

Some Comments on the Unsuitability of the General Data Protection Regulation in the Field of Employment Relations in the Context of Automated Decision-Making

Juraj Hamulák*
Andrea Kluknavská**

Summary: New technologies currently affect all human activities and are becoming a part of our everyday lives. The use of digitalisation, algorithmic management, and the withdrawal of human decision-making in various phases of working life entails many risks not only in the field of work and human resource management. Even though the rules of algorithmic management do not come only within the scope of employment law, and at the same time employment law fails to explicitly provide for proper protection of employees against damage suffered as a result of automated decision-making, this issue is partially covered within the scope of personal data protection. At the centre of our attention is the issue of the sufficiency of these rules in the field of personal data protection concerning employment law relations, including certain *de lege ferenda* suggestions.

Keywords: automated management systems, algorithmic management, GDPR

Citation: HAMULÁK, J., KLUKNAVSKÁ, A. Some Comments on the Unsuitability of the General Data Protection Regulation in the Field of Employment Relations in the Context of Automated Decision-Making. *European Studies – the Review of European law, Economics and Politic.* 2023, vol. 10, no. 2, pp. 203–220, DOI: 10.2478/eustu-2023-0018.

Acknowledgement: Preparation of the paper was supported by VEGA no 1/0091/23 “Limits of European Integration in the Slovak Constitutional Order.

* Professor of labor law at the Law Faculty, Comenius University in Bratislava. Contact: juraj.hamulak@flaw.uniba.sk

** Andrea Kluknavská is an assistant professor at the Faculty of Law, Matej Bel University in Banská Bystrica. Contact: Kluknavska.andrea@umb.sk

1. Introduction

Currently, there is probably no area of human life not affected by digitalisation, and it is no different in the world of work and human resource management. Automated decision-making systems (algorithmic management, algorithmic administration) are becoming more and more widespread and serve to make decisions that were initially reserved for human beings.

We can definitely say that automated decision-making systems are used in all phases of working life and significantly affect not only the working conditions but also the very status of employees, basically from the first moment of employment, particularly the scrutiny and evaluation of job applications and candidate resumes. At the same time, these systems facilitate the choice as to whom to invite for an interview and whom to employ for work. Subsequently, during the existence of the employment relationship, these systems assist in the assignment of tasks, monitoring, supervision, evaluation of work performance, remuneration, forecasts of future behaviour, or disciplinary measures that may lead to the termination of the employment relationship.

It is therefore obvious that these systems pose risks to employees in terms of the exercise of fundamental rights and freedoms relating to the performance of their jobs, such as the right to work, the right to protection of the health of employees, dignity, and privacy of employees.¹

There are practical issues associated with the introduction of automated artificial intelligence decision-making tools in workplaces, which intervene with the scope of several areas, including employment law, and in this context, the question here arises as to what extent is the existing legal framework at the national and European level sufficient, especially in the absence of explicit rules on algorithmic management. At the same time, this is also related to the fact that employment law also fails to explicitly provide for protection for employees against damage caused by automated management, which raises the question of whether protection provided for by the data protection legislation is currently sufficient.

2. GDPR and automated decision-making systems

Due to the massive flow of processed data in decisions made by automated systems in the performance of work and human resources management, the rights

¹ ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*, 2023, vol. 14, no. 2, p. 9. [online] Available at: <https://ssrn.com/abstract=4417954>

vested in employees partially overlap with the safeguards under 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 (the “GDPR”). The GDPR also fully applies to automated decision-making systems.

In addition to the universal rules governing the processing of personal data, such as the right to information, and access to data, including data protection impact assessment², the Regulation also contains one specific rule laid down in Article 22 of the Regulation.³ This provision also applies to automated individual decision-making, including profiling, which on the one hand is considered the most important safeguard against harm caused by algorithmic control, but on the other hand is considered the most complex and controversial provision in theory and practice⁴, particularly since it stipulates that high-risk decisions should be made by humans and not algorithms.

2.1. Right to ex-ante and ex-post personal data control

The objective of the GDPR is that these rules provide employees, being data subjects in this context, with control over their personal data and to provide sufficient

² See also VARDANYAN, L., KOCHARYAN, H., HAMULÁK, O., MESARČÍK, M., KERIK-MÁE, T., KOOKMAA, T. The Unwanted Paradoxes Of the Right to Be Forgotten. *Masaryk University Journal of Law and Technology*. 2023, vol. 17, no. 1, pp. 87–109. ISSN 1802-5943. DOI 10.5817/MUJLT2023-1-3.

