

ILDAR BEGISHEV

Doctor of Legal Sciences, Associate Professor, Chief Researcher, Research Institute of Digital Technologies and Law, Professor, Department of Criminal Law and Process, Kazan Innovative University named after V.G. Timiryasov, Honored Lawyer of the Republic of Tatarstan

IRINA FILIPOVA

Candidate of Legal Sciences, Associate Professor, Department of Labour and Environmental Law, Lobachevsky State University of Nizhny Novgorod

**PROTECTION OF EMPLOYEES' PERSONAL DATA
IN THE CONTEXT OF THE SPREAD OF ALGORITHMIC MANAGEMENT
(BASED ON COURT PRACTICE)**

DOI: 10.30729/2541-8823-2025-10-4-190-212

Abstract. *The importance of employees' personal data, the protection of which is provided for by current legislation, is changing in the context of the current transformation of labour relations. This is due to the spread of digital technologies, primarily artificial intelligence technologies and products based on them, the efficiency of which directly depends on access to gigantic volumes of data. Employers are increasingly introducing digital technologies into the workplace, which means that the confidentiality of employees' personal data is exposed to additional, previously absent risks, as evidenced by the increasingly extensive case law on this issue. One of the most significant changes made in recent years in the management of production processes is algorithmic management. It is built primarily on the work of artificial intelligence systems that collect numerous data, analyse it, and actually make many decisions for the employer or significantly facilitate their adoption with the intellectual support. Algorithmic management allows for the optimisation of management, including personnel management, but increases the risks of leakage or misuse of information*

required for the operation of artificial intelligence systems, threatening the privacy of employees, which in the long term may become a fairly common cause of labour disputes. A study of existing judicial practice makes it possible to more accurately identify gaps and shortcomings in legal regulation that need to be eliminated, including those that hinder the administration of justice in resolving disputes concerning the processing of employees' personal data by employers.

Keywords: *personal data, biometrics, employee, right to privacy, employer, algorithmic management, artificial intelligence, labour dispute*

1. Introduction

The question of protecting employees' personal data, access to which employers obtain by virtue of the existence of an employment relationship, has traditionally attracted research interest among labour law specialists¹, who note the vulnerable position of employees and the important role of the developing case law on this issue, which plays a key role in interpreting the law. This topic becomes even more acute owing to the ongoing digitalization and intelligent automation of the sphere of labour, which heightens the risks of violations of employees' rights to privacy (confidentiality) and to the protection of personal data, as noted in their studies by both Russian² and foreign legal scholars³. Courts are already hearing disputes concerning improper processing by employers of employees' personal data using artificial intelligence, since an employer's deployment of such digital technologies substantially strengthens the employer's position as a party to the employment relationship in comparison with the other party — the employee, who is already the “weaker” party in labour relations. Familiarization with court decisions that have been handed down makes it possible to improve the accuracy of conclusions as to the direction in which the legal regulation of the protection of employees' data will further develop. In rendering decisions on the abovementioned issue, Russian courts rely, first and foremost, on the provisions of two regulatory legal acts — Federal Law No. 152-FZ “On Personal Data” of 27 July 2006 (hereinafter — the Personal Data Law) and the Labour Code of the Russian Federation (Chapter 14). In addition, the position of a specially established executive authority — the Federal Service

¹ Berezhnov A.A. (2024). Problemy zashchity personalnykh dannykh rabotnikov na sovremennom etape // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 3. Pp. 8–13.

² Filyushchenko L.I. (2024). Tsifrovoy profil rabotnika: problemy zashchity personalnykh dannykh // Zakony Rossii: opyt, analiz, praktika = Laws of Russia: experience, analysis, practice, 1. Pp. 28–37.

³ Abraha H. (2023). Regulating algorithmic employment decisions through data protection law // European Labour Law Journal, 14(2). Pp. 172–191. (In English); De Stefano V. (2020). “Masters and Servers”: Collective Labour Rights and Private Government in the Contemporary World of Work // International Journal of Comparative Labour Law and Industrial Relations, 36(4). Pp. 425–442.

for Supervision in the Sphere of Communications, Information Technologies and Mass Communications (hereinafter — Roskomnadzor) — is also taken into account. Similar legislation exists in foreign jurisdictions as well. The issue under consideration also affects the administration of justice; for example, British researchers note that the online publication of court decisions in employment disputes in the United Kingdom significantly facilitates employers' automated search for the names of job applicants among those listed as claimants, followed by the inclusion of such persons on "blacklists"¹. As can be seen, problems with the protection of employees' personal data are cross-border in nature and require further study in order to choose a strategy for the future development of legislation and law enforcement in connection with the progressively increasing spread of algorithmic management and artificial intelligence systems (hereinafter — AI systems) in the sphere of labour. This is also confirmed by the discussion of these matters at the level of the International Labour Organization².

2. Employees' personal data: concept, composition and significance

Pursuant to the Personal Data Law, personal data includes any information that allows one to identify directly or indirectly a specific natural person, who, in turn, is called the data subject. Personal data is similarly understood by the General Data Protection Regulation (hereinafter — GDPR) of the European Union (hereinafter — EU), to which reference will need to be made repeatedly in the course of comparison, owing to the fact that the said regulatory act is considered the exemplar of regulation in the relevant field, and many of its provisions have been borrowed by regulatory acts subsequently adopted in various countries of the world.

Personal data may be divided into the following groups:

1) general personal data (surname, first name, patronymic, passport data, etc.), section 1 of Article 3 of the Personal Data Law;

2) special data (racial or ethnic origin, political views, religious or philosophical beliefs, health status, intimate life, criminal record), sections 1 and 3 of Article 10 of the Personal Data Law;

3) biometric data—information characterizing physiological features of a human being that allows one to establish his or her identity (photograph, voice, iris, etc.), Article 11 of the Personal Data Law;

4) other data (affiliation to a certain social group, etc.).

An employee's personal data were initially defined by the Labour Code of the Russian Federation as information necessary to the employer in connection with

¹ Adams Z., Adams-Prassl A., Adams-Prassl J. (2022). Online tribunal judgments and the limits of open justice // *Legal Studies*, 42(1). Pp. 42.

