jobs that needs to be filled quickly, or to attract candidates who, because of their current state of financial duress, might be willing to accept other jobs under significantly worse conditions than originally advertised. Due to the fact that the employer is authorised to regulate the work process completely autonomously, there is practically no way to prove that ghost-job advertising is malicious, let alone illegal (if the data of applicants is collected in accordance with existing restrictions). Therefore, this practice is considered primarily immoral and unethical, but because of its formal legality it is gaining increasing popularity.<sup>17</sup>

The results of profiling can therefore be twofold. On the one hand, profiling allows employer to gain a precise insight into employees' capabilities and potential and to assign them to tasks that best suit them accordingly, to reward them or engage them in programs of professional development, and so on. Vereb, Krajcsak and Kozak suggest several work-related usages of “predictive analytics”, such as help with employees' selection, career planning, training and development.<sup>18</sup> It can also identify the weakest links in the work process and, accordingly, to warn employees

---

<sup>17</sup> B. Kesslen, 1 of every 5 job postings is actually fake, study says, <https://qz.com/one-in-five-job-postings-is-fake-ghost-jobs-1851738201>, 27. 7. 2025.

<sup>18</sup> D. Vereb, Z. Krajcsak, A. Kozak, “The importance of positive employee experience and its development through using predictive analytics”, *Journal of Modelling in Management* 1/2025, 59–60.

about unsatisfactory work results, to work with them further to improve those results, or, as a last resort, to dismiss them so they can be replaced by higher-quality employees. There are ideas on the web platform for profiling scholars, in order to easily connect with job-related researchers around the globe.<sup>19</sup> Profiling in this sense can be a useful tool for both sides in an employment relationship and is often used in complex production systems and work processes where it is important to manage human resources optimally.

On the other hand, profiling aimed at collecting data that should give employers insight into aspects of the employee's life that are not permitted to be accessible to them, such as health status or trade union activity, results in creating a profile that will answer the questions employer is not allowed to ask because it is illegal – for example, whether there is a real possibility that the employee is ill with a serious chronic disease that will cause them to be absent from work more frequently in the future, or whether it is a realistic scenario that the employee, if dissatisfied with working conditions, will mobilise others for unionisation.

Thus, an important aspect of profiling is predictability. Predicting how an employee will behave in certain situations is not always immoral or illegal. Employees can be tested on how they perform in crisis situations, under pressure, during overtime, and so on. In this sense, predicting the reaction – the speed and quality of resolving problem situations related to the work process – is justified by the employer's economic and organisational interests. Certainly, problems can arise in those situations as well, and as Kovačević observes it's necessary to consider all the data relevant for monitoring an employee's work performance.<sup>20</sup> But when it comes to deeper analyses that go beyond work tasks, profiling becomes a dangerous "pre-emptive tool" in the hands of the employers. And not only that, but it can also be discussed about distorted perception of predictability. The employer will as a rule consider the profiling outcome as an absolute truth. Most times, this will be a misconception. For example, an algorithm can make a psychological profile of an employee created by processing data collected from her/his social networks, even though it is not realistic for that profile to contain all the necessary information, nor that collected data is accurate (an individual's life on social networks most often represents only one segment of their personality, where they present themselves as they want others to see them, it does not always correspond to the real state of affairs).

In such situations, the question arises: what is the purpose of such profiling? Ever since the era of genetic screening, which has since been banned in a number of countries, employers have tried to learn more about their employees than they should, all under the guise of "legitimate economic self-defence". Thus, in many countries today impermissible questions are still asked about family planning, the financial or health status of candidates during job interviews, psychological tests

---

<sup>19</sup> See: C. Etus, T. Okonkwo, "Development of Staff Profiling and Identification System", *International Journal of Novel Research in Computer Science and Software Engineering* 2/2022, 1–19.