³ Pursuant to this provision, a) 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.

b) Paragraph 1 shall not apply if the decision:

- a. is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - b. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
 - c. is based on the data subject’s explicit consent.
- c) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
- d) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

⁴ ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*. 2023, vol. 14, no. 2, p. 9. [online] Available at: [https:// https://ssrn.com/abstract=4417954](https://ssrn.com/abstract=4417954)

and strict requirements for transparency and accountability in the processing of personal data by employers.

Employees must be informed prior to the processing of their personal data,⁵ while the decisive factor in complying with this requirement is both the content of the information, i.e., which is the matter of categories and sources of information to be provided to employees as well as the time frame for providing the information, and finally, how the information must be provided. With regard to this duty, we must take into account the fact that employers currently obtain information about employees from various sources, not only from delivered resumes but also from social media, former employers, or recruitment agencies.

Coming back to the time frame for providing information when complying with the information duty, the GDPR does not stipulate a uniform rule, because it takes into account different requirements depending on the purpose of processing of individual data, depending on whether the processed data is obtained directly from the employee because then the information must be provided at the time when the personal data is collected,⁶ or whether the information comes from other sources such as social networks or employment agencies and others, because then the information must be provided “within a reasonable period” after obtaining the personal data, but no later than within one month.⁷

The last requirement of the information duty is the method of providing information to the employee, which according to Article 12 of the GDPR should be “*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*”. The GDPR thus fails to specify the precise manner in which the employer must comply with its information duty towards the employee, and, on the contrary, it allows the employer to “take measures” that will meet the requirements of the legislation and at the same time correspond to the actual circumstances of data processing.

The right of access to personal data by the data subject also enables employees to control their data. According to Art. 15 of the GDPR, the data subject, i.e. the employee, shall have the right to obtain from the controller, which is the employer, confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data, and if so, he or she shall have the right to obtain access to this personal data, whereas point (h) of this provision applies directly to automated decision-making systems. According to this provision, employees have the right to know about the existence of automated decision-making, including profiling, and in these cases,

⁵ See Articles 12 to 14 of the GDPR.

⁶ Article 13(1) of the GDPR.

⁷ Point (a) of Article 14(3) of the GDPR.

they have the right to at least meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.⁸ Therefore, employees have the right to know about the existence and to at least basic information on how algorithmic management is used.

The right of access to data applies only when is exercised by the employee, which means that the employee may rely on this right at any time within a reasonable time interval being different from the information duty, which requires that information be provided at a specified time and by way of appropriate means.

The right of access to data provided for in point (h) of Art. 15(1), however, raises several questions mainly associated with the lack of clarity as to the scope of the information, because when interpreting the requirement for “meaningful information about the logic involved, as well as the significance and the envisaged consequences”, we may encounter a problem that can lead to legal uncertainty when this requirement as such is applied. What we may consider as “meaningful information” we can interpret as an explanation of a specific algorithmic decision, and as suggested by the academic literature, we should at all times interpret this requirement in connection with the principle of transparency?⁹

Transparency, according to point (a) of Article 5(1) of the GDPR, includes both a prospective and a retrospective element.¹⁰ First, prospective transparency means that individuals must be informed of ongoing data processing before such processing takes place and is therefore related to the information duties under the GDPR, whereas under the Data Protection Act prospective transparency requires data controllers (i.e., any organization processing the personal data) to inform data subjects (i.e., the individuals to whom the personal data belong) concisely and in an easily accessible, easy understandable and clear and plain language (and, where appropriate, with visualization).¹¹ Such information must be provided in writing or, where appropriate, by electronic means, and the information must be provided in an intelligible and easily accessible form.¹² The legislation requires data controllers to provide information about themselves (who), the amount and quality of data processed (how), the time (framework) of processing activities (when), the ground (why), and the purpose of data

⁸ Point (h) of Article 15(1) of the GDPR.