² Hendrickx F. (2022). Protection of workers' personal data: General principles // ILO Working Paper 62. Geneva: ILO. Pp. 5.

the employment relationship and concerning a specific employee, but in 2013 Article 85 of the Labour Code of the Russian Federation, which contained this definition, was repealed. On the basis of the provisions of the Personal Data Law, it is possible to designate as an employee's personal data any information directly or indirectly relating to a specific employee that is processed by an employer within the framework of labour relations.

An employee's personal data may be information included in any of the four groups listed above; it is typically contained in questionnaires completed by employees or job applicants (i.e., persons applying for a job), in employment contracts, in labour books, in payslips, in payroll documents, in photographs of employees, in documents presented by employees upon conclusion of an employment contract, and so on. The law does not provide a closed list of such data. The list of personal data required by the employer is approved by each employer independently and may differ depending on the characteristics of the work and the sphere in which the person works. It should be noted that in Section 10 of the Ruling of the Plenum of the Supreme Court of the Russian Federation of 17 March 2004 No. 2 "On the Application by the Courts of the Russian Federation of the Labour Code of the Russian Federation", emphasis is placed on the absence of any restrictions on employers in choosing a method for assessing the business qualities of a job candidate. "The criteria determining these qualities are not exhaustive, which actually gives employers the right, at their discretion, to use any assessment tools, including systems based on artificial intelligence"¹.

General personal data of an employee may include basic identification data contained in a passport, taxpayer identification number, social insurance number, military records, and may also include:

- employment and biographical information (education, qualifications, work experience, information on previous places of employment and other data from the labour book, position, details of the employment contract, salary—reference to the fact that information about salary is personal data may be found in a letter from Roskomnadzor of 7 February 2014 No. 08KM-3681);

- contact and address data (address of registration and residence, telephone, email address, if the latter can be directly linked to a specific natural person (contains name and surname) or indirectly, when it can be linked to a specific person in the presence of additional information such as a login, and conversely, if an email address is depersonalized, it will not be recognized as personal data; the same applies to telephone numbers);

- information about marital status required by the employer for income tax withholdings.

¹ *Kiyamova D.I. (2025). Iskusstvennyy intellekt v rekrutinge: zashchita personalnykh dannykh i predotvrashchenie diskriminatsii v tsifrovuyu epokhu // Kadrovik = HR Manager, 5. Pp. 61.*

An employee's special data may include:

- health status (information on medical examinations, chronic diseases, disability status);

- trade union membership;

- religious affiliation and nationality.

Biometric data of an employee will be recognized when:

- a photograph is used (for a questionnaire, issuance of a pass, or identification document);

- fingerprints, voice, or facial scan are used (if they are required, in particular, for an access control system).

Other data related to employment activities may include:

- disciplinary penalties;

- materials from official investigations;

- information about access to information systems, etc.

Notwithstanding the recognition of the aforementioned information as personal data as a general rule, in some cases courts refuse to do so. For example, a court refused to recognize as biometric personal data the image of a sleeping employee until such time as it is transmitted for purposes of identification (a decision of the Kineshensky City Court of Ivanovo Region of 27 May 2021 in case no. 2-873/2021)¹.

Thus, in all the cases under consideration, the data subject is the employee (or the person seeking employment), while the employer is the operator — that is, a legal or natural person that processes the employee's personal data and also determines the purposes of data processing, the composition of personal data to be processed, and the actions (operations) performed with personal data (section 2 of Article 3 of the Personal Data Law). The processing of personal data encompasses not only systematization, clarification, extraction, and depersonalization of data, but also other actions, including: collection, storage, use, transmission, blocking, deletion, and destruction (section 3 of Article 3 of the Personal Data Law).

When speaking of the significance of employees' personal data, it is necessary to recognize that they are an integral element of labour relations (or, if one proceeds from the fact that the elements of any legal relationship are the parties, the object, and the content — a sub-element, a part of the content), which affects the rights of employees and the obligations of employers. Every employer is obliged to obtain and process employees' personal data in compliance with the requirements of the law: to request the employee's consent to data processing as a general rule; to ensure the protection of data from leaks, transmitting it only to state bodies in cases provided

¹ All data on decisions of Russian courts used in the research and referenced in this article were taken from the "Judicial and Normative Acts of the Russian Federation" database (<https://sudact.ru/>).

for by law; to use the data obtained only for purposes related to employment activity, etc. In addition, since 2022, employers have been required to notify Roskomnadzor of the processing of employees' personal data. Notification must be provided by the data operator before processing begins. In accordance with section 3.1 of Article 22 of the Personal Data Law, with respect to each purpose of data collection, it is necessary to clarify the following parameters: categories of data and data subjects; lists of personal data that will be processed; the legal basis for their processing; a list of actions with personal data and methods of processing. Notification is submitted to the territorial office of Roskomnadzor at the location of the employer in paper form or in electronic form, including through the "State Services" portal. Separate notification must be submitted by the employer within twenty-four hours of the discovery of unlawful or accidental transmission of data (section 3.1 of Article 21 of the Personal Data Law). Special notification is also submitted in the event of cross-border transmission of employees' personal data by the employer. Failure to fulfil these obligations entails administrative liability (Article 19.7 of the Code of Administrative Offences of the Russian Federation).

Employees' personal data have organizational significance for the parties to labour relations. They make it possible to formalize these relations and are necessary for further personnel record-keeping, reporting to state bodies, for example to the tax inspection service. The establishment of a category of personal data guarantees employees the confidentiality of their personal information, grants them the right to control the use of their data, to demand the correction of inaccurate information, and to demand the deletion of information obtained by the employer in violation of law. Thus, employees' personal data are important both for compliance with the law in labour relations (without their use it would be impossible to employ a person) and for the protection of employees' rights (rights to the inviolability of private life), as well as for the safe functioning of the employer (sanctions are provided for data leaks or receipt of data in violation of law). Every employer, except employers who are natural persons not being individual entrepreneurs (Article 22 of the Labour Code of the Russian Federation) and microenterprises (Article 309.2 of the Labour Code of the Russian Federation), is obliged to adopt a Regulation on the Personal Data of Employees. This local regulatory act regulates the organization of work with personal data at a specific employer in accordance with section 8 of Article 86 and Article 88 of the Labour Code of the Russian Federation. The Regulation on Employees' Personal Data should describe the procedure for data processing and list the rights and obligations of the employer and employees. In addition to the aforementioned local regulatory act, the data operator must also publish a policy regarding the processing of personal data, explaining the principles for working with the personal data of employees, customers, and other natural persons (section 2 of section 1 of Article 18.1 of the Personal Data Law).