<sup>20</sup> T. Kovačević, „Izazovi digitalizacije rada i zaštite ličnih podataka“, *Strani pravni život* 2/2023, 312.

are conducted on candidates and employees, and private detectives are hired to monitor employees outside the employer's premises and outside working hours. New technologies have enabled a whole range of other, usually more subtle but also not legal, ways of collecting data about employees – such as constant GPS tracking 24/7 and video surveillance, or even more drastically, installing software that records every keystroke on employees' computers. The possibilities for abuse are therefore very widespread, but the effects are very modest. Besides the fact that in this way the employer most often violates regulations, even when they don't, they create an atmosphere of distrust and fear, constant surveillance among employees, which cannot lead to either higher productivity or better interpersonal relationships.<sup>21</sup> However, the low level of predictability of employees' reactions to certain circumstances does not diminish the importance of profiling in the eyes of employers, so it is more prevalent today than ever.

Furthermore, any use of information learned by the employer that is not relevant to performing the work for which the employee is engaged (or might be engaged) can lead to discrimination.<sup>22</sup> Using employee data outside the narrow circle of information that the employer would otherwise need to know will practically always constitute discriminatory treatment whenever it is used to deny the employee a right they would otherwise enjoy if the employer did not use information they should not even know.<sup>23</sup> This type of discrimination is most common during hiring, e.g. when an employer investigates a candidate's family life, and the information obtained in this way directly influences their decision on whether to offer employment. However, it can also be applied at later stages of the labour relationship. For example, if an employee is passed over for promotion because her/his profiling showed she/he is prone to trade union activism, this would constitute discrimination based on union membership because this type of information should not be relevant when the employer decides. The person at the employer who decides on employees' rights may also unconsciously be guided by some of the data that classifies (or does not classify) the employee into the same value category to which she/he belongs. "Bias can also occur whereby recruiters select applicants who are similar to themselves or who share common interests."<sup>24</sup>

---

<sup>21</sup> According to the American Psychological Association, workers subject to electronic monitoring are nearly twice as likely as workers free from monitoring to report issues with stress at work (60%) and to experience negative impacts of the work environment on their mental health (45%). American Psychological Association, Workers Appreciate and Seek Mental Health Support in the Workplace, <https://www.apa.org/pubs/reports/work-well-being/2022-mental-health-support>, cited according to: R. Bortnick, 1484.

<sup>22</sup> "Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products". The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, 10.

<sup>23</sup> P. McDonald, P. Thompson, P. O'Connor, "Profiling employees online: shifting public-private boundaries in organisational life", *Human Resources Management Journal* 4/2016, 546.

<sup>24</sup> W. Smith, D. Kidder, "You've been tagged! (Then again, maybe not): employers and Facebook", *Business Horizons* 53/2010, 491–499, cited according to: P. McDonald, P. Thompson, P. O'Connor, 549.

The General Data Protection Regulation of the European Union (GDPR)<sup>25</sup>, which also applies outside the EU's borders, restricts profiling in general and the use of data generated from profiling: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."<sup>26</sup> One of the exceptions to this rule relates to the explicit consent of the profiling subject for the collection and processing of data.<sup>27</sup> It cannot be said that the employee's explicit consent was given when the employment contract was signed, and this for at least two reasons. The first is that the relationship between employer and employee must be viewed as a relationship of unequal power, and in this sense, it should not be assumed that by signing the contract, the employee has granted the employer broader powers than those minimally necessary for their work and the realisation of the rights and obligations of both parties to the contract. National legislations across Europe consider workers as vulnerable individuals when the processing involves certain types of data.<sup>28</sup> The second is that it cannot be assumed that the employee has given the employer free rein to intrude into their privacy in a way that is otherwise impermissible, regardless of the employee's willingness to waive a certain range of their rights. Therefore, in certain situations, even the employee's consent will not affect the illegality of the employer's actions, and any data collection that the employee has not agreed to will not comply with GDPR. A similar solution is also contained in the Serbian Law on the Protection of Personal Data: with this type of data processing, the employee must explicitly agree.<sup>29</sup>

The next question that arises is whether it is justified for an employer to use information obtained through profiling to dismiss an employee, if it concerns some socially undesirable behaviour? The answer to this question is not at all simple and will depend on whether the information the employer learned impacts the work process. For example, if it learns that an employee is using narcotics, it can pay attention to their behaviour at work and potentially ask the employee to take a drug test. Such behaviour is in line with protecting not only the employer's property and the quality of the work process, but also the safety of other employees and everyone else in the work area. A similar response can be imposed for some more controversial information. For example, if a social worker posts racist statements, the employer will certainly check whether such views affect her/his work environment and whether there has been any violation of ethical norms of

<sup>25</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016, 1–88.