⁹ SELBST, D. A., POWELS, J. Meaningful Information and the Right to Explanation. *International Data Privacy Law*. 2017, vol. 7, no. 4, p. 234. [online] Available at: <https://ssrn.com/abstract=3039125>

¹⁰ FELZMANN, H., VILLARONGA FOSCH, E. LUTZ, Ch., TAMÓ-LARRIEUX, A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*. 2019, vol. 6, no. 1, pp. 1–14 [online]. Available at: <https://doi.org/10.1177/2053951719860542>

¹¹ Recitals 39 and 58 of the GDPR.

¹² See Article 12 of the GDPR.

processing (what for).¹³ The retrospective element of transparency refers to the possibility to trace back how and why a particular decision was made.

Recital 71 of the GDPR emphasizes that the data subject has “*the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*”.

From the above, we can conclude that information on automated management systems may be considered meaningful if it helps employees understand how their personal data is processed and enables employees to exercise their rights. Therefore, it will certainly not be considered meaningful information where the employer provides employees with information on algorithmic management, but such information will be too general or, on the contrary, too detailed, which will certainly not achieve the objective of the legislation, and therefore in this context the EDBP explained that “the information provided should be sufficiently comprehensive, so that the data subject, in our case the employee, understands the grounds for the algorithmic decision”.¹⁴

Other questions are raised by the right to access data according to point (h) of Art. 15(1) in the context of restrictions on the right of access, because employers can both restrict or refuse the right of access if it is necessary to protect the rights and freedoms of others, trade secrets, as well as use the exception of intellectual property in the terms of Recital 63 of the GDPR. In practice, this could mean that employers will not provide information to employees because they may have concerns that such information may get easier to their competitors. Similarly, the protection of trade secrets, e.g. regarding information systems, could be subject to such protection, as well as the results of the employees’ work as these may contain information that may be subject to either intellectual property protection, or trade secret.

The employer may also refuse the employee’s request for access to the data if, according to Article 12(5) of the GDPR, the data is excessive and may require the employee to specify the required data.¹⁵ In the context of the above, Abraha

¹³ FELZMANN, H., VILLARONGA FOSCH, E. LUTZ, Ch., TAMÓ-LARRIEUX, A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*. 2019, vol. 6, no. 1, pp. 1–14 [online]. Available at: <https://doi.org/10.1177/2053951719860542>. Recitals 39 and 58 of the GDPR.

¹⁴ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). [online] Available at: <https://ec.europa.eu/newsroom/article29/items/612053>

¹⁵ Indeed, Recital 63 of the GDPR allows employers to ask employees requesting access to data to specify that data. As a practical example the case of the Uber drivers’ dispute with Uber, where the company referred to Recital 63 of the GDPR, and subsequently the District Court of Amsterdam agreed with Uber and dismissed the request for the right of access because it was

rightly observes that the specification requirement assumes that employees are aware of all categories of personal data collected by employers, however, experience has shown quite the opposite as employees often do not know much at all about the personal data that their employers process.¹⁶ So the question remains, would it be right and fair to demand this from employees? We tend to share the view that requiring any specifications from employees, provided that they are unfamiliar with personal data and processing activities due to various reasons, would be contrary to the purpose of the right to access data under the GDPR.

2.2. Specificity of automated individual decision-making

So, what is the complexity and controversy of automated individual decision-making, including profiling? The fundamental problem that gives rise to the problem of application of this legislation in practice is the wording stating that the employee must not be the subject of a decision based solely on the automated processing of personal data.

In terms of the Recitals¹⁷, the data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing, and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of recruitment of employees without any human intervention. Such processing includes profiling that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

This was also confirmed by the Data Protection Working Party established by Article 29 (currently renamed the European Data Protection Board – the EDPB) (hereinafter referred to as the “EDPB”) that in its guidelines explained that *“the controller cannot avoid the Article 22 provisions by fabricating human*

too general and did not sufficiently specify the data requested. For more details, please see the Judgement of the District Court of Amsterdam. [online] Available at: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1020>

¹⁶ ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*. 2023, vol. 14, no. 2, p. 8. [online] Available at: <https://ssrn.com/abstract=4417954>

¹⁷ For more details see 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 (GDPR). [online] Available at: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32016R0679>

*involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data”.*¹⁸

In other words, a *pro forma* human validation (in technical jargon called *rubber stamping*)¹⁹ must not serve to deny the fact that the decision comes within the scope of an automated decision-making system.