3. Protection of employees' personal data

An employer must comply with the general principles of personal data processing established by Article 5 of the Personal Data Law. The processing of such data:

1) must be carried out on a lawful and fair basis and must be limited to achieving specific, predetermined, and lawful purposes;

2) does not permit the combination of databases containing personal data whose processing is carried out for purposes that are incompatible with each other;

3) must encompass only data that meets the purposes of processing, without excess;

4) must ensure the accuracy of personal data, their sufficiency, and, where necessary, their relevance with respect to the purposes of processing;

5) requires the destruction or depersonalization of data upon achievement of the purposes of processing or in the event of loss of the need to achieve such purposes, unless otherwise provided by federal law.

6) Furthermore, from 1 July 2025 onwards, Russia prohibits the processing of personal data through foreign services (section 5 of Article 18 of the Personal Data Law).

Requirements for the processing of employees' personal data directly are set out in Article 86 of the Labour Code of the Russian Federation:

— processing may be carried out exclusively for the purposes of compliance with the law, assistance to employees in finding employment, obtaining education and promotion, ensuring the personal safety of employees, monitoring the work performed, and preserving property (special attention should be paid to the last two items, which are aimed at protecting the interests of the employer);

— in determining the scope and content of an employee's processed data, the employer must be guided by the law;

— all personal data of an employee should be obtained from the employee himself or with the written consent of the employee;

— an employer does not have the right to obtain and process personal data belonging to the category of special data, except in cases provided for by law (for example, an employer has the right to process information about an employee's health status that is relevant to the employee's ability to perform his or her labour function, in accordance with Article 69 of the Labour Code of the Russian Federation; for this, the employer does not even need to obtain the consent of the employee);

— an employer does not have the right to request information about an employee's membership in public associations, including trade unions, again, except in cases provided for by law;

- in making decisions affecting an employee's interests, an employer does not have the right to rely on personal data obtained exclusively as a result of automated processing or electronic receipt (without human participation);
- protection of an employee's personal data from unlawful use or loss must be ensured by the employer in the manner provided for by law at the employer's own expense;
- employees and their representatives must be informed by signature of the employer's documents establishing the procedure for processing personal data, with information about their rights and obligations in this area;
- there is no provision for employees' refusal of their rights to preserve and protect confidentiality;
- employers, employees, and their representatives should jointly develop measures to protect employees' personal data.

The aforementioned principles and requirements for the processing of personal data form the basis of a legislative-restrictive approach to the protection of employees' personal data. Within the framework of the existing approach, an employer must obtain an employee's consent to the processing of his or her personal data as a general rule (except, for example, for the legally required transmission of data to state bodies — the Social Fund of Russia, military commissariat, tax inspectorate, etc.). Consent may be included in the employment contract or may be executed as a separate document, and the employee may later withdraw his or her consent. In the latter case, the employer will be able to continue processing personal data in the minimum scope necessary to preserve labour relations (section 5 of section 1 of Article 6 of the Personal Data Law). Upon withdrawal of consent, it will not be possible, for example, to process biometric data of the employee. Some data the employer will not be able to delete even after the dismissal of the person who has withdrawn consent, in compliance with the requirements of Federal Law of 22 October 2004 No. 125-FZ "On Archival Work in the Russian Federation", in accordance with which a number of documents on personnel must be stored for up to 75 years. It should be noted that the dissemination of an employee's personal data requires separate written consent (Article 10.1 of the Personal Data Law).

Upon discovery of violations, the employer will be held liable in the form of a fine. Notwithstanding the fact that an employer who has disregarded the established procedure for processing personal data is held administratively liable, claims for the protection of personal data are considered in accordance with the rules of civil procedure, as follows from section 6.1 of Article 29 of the Code of Civil Procedure of the Russian Federation. This also applies to situations where, in the interests of a specific citizen, a claim for the protection of his or her rights as a data subject is brought by Roskomnadzor, which has the right to apply to the court with a statement in protection of the rights, freedoms, and legitimate interests

at the request of a specific person or in protection of the rights, freedoms, and legitimate interests of an indefinite circle of persons on the basis of Article 46 of the Code of Civil Procedure of the Russian Federation (a ruling of the Civil Chamber of the Supreme Court of the Russian Federation of 14 July 2020 No. 58-KT20-2). In addition, civil law liability of the employer is provided for — compensation of losses (Article 15 of the Civil Code of the Russian Federation) and compensation for non-pecuniary damage (Article 151 of the Civil Code of the Russian Federation). Employees directly responsible for the violation may be held liable to disciplinary or even criminal responsibility.

The general principles and requirements for the processing of personal data are reflected in court decisions concerning the protection of employees' personal data. Thus, courts strictly assess the correspondence of the information requested to the purposes of processing. An employer may request only necessary data; if it demands the provision of excessive information, it violates the employee's right to the inviolability of private life and the right to the protection of personal data. Typical violations by employers of the procedure for processing personal data include: absence of the employee's consent to data processing (in cases where it is required); use of data for personal purposes not related to the employee's employment activity; transmission of data to third parties without sufficient grounds.

As practice shows, currently a significant portion of labour disputes are related to the use of video surveillance in the process of work. Courts, in considering such disputes, ascertain the lawfulness of the implementation of video surveillance, which will be considered lawful if:

- the use of video surveillance is mentioned in the Rules of Internal Labour Procedure, or the employer has adopted a separate local regulatory act — a Regulation on Video Surveillance, with which employees are acquainted by signature;
- there is the employee's consent to the processing of personal data, including the processing of data obtained in the course of video surveillance;
- video cameras are installed only at work stations, in production premises, in corridors, but not in changing rooms, rest rooms, toilets, and shower rooms;
- employees are notified of the surveillance and of the visibility zones of the cameras;
- recordings are not posted on the internet and are not transmitted to third parties.