<sup>26</sup> GDPR, Art. 22(1).

<sup>27</sup> GDPR, Art. 22(2c). See also for comment and examples: A. Diligenski, D. Prlja, D. Cerović, *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd 2018, 51–61.

<sup>28</sup> G. Malgieri, *Vulnerability and Data Protection Law*, Oxford University Press, 2023, 156–157.

<sup>29</sup> Zakon o zaštiti podataka o ličnosti, *Official Journal of the Republic of Serbia* No. 87/2018. See Art. 23(2.6) and Art. 24(2.7).

behaviour towards colleagues, or potential discrimination by that employee on racial or other grounds. In these situations, the employer only uses the information it has obtained to focus attention on certain employee actions, to protect a more significant good – therefore, it will not be used directly as the reason for the employer’s specific actions towards the employee. However, there are also cases where the employer, immediately after learning that an employee holds certain socially unacceptable beliefs (for example, that they are a racist or a Nazi), will react by firing the employee, who in the employer’s opinion is damaging the employer’s reputation and whose off-duty behaviour potentially contributes to the disruption of interpersonal relationships in the work process. Here the information is used directly, and there is no proven consequence for the employer’s interests or safety of other employees – the disputed employee is removed from the work collective solely because the employer is aware of their activities outside of work. This practice is highly questionable and could lead to a lawsuit against the employer. The only potential exception might be the situation when an employee, by posting such content, implies that it is also her/his employer’s view (thus tangibly damaging the employer’s reputation), or when it is clear that by expressing such views the employee does not meet the basic requirements for performing the duties they currently hold (for example, an employee in an organisation that accepts and assists migrants expresses violent anti-migrant views). Besides these (relatively rare) exceptions, such employer practices – although they could be called ethically acceptable in a way – raise a number of legal uncertainties. The basic conclusion, however, is that if the employer cannot prove a direct threat to an important interest (for example, employees safety) or a violation of regulations or internal acts by the employee simply by publishing certain information, they cannot proceed with their dismissal or sanction them in any other way for work non-related views and actions.

#### **4. CONCLUSIONS AND FINAL REMARKS**

It is not disputed that the employer has the right to protect themselves from so-called “negligent hiring”, or “negligent promotion”, which is often cited as one of the main excuses for using profiling on candidates and employees. However, this has been done in the past few decades only by violating their rights – in this case, not only labour rights but also basic civil rights to privacy and personal dignity – to create an entire system of assuring the employer that their choice will be correct not only in terms of business and professional criteria but also in relation to many other details from their private and family life that make the selection “perfect”. It is clear that the protection of employees’ rights and their human rights take precedence over the protection of the employer’s economic interests. Also, over the decades of developing modern human resource management science, a number of other tools have been identified through which relevant worker

characteristics can be examined without violating labour regulations and human rights.

Profiling of employees carries the risk of crossing the boundaries of private and family life. Simply put, profiling to eliminate employees from their work collectives or prevent them from exercising legal rights leads to discrimination and is undoubtedly illegal. The so-called predictability obtained as a result of complex profiling and creating models of employees' potential responses in certain complex or socially (or politically) sensitive situations is not only impermissible but will also be inaccurate in many cases because it is based on a limited number of information, and of uncertain accuracy. Thus, Longo's words should be understood as a critic to the easy road for employers to getting to know their employees: "Thanks to the measurability of everything, the primary production of vast amounts of data (datafication) and the ability of automatic processes to create correlations, algorithms replace the critic, the expert and ultimately our ability to judge."<sup>30</sup>

From this, it can be concluded, considering the research objective stated at the beginning of this paper, that worker profiling is only a useful tool if used cautiously and in accordance with existing legal limitations. In this way, positive selection of employees can be achieved, and a genuine contribution can be made to advancing the employer's economic interests. For example, if profiling is based on work results from the previous five years, an employer might discover that one of its employees who doesn't usually stand out, is actually the most efficient and reliable at solving complex work tasks – it's logical that the employer would want to invest further in such a professional profile, even though there's a high chance they would never have singled out that specific employee for promotion without conducting the profiling. This is also a situation where the employer can benefit from the entire concept of profiling, while the employees who are truly achieving the best results feel that their efforts are valued, and remain not only equally valuable at work but also more loyal to the employer.