Certainly, questions immediately arise here as to what a meaningful human contribution is, or in which phase of the decision-making process the human involvement is required. Briefly, any acting person should be able to independently assess the case and evaluate the outputs of the system, and not just nod to them without thinking. Such a person should have the authority to override automated outputs and consider additional information and mitigating factors.²⁰

It is necessary to draw attention here to one more very important aspect, pointed out by Aloisi, who in the context of “the right to human intervention” reminds us that it is not clear who the “human” should be and whether he or she will be able to examine the process that could have been based on third-party algorithms, pre-learned models or datasets, including other personal data of other persons, or incomprehensible machine learning models. It is not even clear that the person charged with reviewing the decision may be the same person who made the decision first as this person may be still subject to the same conscious or subconscious biases and prejudices in relation to the data subject as before.

Therefore, it follows from the above that profiling takes place when the employee’s personal qualities are evaluated in particular to create forecasts, even when no decision is made. For example, if a company or an organization assesses the qualities of an employee or assigns an employee to a certain category. Decision-making based solely on automation takes place when decisions about an employee are made using technology without any human intervention. These

¹⁸ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). [online] Available at: <https://ec.europa.eu/newsroom/article29/items/612053>

¹⁹ ALOISI, A., POTOCKA-SIONEK, N. De-gigging the labour market? An analysis of the ‘algorithmic management’ provisions in the proposed Platform Work Directive. *Italian Labour Law e-Journal*, 2022, vol. 15, no. 1, p. 39. [online] Available at: <https://illeg.unibo.it/article/view/15027>

²⁰ BINNS, R, VEALE, M. Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR. *International Data Privacy Law*, 2021, vol. 11, no. 4, p. 320. [online] Available at: https://www.researchgate.net/publication/355575981_Is_That_Your_Final_Decision_Multi-Stage_Profiling_Selective_Effects_and_Article_22_of_the_GDPR

decisions may be made even without profiling. The right not to be subject to decision-making based solely on automation therefore applies to all decisions that would lead to any legal effects, which could affect legal rights.

In this context, the stakeholders get no benefit from the ambiguous wording of paragraph 1 either, i.e., as to whether it means an absolute prohibition of automated decision-making, or whether the data subject has any right to object thereto. Each interpretation has different effects not only on the parties to employment relationships but also on the procedures of the personal data supervisory authority.

In this context, the EDPB provides guidance stating that *“the term ‘right’ in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data”*.²¹

This interpretation and the reasoning of the EDPB reinforces the argument that the data subject has control over his or her personal data, which is in line with the fundamental principles of the GDPR and that Article 22 of the GDPR should be construed as a prohibition rather than a right to be exercised and at the same time that individuals (in our case, the employees) shall automatically enjoy protection against any potential effects that such data processing may cause. On this basis, it can be concluded that data processing according to Article 22(1) of the GDPR is generally not permitted.

However, it is worth drawing attention to the counter-argument of Tosoni, who is convinced, in terms of linguistic, contextual, systematic, and teleological interpretation, that the GDPR actually confers on data subjects a right that they may exercise at their own discretion.²² At the same time, however, he realizes that if we were to understand the provision of Art. 22 of the GDPR as a right and not as a prohibition, it may be difficult to obtain the support of stakeholders for his claims as these contradict the guidelines as cited above.²³

Based on the above it can be concluded that the provision of Article 22 of the GDPR is both very vaguely worded and subject to several exceptions which complicate and undermine the practical effectiveness of the provision.

²¹ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). [online] Available at: <https://ec.europa.eu/newsroom/article29/items/612053>

²² TOSONI, L. The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*. 2021, vol. 11, no. 2, pp. 145–162. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3845913.

²³ Ibid.

2.3. Exceptions undermining the effectiveness of Article 22 of the GDPR

As we mentioned above, in addition to the fact that the wording of Article 22 of the GDPR is rather vague, it is also subject to several exceptions that can make the positive effect for the employee toothless. The absolute prohibition is relativized, in particular, by three exceptions according to Article 22(2) of the GDPR pursuant to which the data subject fails to have the right not to be subject to a decision that is based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. These include cases where the decision is based solely on automation significantly affecting employees is justified because it is necessary for entering into, or performing of a contract between the data subject and a data controller; or where the decision is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or where such decision is based on the data subject's explicit consent.²⁴

In connection with the performance of dependent work, the legal ground of (pre)contractual necessity is particularly relevant if there are no other effective and less intrusive means to achieve the same objective. It is for this ground that employers usually rely on when introducing automated decision-making systems, for example, where the employer processes a huge amount of data from job applicants.