In accordance with Article 22 of the Labour Code of the Russian Federation, an employer has the right to require employees to perform their employment duties, to comply with labour discipline, and to treat the employer's property with care. "The law does not specify exactly how an employer may monitor subordinates, therefore, the establishment of video surveillance to achieve a purpose related to the labour process is not a measure contrary to the law" (a decision of the Hostinsky District

Court of Sochi of 13 January 2025 in case no. 2-4578/2024). Permissible purposes of video surveillance include: monitoring the efficiency of work, improving labour productivity, control and accounting of working hours. If an employee has not given consent to the processing of biometric personal data, this does not mean that the employer does not have the right to conduct video surveillance. Such surveillance is possible if all employees have been acquainted by signature with the local regulatory act mentioning video surveillance (if an employee does not agree to sign a statement of acquaintance, an appropriate act is drawn up), and in premises where there are video cameras, warning notices are displayed indicating the openness of the surveillance. Accordingly, video surveillance in premises intended for employee rest is not permitted, as it violates the employee's right to the inviolability of private life (a ruling of the Third Cassation Court of General Jurisdiction of 3 July 2023 in case no. 88-14171/2023).

With the development of digital technologies, the use of employees' biometric data is becoming increasingly common. It should be noted that the processing of biometrics includes the use by an employer of an employee's photograph, including for image-related purposes. The fact of an employee's participation in a photo shoot does not mean consent to the use of the image by the employer; written consent of the employee is required (a ruling of the Second Cassation Court of General Jurisdiction of 4 July 2023 in case no. 88-13675/2023).

The number of labour disputes related to employers' making of decisions exclusively on the basis of automated data processing or electronic receipt of data is also increasing, which is not permitted under section 6 of Article 86 of the Labour Code of the Russian Federation. Thus, in a decision of the Balashikha City Court of Moscow Region of 14 January 2025 in case no. 2-11858/2024, it is emphasized that the law prohibits subjecting employees to disciplinary liability solely on the basis of information obtained from the functioning of an electronic access control system. Employees' applications to court may concern information leaks due to insufficient protection of data by the employer, disclosure of personal data, or refusal to provide an employee access to his or her personal data. Usually, in such cases, plaintiffs, in addition to restoration of the violated right, demand compensation for non-pecuniary damage. A typical example of courts' decisions on such questions is the decision of the Sverdlov District Court of Kostroma of 24 December 2024 in case no. 2-4521/2024, which recognizes the employer's inaction (failure to provide information requested by the employee regarding the processing of his or her personal data) as unlawful and grants the employee's claim for compensation for non-pecuniary damage.

A separate question deserves attention: does an employer have the right to disseminate information about disciplining a specific employee? Discussion of this question reached the Constitutional Court of the Russian Federation. The claimant challenged the constitutionality of section 1 of Article 152 of the Civil Code of

the Russian Federation, according to which a person has the right to demand the refutation of information damaging his or her honour, dignity, or business reputation only if the person who disseminated the information does not prove that it is true. By a Ruling of the Constitutional Court of the Russian Federation of 21 July 2023 No. 44-Π “In the Case Concerning a Check of the Constitutionality of Section 1 of Article 152 of the Civil Code of the Russian Federation in Connection with a Complaint of Citizen E.A. Popkova”, the aforementioned section of Article 152 of the Civil Code of the Russian Federation was recognized as corresponding to the Constitution of the Russian Federation, as a result of which the employer’s right to determine the expediency of disseminating information about an employee subjected to disciplinary punishment, provided that the information corresponds to the purposes of its dissemination, was confirmed.

4. The impact of algorithmic management on the sphere of labour and employee rights

Algorithmic management (algorithmic governance)¹ is the automated management of employees and business processes within an organization for purposes of optimization. Automation of management entails the making of decisions on the basis of the use of AI systems, which increasingly actually perform the employer’s functions in fact, from the hiring of workers to their dismissal.

Algorithmic management includes:

- 1) automated data collection and monitoring of employees;
- 2) real-time response to data used for making management decisions;
- 3) automated or semi-automated decision-making;
- 4) conversion of performance assessments into rating systems and other metrics;
- 5) the use of “nudging” to indirectly encourage particular employee behaviour².

Initially, algorithmic management penetrated the sphere of labour through digital labour platforms; gradually, new digital tools came to be applied by “traditional” employers as well. The EU Regulation on Artificial Intelligence, adopted in 2024³,

¹ Algorithmic management as algorithmic control at the micro level, should be distinguished from the concept of Algorithmic governance, that is, algorithmic management at the macro level through the use of algorithms to regulate and coordinate social, economic, and political processes in society, including state and corporate governance.

² *Filipova I. A.* (2023). *Algoritmicheskiy menedzhment i tsifrovoye profilirovaniye v sfere truda* // *Trudovoye pravo v Rossii i za rubezhom* = Labor Law in Russia and Abroad, 1. Pp. 16.

³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (date of address: 10.08.2025).

confirms that automated decision-making in the workplace entails significant risks to decent working conditions and the protection of workers' rights (AI systems applied in the field of employment and personnel management are classified as high-risk). The subsequent adoption of the EU Directive on improving working conditions on digital labour platforms¹ was aimed at increasing the level of transparency in the application of artificial intelligence for the functioning of digital platforms. Thus, the task of preserving human control over compliance with working conditions was accomplished, and workers were given the right to challenge automated decisions. This directive, according to European legal scholars, was a step forward for European legislation, but since it concerns only digital labour platforms, it has not satisfied the growing need to regulate the application of algorithmic management in the sphere of labour as a whole. Regulation of such application will require the adoption of another legal act — a Directive on Algorithmic Management, a draft of which has already been created and includes a prohibition on particularly harmful practices, the right to challenge automated decision-making in “traditional” workplaces, and so on². For the use of digital tools by any employer enables large-scale monitoring and data collection, leading to violations of confidentiality, reducing the level of protection of workplaces and worker autonomy³.

Algorithmic management is carried out on the basis of various systems that automate management processes, including:

- project planning and management systems that carry out real-time monitoring, analysis of data obtained with the identification of trends, forecasting of probable future events, distribution of tasks, resources, and control of deadlines;
- human resource management systems that optimize personnel work through data analysis, enabling improved management of work performance and worker engagement;
- AI recruiters — digital platforms for personnel selection that accelerate the search for the most suitable candidates for jobs whilst simultaneously reducing the costs of such search⁴;

¹ Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work. Available: URL: <https://eur-lex.europa.eu/eli/dir/2024/2831/oj> (date of address: 10.08.2025).

² Adams-Prassl J., Abraha H., Kelly-Lyth A., Silberman M., Rakshita S. (2023). Regulating algorithmic management: A blueprint // *European Labour Law Journal*, 14(2). Pp. 124.