Any other use of profiling inevitably leads to a violation of regulations. Even when this is not formally true – for example, when an employer gathers a range of information about an employee through social media profile research that is publicly available to everyone, including the employee – the question arises how such information can be used without breaking the legal framework of employers acting on data gathered and conclusions drawn from it. Even when they are not used or are only used in informal communication between the employer and the employee, knowing that the employer is monitoring aspects of private life that should not concern it certainly does not increase work morale, enthusiasm, or employee's loyalty – quite the opposite.

---

<sup>30</sup> E. Longo, "The Risks of Social Media Platforms for Democracy: A Call for a New Regulation", in: *Law and Artificial Intelligence - Regulating AI and Applying AI in Legal Practice, Information Technology and Law Series Volume 35* (eds. B. Custers, E. Fosch-Villaronga), Asser Press, The Hague 2022, 172–173.

**Mario Reljanović**

Institut za uporedno pravo, Beograd

## PROFILISANJE ZAPOSLENIH – ETIČKE I PRAVNE GRANICE

### *Apstrakt*

*Profilisanje zaposlenih nastalo je kao težnja poslodavca da učini proces rada što efikasnijim i svakom licu koje je angažovano dodeli najoptimalnije radne zadatke. Međutim, sa pojavom takozvane veštačke inteligencije, algoritama koji mogu obrađivati veći broj informacija u elektronskoj formi i na osnovu toga vršiti optimizaciju rada ili predikciju postupanja zaposlenih, profilisanje dobija nove dimenzije. Poslodavci vrše istraživanja koja daleko prevazilaze njihova zakonom dozvoljena interesovanja o privatnom i porodičnom životu zaposlenih, sakupljajući sve podatke koje lice ostavlja o svom digitalnom otisku, uključujući i one koji se odnose na najintimnije aspekte života. Pravljenje medicinskih i psiholoških profila tako postaje u domenu tehničke ostvarivosti za poslodavca, ali to ovu aktivnost ne čini dozvoljenom. Pravo na dostojanstvo ličnosti, kao i pravo na privatnost, ostvaruju se u procesu rada podjednako sa pravom na dostojanstven rad i pravom na razumno očekivanje privatnosti na radu. Istraživanje prati pravne i etičke aspekte profilisanja zaposlenih u uslovima savremenih komunikacija i masovne obrade informacija sa društvenih mreža, javnih i nejavnih baza podataka, ukrštajući ih sa klasičnim (i još uvek važećim) principima odnosa između poslodavca i zaposlenog, i ukazuje na rizike i opasnosti, ali i koristi korišćenja novih digitalnih alata u poslovanju.*

**Ključne reči:** *profilisanje zaposlenih, algoritamsko predviđanje, zaštita ličnih podataka zaposlenog, pravo na privatnost na radu, razumno očekivanje privatnosti na radu.*

### References

- Beadle, N. D. "A Risk Not Worth the Reward: The Stored Communications Act and Employers' Collection of Employees and Job Applicants' Social Networking Passwords", *American University Business Law Review* 2/2012, 397–412.
- Bortnick, R. "Restoring Reasonable Expectations to Privacy at Work in the Face of Modern Electronic Monitoring Practices", *UC Law Journal* 5/2024, 1479–1534.
- Diligenski, A., Prlja, D., Cerović, D. *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd 2018.