In this context, the EDPB also uses as a model example a situation where routine human intervention may be impractical or impossible due to the amount of data being processed: *“A business advertises an open position. As working for the business in question is popular, the business receives tens of thousands of applications. Due to the exceptionally high volume of applications, the business may find that it is not practically possible to identify fitting candidates without first using fully automated means to sift out irrelevant applications. In this case, automated decision-making may be necessary in order to make a short list of possible candidates, with the intention of entering into a contract with a data subject.”*²⁵ Thus, in such a case, an employer processing a large amount of data about job applicants would use the contractual necessity exception to justify fully automated screening of job applicants.

²⁴ For more details see Art. 22(2) of the GDPR.

²⁵ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). [online] Available at: <https://ec.europa.eu/newsroom/article29/items/612053>

Some EU Member States have deviated from the above opinion of the EDBP, such as the Baden-Wuerttemberg State Commissioner for Data Protection and Freedom of Information (*Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg*) in the Federal Republic of Germany, that has taken a completely opposite position stating in its Annual Report that automated language analysis of written expressions (resumes, motivation letters) of job applicants that decide with whom to continue the recruitment process may only be carried out with the prior consent of these job applicants. As the State Commissioner rightly states, the application of such a procedure in practice is problematic because of the applicants' fears that if they do not give their consent, they would not be considered further, and therefore the State Commissioner calls on the voluntary nature of the consent²⁶, the meaning of which is then more than questionable if the job applicant gives his or her consent due to his or her concerns of being excluded from the recruitment process.

Regarding the legal concept of the explicit consent of the data subject, this is an exception that raises doubts about the sufficient protection of the weaker party to the contract. Even though simple consent is insufficient, and explicit consent is required, this is a relatively easy way to circumvent the prohibition on deploying automated decision-making systems, as it is not difficult for the employer to obtain consent, even an explicit one. The EU legislature adopted the derogation as mentioned above even though, given the nature of the employment relationship, the employee is generally not in a position to freely give consent, refuse to give it, or revoke it.

At the same time, it is also necessary to draw attention to the fact that explicit consent is also not suitable because algorithms are inherently non-transparent in terms of their function and design or because, even if they are transparent, they may not be comprehensible to the data subject,²⁷ which may also be deemed as making it more difficult to protect the employee as the weaker party.

Therefore, if the employer relies on the exception of contractual necessity or explicit consent to justify the use of fully automated decision-making with a significant impact on employees, the employer shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Although having this list of

²⁶ Tätigkeitsbericht Datenschutz 2020, p. 106. [online] Available at :https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_20_20_WEB.pdf

²⁷ KAMARINOU, D., MILLARD, Ch., SINGH, J. Machine Learning with Personal Data. *Queen Mary School of Law Legal Studies Research Paper*, 2016, no. 247, p. 15. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811

rights, it is still not well determined how to apply them directly in practice, for example in a situation where the employer uses algorithmic decision-making, but the system is developed, provided, and controlled by a third party. Likewise, the requirement of meaningful human evaluation raises many questions about how to ensure that it does not remain only at the level of formality, or when human intervention should take place and at each stage of processing.²⁸

Last but not least, we would also like to draw attention to the consistency of the data protection impact assessment, which is associated with the information duty as discussed in more detail above, and which is based on the requirement for employee involvement and prior consultation with the relevant supervisory authority, however, the proper implementation of the impact assessment on the part of the employees is limited, because their opinion should be taken into account only when necessary.