³ Cox Th., Oosterwijk G.R. (2024). Algorithmic management in traditional workplaces. Case studies on the impact of algorithmic technologies in seven sectors in the Nordics // *Policy Study*. Brussels: FEPS. Pp. 3.

⁴ Lipko V.D., Lipko N.I. (2025). Tsifrovaya transformatsiya kadrovyykh protsessov v epokhu tekhnologiy // *Kadrovik = HR Manager*, 6. Pp. 56.

— decision support systems that generate recommendations, providing intellectual assistance in analysis, forecasting, and choice of solutions in complex situations.

Next, we shall identify the main consequences of the implementation of algorithmic management by employers, which create or exacerbate already existing problems.

Consequence 1. The implementation of algorithmic management creates a need for large volumes of data for the proper functioning of AI systems. Obtaining such data is possible by means of access to numerous databases and the use of a variety of sensors. AI monitoring has become standard practice, “based on advanced computational methods to obtain statistical inferences about workers on the basis of their data. These inferences are subsequently used by employers to make various organizational and management decisions”, which effectively turns workers into “data-based commodities... the boundaries between technological innovation and human individuality are becoming increasingly blurred, challenging traditional understandings of confidentiality”¹.

A worker risks finding themselves “behind glass”; their private life becomes a fiction. The problem of reduced confidentiality is intensified by the spread of wearable devices used in healthcare to help diagnose diseases and monitor an individual’s health status. Some of these devices have already been brought to market and are used in the workplace for purposes of protecting workers’ health and safety. Neither Russian nor European legislation yet regulates the use of wearable devices in the sphere of labour, which increases the problem of realizing the worker’s right to the inviolability of their private life. The existing regulatory framework relates to the use of medical devices and is focused on the safety, performance, and quality of technological products, but is unable to address data protection problems associated with the use of wearable devices for purposes of occupational health and safety². Discrepancies between labour legislation and occupational health and safety legislation leave room for the use of various high-technology systems to collect information about the worker and their participation in the production process³.

Consequence 2. The use of algorithmic management makes it possible not only to collect but also to generate vast volumes of new information about

¹ Carter C. (2025). AI surveillance: Reclaiming privacy through informational control // *European Labour Law Journal*, 16(2). Pp. 245.

² Marassi S., Földes M.É. (2025). From healthcare to employment: Tackling the regulatory challenges of in-body wearable devices at work in the European Union // *European Labour Law Journal*, 16(2). Pp. 195.

³ Zaitseva L. V. (2024). Risks for Personal Data of an Employee When the Employer Uses Technologies of Artificial Intelligence in the Countries of the Eurasian Economic Union // *European and Asian Law Review*, 7(4). Pp. 31.

workers, each of whose actions leaves a digital trace. This trace can be recorded and analyzed using artificial intelligence with minimal effort and cost. Digital traces and the results of their intelligent processing fill the created digital profile of each worker as a collection of current and reliable data about a specific person in digital format. The employer (through AI systems functioning to achieve the goals set by the employer) gains access to data that makes it possible to make management decisions optimal for the employer on the basis of information about the worker, of which the worker himself or herself may not yet even be aware. This is facilitated by the use of personnel electronic document circulation, the maintenance of which is permitted by Articles 22.1–22.3 of the Labour Code of the Russian Federation.

Already at the stage of employment, intelligent analysis of data obtained from the job applicant and from external sources makes it possible to identify hidden risks associated with the candidate and to prevent him or her from passing through the “entry” filter¹. Thus, algorithmic management increases the risk of discrimination against job candidates, while simultaneously threatening the inviolability of their private life. Moreover, discrimination is the easiest to detect from a technical point of view. As a result, thanks to the employer’s access to technical information about the operation of AI systems (through the specialists he or she has) and the absence of comparable access for the job seeker, the problem of discrimination will be exacerbated. The same applies not only at the stage of employment but also in subsequent periods of work, since although “the automation of decision-making processes previously performed by humans may make the criteria for discrimination more traceable and the results more quantitative... algorithmic decision-making processes are rarely transparent”².

Consequence 3. Algorithmic management is an element of intelligent automation of production, the degree of which is continuously increasing. In a number of sectors, there is already an “expulsion” of some workers from their jobs, with reference being made to call centres, the banking sector, and logistics. Other workers are forced to come to terms with the fact that their rights, enshrined in legislation formed predominantly under the conditions of Society 3.0 (industrial society), are meaning less and less in practice under the current stage of civilization’s development — Society 4.0 (post-industrial information society) — and risk becoming meaningless formalities in the era of the merger of physical and digital environments — the future of Society 5.0 (Smart Society). Thus, a problem emerges of ensuring real guarantees of workers’ rights in the conditions of a society managed with the aid

¹ *Filipova I. A. (2023). Algoritmicheskii menedzhment i tsifrovoe profilirovanie v sfere truda // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 1. Pp. 17.*

² *Kelly-Lyth A. (2023). Algorithmic discrimination at work // European Labour Law Journal, 14(2). Pp. 152.*

of artificial intelligence, the approach of which is signalled, among other things, by the spread of algorithmic management.

For now, case law on the use of algorithmic management is largely related to work based on digital platforms, which corresponds to the chronology of the spread of algorithmic management in the sphere of labour. This is illustrated by numerous decisions of American and European courts handed down in claims by taxi drivers and couriers, as well as decisions of Russian courts, in particular concerning the services “Yandex.Taxi” and “Yandex.Food”, for example, a decision of the Peace Court of the Zamoskvoretsky District of Moscow of 2 August 2022 imposing a fine for the leakage of personal data of “Yandex.Food” couriers. Indeed, algorithmic management increases the threat of data leaks, as the employer’s information systems contain numerous information about workers, the disclosure of which may result from cyber-attacks on these systems or unlawful access by insiders. Additionally, risks related to the use of cloud services and mobile devices for processing and storing personal information are increased¹. In addition, personal data are often used as training data in the training of AI models or the “retraining” of AI systems, the results of which depend on the set of databases “feeding” these systems². An additional risk is the connection to “open” AI systems, including chatbots, since information entered into such an AI system may be unintentionally transmitted to another user and retained for use in further training of that AI system³.