- Etus, C., Okonkwo, T. “Development of Staff Profiling and Identification System”, *International Journal of Novel Research in Computer Science and Software Engineering* 2/2022, 1–19, <https://doi.org/10.5281/zenodo.6539283>
- European Commission, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, COM(90) 314 final.
- European Court of Human Rights, *Bărbulescu v. Romania*, Application no. 61496/08, Judgment of 12. 1. 2016.
- European Court of Human Rights, *Halford v. the United Kingdom*, Application no. 20605/92, Judgment of 25. 6. 1997.
- European Court of Human Rights, *Libert v. France*, Application no. 588/13, Judgment of 22. 2. 2018.
- Golubović, D., Galetin, M. „Pregled prakse Evropskog suda za ljudska prava od značaja za obradu podataka o ličnosti putem video-nadzora”, *Strani pravni život* 1/2024, 61–81, [https://doi.org/10.56461/SPZ\\_24104KJ](https://doi.org/10.56461/SPZ_24104KJ)
- Hildebrandt, M. “Defining Profiling: A New Type of Knowledge?”, in: *Profiling the European Citizen Cross-Disciplinary Perspectives*, Springer Science (eds. M. Hildebrandt, S. Gutwirth), Business Media B.V., Houston 2008, 17–45. [https://doi.org/10.1007/978-1-4020-6914-7\\_2](https://doi.org/10.1007/978-1-4020-6914-7_2)
- Kesslen, B. 1 of every 5 job postings is actually fake, study says, <https://qz.com/one-in-five-job-postings-is-fake-ghost-jobs-1851738201>, 27. 7. 2025.
- Kluemper, D. H. “Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment”, *Selection, Social Media in Human Resources Management Advanced Series in Management*, 2013, 1–21, [https://doi.org/10.1108/S1877-6361\(2013\)0000012005](https://doi.org/10.1108/S1877-6361(2013)0000012005)
- Kovačević, T. „Izazovi digitalizacije rada i zaštite ličnih podataka”, *Strani pravni život* 2/2023, 299–320, [https://doi.org/10.56461/SPZ\\_23207KJ](https://doi.org/10.56461/SPZ_23207KJ)
- Longo, E. “The Risks of Social Media Platforms for Democracy: A Call for a New Regulation”, in: *Law and Artificial Intelligence - Regulating AI and Applying AI in Legal Practice, Information Technology and Law Series Volume 35* (eds. B. Custers, E. Fosch-Villaronga), Asser Press, The Hague 2022, 169–186, <https://doi.org/10.1007/978-94-6265-523-2>
- Malgieri, G. *Vulnerability and Data Protection Law*, Oxford University Press, 2023. <https://doi.org/10.1093/oso/9780192870339.001.0001>
- McDonald, P., Thompson, P., O'Connor, P. “Profiling employees online: shifting public-private boundaries in organisational life”, *Human Resources Management Journal* 4/2016, 541–556, <https://doi.org/10.1111/1748-8583.12121>
- Rafae, A., Erritali, M. “Using a Profiling System to Recommend Employees to Carry Out a Project”, *Electronics* 12/2023, 1–18, <https://doi.org/10.3390/electronics12163388>
- Rajić Čalić, J. „Pravo na isključivanje – između porodičnog života i profesionalnih dužnosti”, *Radno i socijalno pravo* 2/2023, 303–319.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016, 1–88.
- Reljanović, M. „Informacione tehnologije i izazovi u reformi radnog prava”, *Zbornik Pravnog fakulteta u Novom Sadu* 2/2020, 763–779, <https://doi.org/10.5937/zrpfns54-23133>
- Reljanović, M., Knežević Bojović, A. *Pravo na privatnost na radu*, Institut za uporedno pravo, Beograd 2025, [https://doi.org/10.56461/M205\\_25MR.AKB](https://doi.org/10.56461/M205_25MR.AKB)
- Reljanović, M., Misailović, J. „Radnopravni položaj digitalnih radnika”, *Strani pravni život* 3/2021, 407–432, <https://doi.org/10.5937/spz65-33727>
- The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018.
- Vereb, D., Krajcsak, Z., Kozak, A. “The importance of positive employee experience and its development through using predictive analytics”, *Journal of Modelling in Management* 1/2025, 51–69, <https://doi.org/10.1108/JM2-02-2024-0057>
- Zakon o zaštiti podataka o ličnosti, *Official Journal of the Republic of Serbia*, No. 87/2018.