This limitation, along with the fact that the employer has no obligation to disclose the results of the data protection impact assessment, means that the position and role of the employees, or employee representatives is very weakened. The employer shall consult the supervisory authority before processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.²⁹ The aforementioned provision could pave the way to independent control of the use of algorithmic interests, which is, however, weakened and problematic in practice because the employer should request the supervisory authority for a prior consultation only if the employer cannot find sufficient measures to mitigate the risk. However, which criteria or risks should be considered is not precisely defined and this decision is left to the employer. The second aspect, complicating the independence of control and the effective use of the provision in question, is associated with the fact that even if the employer decides to consult with the relevant supervisory authority, it does not mean the success of solving or mitigating the excessive risk. The supervisory authorities of the Member States, and it is no different even in the Slovak Republic, do not have sufficient resources, and professional and technical knowledge, and often the GDPR enforcement agenda in workplaces is not their “priority.”

Therefore, we can certainly say that despite the importance of data protection in the field of employment law and in general in the field of human resource management, the legislation under the GDPR is not entirely suitable for this extensive area.

²⁸ See more in ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*. 2023, vol. 14, no. 2, p. 8. [online] Available at: <https://ssrn.com/abstract=4417954>

²⁹ Article 35 of the GDPR.

3. The problematic nature of the GDPR application to employment law and human resource management

3.1. Fragmentation of legislation at Member States level

The GDPR allows to deviate from the prohibition under Article 22 at national level by adopting a special legislation. The Slovak Republic, just like most of the Member States, did not make use of this option and implemented Article 22 of the Regulation verbatim. Only nine Member States in their national laws make use of the option to deviate from the provisions of the GDPR with regard to automated decision-making and adopted special exceptions under point (b) of Article 22(2) of the GDPR. These Member States are Belgium, the Netherlands, France, Germany, Hungary, Slovenia, Austria, the United Kingdom, and Ireland. This deviation can also be seen as problematic, as in individual Member States it naturally leads to different degrees of protection³⁰ in the relevant area.

In the context of the above, it should be emphasized that where a Member State allows algorithmic management, there would be no catalogue of rights available for the employee (the right to obtain human intervention, to express his or her point of view, to challenge the decision). To ensure the protection of the rights and freedoms and legitimate interests of the data subject, national legislation must take appropriate measures. However, the GDPR itself fails to explain what measures should be taken (this is discussed in more detail in the text above).

Some scope for different solutions when processing personal data in the context of employment is also provided by the little used Article 88 of the GDPR³¹, which, while respecting national particularities, is to ensure adequate protection of employees by enabling Member States either by law or by collective agreements to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment

³⁰ The approaches and even the specific safeguards proposed are very diverse among the above nine Member States. See more on the topic above in MALGIERI, G. Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations. *Computer Law & Security Review*, 2019, vol. 35, no. 5, pp. 1–26. [online] Available at: <https://www.sciencedirect.com/science/article/pii/S0267364918303753>

³¹ From legal perspective, this provision also paves the way for social partners, who can also play a key role in preventing the risks of algorithmic human resource management. Collective bargaining appears to be the most effective tool taking into account how quickly new technologies are being developed and introduced in workplaces. See more In: DE STEFANO, V. Master and Servers: Collective Labour Rights and Private Government in the Contemporary World of Work. *International Journal of Comparative Labour Law and Industrial Relations*. 2020, vol. 36, no. 4, p. 442. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3675082.

context, in particular for the purposes of recruitment, performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

At the same time, these rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests, and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in joint economic activity and monitoring systems in workplaces.

The purpose of this provision was to ensure adequate and consistent protection of employees, taking into account regulatory diversity and respecting national particularities as well as the protection of the autonomy of Member States. In this context there is a question of whether this clause has met this intended and ambitious purpose. In this context, Abraha argues that although the compromise sought by the clause has fulfilled some of its promises, he adds that while promoting diverse and innovative regulatory approaches, Article 88 produces further legislative fragmentation, legal uncertainty, and inconsistent implementation, which may lead to inconsistent interpretation and enforcement of data protection rules.³²

3.2. Concept of explicit consent of the employee

The concept of explicit consent of the employee represents an exception that raises doubts about the sufficient protection of the weaker party to the contract. The employee-employer relationship is a relationship defined by power, which logically casts doubt on the suitability of the employee's consent as a legal ground in the context of the protection of personal data. In order for us to consider consent as a legal ground, two fundamental requirements have to be complied with, namely that the data subject must have adequate information and must understand the processing, and also must be able to give his or her consent. If we examine these requirements more carefully in the context of employment law, these requirements cannot be applied. Despite this fact and given the nature of the employment relationship, the EU legislature adopted the derogation as well as the requirement that simple consent of the employee is not enough and