5. Ways of solving problems related to the spread of algorithmic management

At the present time, the transformation of labour relations and the sphere of labour as a whole continues, which has become an inevitable consequence of society’s transition from an industrial to a post-industrial type⁴, and moreover, the prospects for a further transformation are already emerging, related to humanity’s forthcoming transition to Society 5.0, in which digital technologies will occupy an even more important place. The rising intelligent automation of production as a sustained trend is supplemented by the spread of algorithmic management:

¹ Novikov P.A. (2025). Sovremennye vyzovy v obespechenii zashchity personalnykh dannykh rabotnikov // *Yuridicheskie issledovaniya* = Legal Studies, 3. Pp. 29.

² Lukács A., Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work // *Computer Law & Security Review*, 50. Art. 105848.

³ Novikov D.A. (2024). Ispolzovanie iskusstvennogo intellekta pri naime rabotnikov: problemy i perspektivy pravovogo regulirovaniya // *Journal of Digital Technologies and Law*, 2(3). Pp. 616.

⁴ Tomashevskiy K.L. (2025). Transformatsiya trudovykh pravootnosheniy (ot industrialnogo k postindustrialnomu tipu) // *Zhurnal rossiyskogo prava* = Journal of Russian Law, 29(2). Pp. 94.

AI systems increasingly not only take positions alongside workers but also manage production processes. From the perspective of the employer, such a “digital future” obviously has a positive effect, as it leads to reduced costs, increased productivity, and the possibility, when making decisions, of relying on volumes of data that human beings would simply be unable to process. At the same time, as social researchers warn, the application of algorithmic management potentially creates an imbalance between the technical and social subsystems of an organization, a vivid example of which is the company Amazon.

Workers typically act as a passive object of the implementation of new technologies¹, so the main efforts are directed at adapting the social subsystem to the requirements of the technical subsystem, including minimizing worker resistance, rather than using technologies from the outset with consideration for the specifics of the work². Self-learning AI systems are capable of adapting to new situations, making it possible to delegate to them the making of an increasingly broad range of decisions. Such self-learning is typically opaque, leaving no opportunity to identify the reasons for subsequent decisions and to challenge them³.

A dilemma emerges: parallel to the increasing transparency of workers to AI systems (through the processing of growing volumes of their personal data), the degree of opacity of decision-making for workers increases due to the use of algorithmic management. It is difficult to combat trends, but at least it is possible to adjust them. One of the solutions capable of preventing the degradation of workers' position is a prohibition enshrined in legislation on making decisions exclusively on the basis of automated data processing (section 6 of Article 86 of the Labour Code of the Russian Federation, section “h” of Article 15 of the GDPR).

As is well known, the EU aspires to global leadership in the formulation of legislation taking into account the development of digital technologies, but even in the provisions of the GDPR relating to automated decision-making and providing workers with certain protection, serious gaps remain. For example, most management decisions today are made with the aid of algorithms, but not fully automated, and in such cases the guarantees provided for in Article 22 of the GDPR (including the right to challenge a decision) are not applicable⁴. At the same time, the results of research

¹ Parker S. K., Grote G. (2020). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world // *Applied Psychology*, 71(4). Pp. 1171.

² Davis M. C., Challenger R., Jayewardene D. N., Clegg C. W. (2014). Advancing socio-technical systems thinking: A call for bravery // *Applied ergonomics*, 45(2). Pp. 171.

³ Petrovskaya I. A., Demchenko V. S. (2023). Algoriticheskiy menedzhment: opyt empiricheskogo issledovaniya // *Vestnik Moskovskogo universiteta. Seriya 6. Ekonomika* = Moscow University Economics Bulletin, 58(6). Pp. 129.

⁴ Abbraha H. (2023). Regulating algorithmic employment decisions through data protection law // *European Labour Law Journal*, 14(2). Pp. 172–191.

in the field of economics show that algorithmic management “is likely to become a notable component of work for many people in the coming years”¹.

The increasing technical possibilities for monitoring workers require legislative limitations not only on the control of the employee’s performance of labour duties but also on the process of using the data obtained to make personnel decisions. It becomes necessary to consider the employee’s right to the inviolability of private life as one of the fundamental principles of the legal regulation of labour relations² with appropriate reflection in the law.

In connection with “the unprecedented scale, depth, rapid pace of transformation, and pervasive impact on labour” of algorithmic management, a draft Directive on Algorithmic Management in the Workplace³ was submitted for discussion in the European Parliament in 2025 (hereinafter — the draft Directive). In the opinion of representatives of the Committee on Employment and Social Affairs of the European Parliament, who are the authors of the draft, the prohibition provided for in the GDPR on fully automated decision-making in a number of cases, for example in hiring, is insufficient. After approval, the new regulatory act should establish a common EU standard for the use of algorithmic management in the workplace, ensuring enhanced transparency and legal certainty in all EU Member States.

According to Article 3 of the draft Directive, no later than the first working day (or immediately before any change in the employment contract, as well as at any time upon receipt of a request from the employee), the employer, in clear and comprehensible form, without unnecessary technical complexity, must provide the employee in writing with information relating to the use or planned use of algorithmic management. The information is necessary for understanding how algorithmic systems will affect decisions affecting workers. This information will include the categories of collected and processed data and the types of worker actions tracked. In accordance with Article 5 of the draft Directive, as a guarantee of workers’ rights, processing of personal data concerning the emotional state of workers, neuro-surveillance, private conversations, worker behaviour outside working hours, as well as predictions regarding the realization of workers’ fundamental rights and conclusions about racial or ethnic origin, migration status, political views, religious

¹ *De Stefano V.* (2022). AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU’s Legal Framework // Brussels: European Parliamentary Research Service. Pp. 7.

² *Serova A. V., Shcherbakova O. V.* (2022). The Employee’s Right to Privacy Transformation: Digitalization Challenges // *Kutaфин Law Review*, 9(3). Pp. 437.

³ Draft report with recommendations to the Commission on digitalisation, artificial intelligence and algorithmic management in the workplace — shaping the future of work (2025/2080(INL)), 26.06.2025. URL: https://www.europarl.europa.eu/doceo/document/EMPL-PR-774283_EN.pdf (date of address: 10.08.2025)

beliefs, health status, trade union membership, or sexual orientation should be directly included in prohibited practices.

Article 6 of the draft Directive refers to the need to maintain human control so that an interested worker is able to obtain from the employer an explanation regarding any decision affecting various aspects of labour relations with him or her. These aspects include distribution of tasks, assessment of labour productivity, working hours schedule, pay, disciplinary penalties, and so on, if the making of the decision was substantially influenced by an algorithmic system. Decisions, however, concerning the beginning or termination of labour relations, any changes in pay cannot in principle be made exclusively on the basis of algorithmic management, but must be considered and finally rendered by a human manager.

The rules proposed by the draft Directive will make it possible to change the new management structure to a more humane one, since algorithmic management is an innovation that changes the relationship between humans and artificial intelligence in the production environment, and in the absence of sufficient control, as M. A. Yudina aptly stated, “may become the last nail in the coffin of confidentiality in the reality of social networks, smart homes, smart cities, and electronic government”¹.

Of course, in the processing of personal data, the principle of lawfulness must be observed first and foremost. If one refers to the practice of the European Court, one may be assured that processing of personal data will be considered lawful with the mandatory observance of the following three conditions:

- processing must correspond to the purpose of pursuing legitimate interests;
- processing must be necessary to achieve such purposes;
- legitimate interests must not override the interests or fundamental rights and freedoms of the data subject.

This is about a phased assessment of proportionality: sufficiency for achieving a legitimate purpose, necessity for achieving that purpose, and balance between achieving the purpose and the rights of the data subject². At the same time, the European Court clarified that the necessity of processing should be assessed taking into account the principle of data minimization set out in section “c” of Article 5 of the GDPR³. Legitimate interests of the employer, if they are insignificant

¹ Yudina M. A. (2024). Algorithmic management in the focus of sociology of technology // RUDN Journal of Sociology, 24(3). Pp. 744.

² Dalla Corte L. (2022). On proportionality in the data protection jurisprudence of the CJEU // International Data Privacy Law, 12(4). Pp. 264.

³ Judgment of the Court (Grand Chamber) of 4 July 2023. Meta Platforms Inc and Others v Bundeskartellamt. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252> (date of address: 10.08.2025).

and not too compelling, may override the interests and rights of workers only in those cases where the impact on those rights and interests is even more insignificant¹.

The aforementioned tasks will have to be solved by the Russian legislator as well, supplementing and amending labour legislation. Here an important point becomes the inclusion of the definition of the very concept of “employees’ personal data” in the Labour Code of the Russian Federation. Whereas prior to 2013, an employee’s personal data were defined in Article 85 of the Labour Code of the Russian Federation as information necessary to the employer in connection with the employment relationship and concerning a specific employee, in 2013 Article 85 of the Labour Code of the Russian Federation was repealed. As a result, Chapter 14 of the Labour Code of the Russian Federation was “decapitated”, leaving only the articles following Article 85 of the Labour Code of the Russian Federation, devoted to individual issues of the processing of personal data, thereby complicating the task for the legal practitioner in understanding and interpreting the law. The return (more precisely, the inclusion in the Labour Code of the Russian Federation of an updated, more comprehensive formulation) of this concept is needed by judges considering relevant cases. Confirmation of this may be provided by the fact that in decisions rendered by Russian courts, references to Article 85 of the Labour Code of the Russian Federation are still encountered. Examples include a decision of the Vakhitovsky District Court of Kazan of 25 February 2025 in case no. 2-1947/2025, a decision of the Georgievsky City Court of Stavropol Territory of 24 February 2025 in case no. 2-293/2025, a decision of the Lenin District Court of Tyumen of 3 September 2024 in case no. 2-7749/2024, and several others. An updated legal definition of employees’ personal data should take into account the growing use of algorithmic management in the production environment. As a possible variant, we propose to formulate the content of Article 85 of the Labour Code of the Russian Federation as follows:

“Employees’ personal data are any information relating to a directly or indirectly identified or identifiable natural person (employee) that is processed by an employer within the framework of labour relations, including data collected in the process of algorithmic management (biometric data, digital traces, behavioural metrics, and derived data as results of automated analysis generated by algorithms)”.

The return of an updated definition of employees’ personal data directly to the labour legislation of the Russian Federation will contribute to the improvement of legal regulation in this area and will have a positive impact on law enforcement.

¹ Warter J. (2025). The legitimacy of modern data processing in the workplace // *European Labour Law Journal*, 16(2). Pp. 180–181.

Conclusion

In the dawning era of artificial intelligence, already having acquired the steady designation in the English-language variant of “AI-driven world”, human personal data are “fuel” for AI systems, enabling them to learn and function with increasing levels of effectiveness. Entrepreneurs acting as employers find in AI systems very useful intellectual helpers that optimize production and management processes. The further things go, the more digital technologies prevail over the social environment, transforming it and subjecting it to new rules. Employees’ personal data become more vulnerable with each passing year, and the implementation by employers of algorithmic management in the workplace only intensifies this trend. Workers risk finding themselves “under glass” with the gradual transformation of confidentiality into fiction. Particular attention is required to the now technically accessible acquisition of biometric data by employers, since intelligent analysis of such data makes it possible to forecast probable human behavior and health status in the future. Legal regulation in the field of personal data protection lags behind technological achievements in terms of speed of formation. The problems caused by this are linked, first and foremost, to the reduction of confidentiality, but also to the increase in the risk of discrimination and, accordingly, to the provision of real guarantees of workers’ rights in the conditions of the development of a society managed with the aid of artificial intelligence. The aforementioned problems are readily “readable” when one refers to case law, both Russian and foreign. The solution of these problems lies not only in the legislative sphere but also in the sphere of law enforcement. In order for justice to perform its task most effectively, the court must rely on a quality legislative base. Consequently, the elimination of gaps in the legislation regulating the protection of employees’ personal data, in particular in the Labour Code of the Russian Federation, will help to ensure this protection, minimizing the risks that emerge or increase owing to the spread of algorithmic management and the rising intelligent automation of the sphere of labour.