³² See also ABRAHA, A. A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law*. 2022, vol. 12, no. 4, pp. 276–296. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198067

explicit consent is required, although it is a relatively easy way to circumvent the prohibition on deploying automated decision-making systems, since for the employer it is not difficult to obtain consent, even explicit, and the employee is not in a position to freely express consent, refuse to give it or revoke it.³³

At the same time, it is also necessary to point out that explicit consent is not suitable either because algorithms are inherently non-transparent in terms of their function and design or because, even if they are transparent, they may not be comprehensible to the data subject,³⁴ which may also be deemed as making it more difficult to protect the employee as the weaker party, which prompts us to conclude that Article 22 of the GDPR fails to provide appropriate protection for employees.

3.3. The individualistic nature of the GDPR in the context of privacy harm

The current wording of the GDPR construes damage in the context of privacy harm on an individual basis only, i.e. it fails to recognize any collective or social protection of data and privacy harm, which is typical for employment relations. Unfortunately, information and power asymmetry in employment relations may not be addressed on an individual level, because any collective damage requires a collective response,³⁵ which, however, the GDPR fails to reflect.

The use of automated systems and the regulation of personal data in this field assumes that any invasion of privacy affects an individual. Artificial intelligence³⁶, however, grows ever more sophisticated and increasingly empha-

³³ Ibid., p. 13.

³⁴ KAMARINOU, D., MILLARD, Ch., SINGH, J. Machine Learning with Personal Data. *Queen Mary School of Law Legal Studies Research Paper*, 2016, no. 247, p. 15. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811.

³⁵ ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*. 2023, vol. 14, no. 2, p. 14. [online] Available at: <https://ssrn.com/abstract=4417954>

³⁶ The use of automated systems and the high risk of artificial intelligence systems in the field of human resources is also highlighted by the Draft Regulation of the European Parliament and the Council, which is set to establish harmonized rules in the field of artificial intelligence (Artificial Intelligence Act), according to which artificial intelligence systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects and livelihoods of these persons. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. Artificial intelligence systems used to monitor the performance and behaviour of these persons may also impact their rights to

sizes the unbalanced position of the parties to the employment relationship. Employees may not even be aware of the involvement of artificial intelligence in management. And even if they learn about it, they have very little chance of understanding its functioning, which means that they cannot effectively use their rights guaranteed by the GDPR. Finally, the exercise of individual rights may be associated with the fear of retaliation by the employer.

4. Some final suggestions

It is evident from the text above that the use of automated management in the field of employment relations in the area of data protection is not sufficient and, at the same time, gives rise to a strong demand for modification that would correspond to current requirements. However, the path to achieving such change seems to be challenging due to the nature and quality of the legislation and the subsequent fragmentation of the legislation concerning some Member States.

The most preferred way would be the adoption of a new legislation at EU level, which would focus primarily on algorithmic management, either by adopting a new special directive or supplementing existing directives or using the upcoming directive on platform work. Such legislation should include, in particular, rules on the regime of algorithmic transparency, the collective right to information, the adoption of a new regime for impact assessment or exclusion of consent as a legal ground in algorithmic management as well as rules on the responsibility of new entities such as employee representatives.

The second option could be the initiative of Member States in this area to adopt rules on special protection of personal data in the context of Article 88 of the GDPR, which is little used today. A significant shift in this area could eventually be made by collective agreements as the result of collective bargaining of social partners, which would be able to respond quickly and effectively to

data protection and privacy. The significance and importance of this provision is complemented by a list of high-risk artificial intelligence systems for the field of employment, workers management and access to self-employment, which should include artificial intelligence systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests as well as artificial intelligence intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behaviour of persons in such relationships. See more about the Draft Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (Artificial Intelligence Act) [online] Available at: <https://eur-lex.europa.eu/legal-content/SK/TEXT/?uri=CELEX%3A52021PC0206>

changes in new technologies, the importance of which is not forgotten by Article 88 of the GDPR.

A possible solution for meeting the requirements in the area of assessment of data protection rules to strengthen transparency, traceability, and awareness could be the invitation of employee representatives (trade unions and employee representatives) to participate in the process of implementation and changes related to automated systems. The employer should mandatorily consult on specific settings and parameters of algorithms that may affect access to employment, working conditions, or maintenance of job positions. The Real Decreto-ley 9/2021 of 11 May 2021 could serve as a model case being the result of an agreement between the Spanish government, representatives of employees, and employers, in which the Spanish lawmaker seeks to clarify that new technological solutions – digital algorithms and platforms – are simply a means of the pursuit of economic activity, and therefore people providing services within the scope thereof, should be considered as employees.³⁷

Finally, regarding the issue of the involvement of social partners again, optional codes of conduct could also play a role in the protection of personal data in employment relations in connection with algorithmic management,³⁸ which could identify significant risks, assess the origin, nature, likelihood, and severity of the risks, and lay down procedures to mitigate those risks as best as possible.

Therefore, we believe that there is a number of possible ways that could be used in connection with the use of algorithmic decision-making, not only in the field of employment and human resource management but if we think about the time frame of any new legislation, we are sceptical, particularly due to the complexity and difficulty of adopting the Data Protection Regulation or in the context of non-use of Article 88 of the Regulation by Member States. We also believe that even if one of the ways means the adoption of rules of a non-legislative nature, for example using ethical codes, probably such rules may not be sufficient and efficient in the long term.

List of references

ALOISI, A., POTOCKA-SIONEK, N. De-gigging the labour market? An analysis of the ‘algorithmic management’ provisions in the proposed Platform Work Directive. *Italian*

³⁷ See more in TODOLÍ-SIGNES, A. Spanish riders law and the right to be informed about the algorithm. In *European Labour Law Journal*. 1-4, 2021. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916688

³⁸ ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*. 2023, vol. 14, no. 2, p. 8. [online] Available at: <https://ssrn.com/abstract=4417954>

- Labour Law*. e-Journal, 2022, vol. 15, no. 1. [online] Available at: <https://illej.unibo.it/article/view/15027>
- ABRAHA, A. A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law*. 2022, vol. 12, no. 4, pp. 276–296. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198067
- ABRAHA, H. Regulating Algorithmic Employment Decisions through Data Protection Law. *European Labour Law Journal*. 2023, vol. 14, no. 2. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4417954
- BINNS, R, VEALE, M. Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR. *International Data Privacy Law*, 2021, vol. 11, no. 4. [online] Available at: https://www.researchgate.net/publication/355575981_Is_That_Your_Final_Decision_Multi-Stage_Profiling_Selective_Effects_and_Article_22_of_the_GDPR
- DE STEFANO, V. Master and Servers: Collective Labour Rights and Private Government in the Contemporary World of Work. *International Journal of Comparative Labour Law and Industrial Relations*. 2020, vol. 36, no. 4. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3675082.
- FELZMANN, H., VILLARONGA FOSCH, E. LUTZ, Ch., TAMÓ-LARRIEUX, A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*. 2019, vol. 6, no. 1, pp. 1–14. [online] Available at: <https://doi.org/10.1177/2053951719860542>
- KAMARINOU, D., MILLARD, Ch., SINGH, J. Machine Learning with Personal Data. *Queen Mary School of Law Legal Studies Research Paper*. 2016, no. 247. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811
- MALGIERI, G. Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations. *Computer Law & Security Review*. 2019, vol. 35, no. 5, pp. 12–26. [online] Available at: <https://www.sciencedirect.com/science/article/pii/S0267364918303753>
- SELBST, D. A., POWELS, J. Meaningful Information and the Right to Explanation. *International Data Privacy Law*. 2017, vol. 7, no. 4, p. 233–242. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125
- TODOLÍ-SIGNES, A. Spanish riders law and the right to be informed about the algorithm. In *European Labour Law Journal* 1–4, 2021. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916688
- TOSONI, L. The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*. 2021, vol. 11, no. 2, pp. 145–162. [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3845913.
- VARDANYAN, L., KOCHARYAN, H., HAMULÁK, O., MESARČÍK, M., KERIK-MÁE, T., KOOKMAA, T. The Unwanted Paradoxes Of the Right to Be Forgotten. *Masaryk University Journal of Law and Technology*. 2023, vol. 17, no. 1, pp. 87–109. ISSN 1802-5943. DOI 10.5817/MUJLT2023-1-3.