References

- Abraha H.* (2023). Regulating algorithmic employment decisions through data protection law // *European Labour Law Journal*, 14(2). Pp. 172–191. (In English)
- Adams-Prassl J., Abraha H., Kelly-Lyth A., Silberman M., Rakshita S.* (2023). Regulating algorithmic management: A blueprint // *European Labour Law Journal*, 14(2). Pp. 124–151. (In English)
- Adams Z., Adams-Prassl A., Adams-Prassl J.* (2022). Online tribunal judgments and the limits of open justice // *Legal Studies*, 42(1). Pp. 42–60. (In English)

Berezhnov A. A. (2024). Problemy zashchity personalnykh dannykh rabotnikov na sovremennom etape // *Trudovoe pravo v Rossii i za rubezhom* = Labor Law in Russia and Abroad, 3. Pp. 25–28. (In Russian)

Carter C. (2025). AI surveillance: Reclaiming privacy through informational control // *European Labour Law Journal*, 16(2). Pp. 245–258. (In English)

Cox Th., Oosterwijk G. R. (2024). Algorithmic management in traditional workplaces. Case studies on the impact of algorithmic technologies in seven sectors in the Nordics // *Policy Study*. Brussels: FEPS. 60 p. (In English)

Dalla Corte L. (2022). On proportionality in the data protection jurisprudence of the CJEU // *International Data Privacy Law*, 12(4). Pp. 259–275. (In English)

Davis M. C., Challenger R., Jayewardene D. N., Clegg C. W. (2014). Advancing socio-technical systems thinking: A call for bravery // *Applied ergonomics*, 45(2). Pp. 171–180. (In English)

De Stefano V. (2022). AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework // Brussels: European Parliamentary Research Service. 84 p. (In English)

De Stefano V. (2020). “Masters and Servers”: Collective Labour Rights and Private Government in the Contemporary World of Work // *International Journal of Comparative Labour Law and Industrial Relations*, 36(4). Pp. 425–442. (In English)

Filipova I. A. (2023). Algoritmicheskiy menedzhment i tsifrovoe profilirovanie v sfere truda // *Trudovoe pravo v Rossii i za rubezhom* = Labor Law in Russia and Abroad, 1. Pp. 16–18. (In Russian)

Filyushchenko L. I. (2024). Tsifrovoy profil rabotnika: problemy zashchity personalnykh dannykh // *Zakony Rossii: opyt, analiz, praktika* = Laws of Russia: experience, analysis, practice, 1. Pp. 93–97. (In Russian)

Hendrickx F. (2022). Protection of workers' personal data: General principles // *ILO Working Paper 62*. Geneva: ILO. 55 p. (In English)

Kelly-Lyth A. (2023). Algorithmic discrimination at work // *European Labour Law Journal*, 14(2). Pp. 152–171. (In English)

Kiyamova D. I. (2025). Iskusstvennyy intellekt v rekrutinge: zashchita personalnykh dannykh i predotvrashchenie diskriminatsii v tsifrovuyu epokhu // *Kadrovik* = HR Manager, 5. Pp. 59–67. (In Russian)

Lipko V. D., Lipko N. I. (2025). Tsifrovaya transformatsiya kadrovyykh protsessov v epokhu tekhnologiy // *Kadrovik* = HR Manager, 6. Pp. 56–60. (In Russian)

Lukács A., Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work // *Computer Law & Security Review*, 50. Art. 105848. (In English)

Lushnikov A. M. (2022). Tsifrovizatsiya trudovogo prava i trudovye otnosheniya // *Zakon* = Law, 10. Pp. 28–37. (In Russian)

Marassi S., Földes M. É. (2025). From healthcare to employment: Tackling the regulatory challenges of in-body wearable devices at work in the European Union // *European Labour Law Journal*, 16(2). Pp. 195–211. (In English)

Novikov D. A. (2024). Ispolzovanie iskusstvennogo intellekta pri naime rabotnikov: problemy i perspektivy pravovogo regulirovaniya // *Journal of Digital Technologies and Law*, 2(3). Pp. 611–635. (In Russian)

Novikov P. A. (2025). Sovremennye vyzovy v obespechenii zashchity personalnykh dannykh rabotnikov // *Yuridicheskie issledovaniya = Legal Studies*, 3. Pp. 28–44. (In Russian)

Parker S. K., Grote G. (2020). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world // *Applied Psychology*, 71(4). Pp. 1171–1204. (In English)

Sapfirova A. A. (2024). Pravovye mery obespecheniya bezopasnosti personalnykh dannykh rabotnikov pri ikh obrabotke rabotodatelayami // *Kadrovik = HR Manager*, 12. Pp. 8–13. (In Russian)

Serova A. V., Shcherbakova O. V. (2022). The Employee's Right to Privacy Transformation: Digitalization Challenges // *Kutafin Law Review*, 9(3). Pp. 437–465. (In English)

Petrovskaya I. A., Demchenko V. S. (2023). Algoritmicheskiy menedzhment: opyt empiricheskogo issledovaniya // *Vestnik Moskovskogo universiteta. Seriya 6. Ekonomika = Moscow University Economics Bulletin*, 58(6). Pp. 109–132. (In Russian)

Tomashevskiy K. L. (2025). Transformatsiya trudovykh pravootnosheniy (ot industrialnogo k postindustrialnomu tipu) // *Zhurnal rossiyskogo prava = Journal of Russian Law*, 29(2). Pp. 94–109. (In Russian)

Warter J. (2025). The legitimacy of modern data processing in the workplace // *European Labour Law Journal*, 16(2). Pp. 179–194. (In English)

Yudina M. A. (2024). Algorithmic management in the focus of sociology of technology // *RUDN Journal of Sociology*, 24(3). Pp. 734–746. (In English)

Zaitseva L. V. (2024). Risks for Personal Data of an Employee When the Employer Uses Technologies of Artificial Intelligence in the Countries of the Eurasian Economic Union // *European and Asian Law Review*, 7(4). Pp. 22–34. (In English)

Information about the authors

Ildar Begishev (Kazan, Russia) — Doctor of Legal Sciences, Associate Professor, Chief Researcher, Research Institute of Digital Technologies and Law, Professor, Department of Criminal Law and Process, Kazan Innovative University named after V.G. Timiryasov, Honored Lawyer of the Republic of Tatarstan (42 Moskovskaia St., Kazan, 420111, Russia; e-mail: begishev@mail.ru).

Irina Filipova (Nizhny Novgorod, Russia) — Candidate of Law, Associate Professor, Associate Professor of the Department of Labor and Environmental Law, National Research Nizhny Novgorod State University named after N.I. Lobachevsky (603022, Nizhny Novgorod, Gagarin Ave., 23; e-mail: irinafilipova@yandex.ru).

Recommended citation

Begishev I.R., Filipova I.A. Protection of employees' personal data in the context of the spread of algorithmic management based on court practice. *Kazan University Law Review*. 2025; 4 (10): 190–212. DOI: 10.30729/2541-8823-2025-10-4-190-212.