DOI 10.52468/2542-1514.2024.8(4).63-72

LEGAL REGULATION OF DIGITAL PROFILING OF A PERSON IN THE PRACTICE OF FOREIGN COUNTRIES[**]

Svetlana S. Kuznetsova
Ural State Law University named after V.F. Yakovlev, Yekaterinburg, Russia

Article info
Received –
2024 June 13
Accepted –
2024 September 10
Available online –
2024 December 20

Keywords
Digital traces, personal data, profiling, automated decision-making, privacy, restriction of profiling, transparency

The subject. The legislation of foreign countries concerning human digital profiling, the advantages and disadvantages of profiling process, that affect the implementation and protection of certain constitutional rights, including the right of privacy, dignity of the human person and right to manage personal data.

The purpose of the article is to systematize the approaches to human digital profiling reflected in the legislation of foreign countries.

Methodology. The author is guided by formal dogmatic, induction and comparative law methods in research.

Main results and conclusions. The author formulates approaches to the concept of human digital profiling that have been developed in the practice of foreign countries. The concept of digital profiling involves the processing of most digital traces, however, the profiling process itself is sometimes limited to solely automated forms of decision-making (most states of the USA), which significantly limits the rights of the personal data subject. Definition of automated forms of decision-making in the personal data protection law of China is positively assessed, because that process is not directly related to personal data, but to areas of human life, which most accurately reflects the essence of the processing digital traces during profiling. Consent to solely automated profiling of a human entailing legal or other significant consequences is required only in the countries of the European Union, while in the USA and China only a subsequent refusal to apply decisions is possible.

It is concluded that obtaining direct consent, considering the volume of information processed about identity for the human profiling and the importance of its consequences for the individual, is a necessary condition for ensuring individual rights. A tendency has been identified to differentiate the procedure for implementing the principle of transparency depending on whether human profiling is carried out by public authorities while making individual decisions, in public interests or by business for commercial purposes. The approach of the EU and China, which provides for the need to disclose the formula of the profiling algorithm when used by public authorities, is a positive practice for implementing the principle of transparency in conjunction with the implementation of the right to know about the activities of a public authority. At the same time, in Sweden and Germany a successful attempt has been made to find a balance between the interests of the individual and the profiling controller when using it for commercial purposes. The American model of legal regulation of personality profiling is assessed negatively, since it removes the possibility of control over the processing of personal data in the human profiling by public authorities and establishes a minimum scope of rights of the data subject when profiling for commercial purposes.

[**] The study was carried out with financial support from the Russian Science Foundation within the framework of scientific project 24-28-01378 “Development of a concept for legal regulation of digital profiling, social scoring and the use of “digital traces”.

1. Introduction

Digital transformation of public and municipal administration, economy and social sphere is defined as one of the goals of national development[1], which implies automation of management decision-making and improvement of digital data management tools. In the era of big data, the use of traditional methods and tools for processing and storing information is impossible [1, p.1], this is due to the characteristics of big data: generation mainly by machines, their unstructured nature, the presence of information in the composition that has no value [2, pp. 14–15]. One of the effective means of processing big data, extracting information and organizing it is digital profiling, which allows " to reduce the overload of information, to make it ‘manageable’, to make sense out of it and to regain control of the effects of one’s actions." [3, p. 30].

For a long time, the term "profile" was associated exclusively with forensic profiling as a method of establishing the identity of a criminal [4, p. 111], identifying his personal and behavioral characteristics [5]. However, the development of digital technologies has revealed the potential for using digital profiling for the purposes of marketing, personnel management [6, p. 49], and public administration [7]. Today, profiling is “the process of collecting and analyzing information about a person or an organization, including those accessing the Internet” [8, p. 9], as well as “treating that person or group (or other persons/groups) in light of these characteristics (i.e., the process of applying a profile)” [9, p. 77].

The digital transformation of society ensures increased efficiency of law enforcement processes [10, p. 10]. However, the automation of processing digital traces has not only a number of advantages [11], but also carries a threat, especially in cases where it is carried out in relation to personal data. The key issue is finding a balance between the interests of the subject of automated data processing and the data subject who wants to protect the right to privacy and respect for the dignity of the individual. Since profiling works with information about the individual and is aimed at obtaining new knowledge about it, including personal information, there is always a risk of the data subject losing control over it [12, p. 92].

The purpose of this study is to identify and formulate the concept of legal regulation of digital profiling. To achieve this goal, an analysis of the norms of legislation and law enforcement practice in foreign countries was conducted, the concept and purposes of profiling, the volume of information subject to processing, and guarantees of the rights of individuals subject to profiling were determined.

2. The concept of profiling

In legislation, profiling is considered in the light of the processing of personal data, therefore the definition of the concept is disclosed in special legislation on data protection.

The General Data Protection Regulation of the European Union uses a broad concept of profiling: "any form of automated processing of personal data" aimed at generating information about an individual, in particular about health, personal preferences, interests, economic situation, as well as creating probabilistic models of human behavior [13], for example, work performance, reliability and movement. Due to the fact that the assessment of

[1] Decree of the President of the Russian Federation of 07.05.2024 No. 309 "On the national development goals of the Russian Federation for the period up to 2030 and for the perspective up to 2036". Rossiyskaya gazeta, May 11, 2024 No. 100.

information from the standpoint of the presence of personal data in it is carried out contextually [14], the processing of most digital traces may fall under the requirements of the General Regulation. Since the Regulation recognizes any form of profiling, both cases of full automation of the decision-making process and those based on human participation fall under regulation [15].

In the United States, there is no legislation at the federal level regulating the profiling process, but this term is used in the legislation of thirteen states. In the states of Virginia, Montana and New York, the concept of profiling closely reproduces the EU concept in content: "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements". In the states of Delaware, Indiana, Connecticut, New Hampshire, Tennessee, Texas, and Florida, profiling falls exclusively on cases of an automated process, in connection with which the processing of information about an individual with the participation of a person excludes the receipt of additional guarantees provided by law. The states have adopted a broad concept of personal data, which allows for the regulation of the profiling process in relation to most digital traces. In the state of California, personal information includes not only that which directly identifies a person, but also that which describes the characteristics of the data subject (shopping list, search queries) that can be associated with him or her and, directly or indirectly, allows identification in combination with other data.

The Personal Data Protection Law of the PRC does not contain the concept of profiling, but Article 73 defines automated decision-making as "an activity to automatically analyze and evaluate a person's behavior habits, hobbies or economic, health or credit status through computer programs and make decisions". The concept of automated decision-making is disclosed not through personal data, but through information about individual areas of an individual's life, thus, the analysis of any digital traces can be considered as automated decision-making if the information about the person reflected in the definition is received. An analysis of Articles 73 and 24 of the Law allows us to conclude that automated decision-making does not exclude the possibility of human participation in this process, but this fact will have legal consequences from the standpoint of the scope of the rights of the data subject.

In the legislation of all the countries considered, profiling involves the processing of most digital traces that are associated with an individual or describe them, identify them or allow them to be identified (EU countries, USA), and provide the opportunity to obtain information about certain areas of an individual's life (PRC). Most countries allow human participation in the profiling process, which provides the data subject with the opportunity to receive additional guarantees for the exercise of the right to manage personal data; however, in some US states, the concept provides for exclusively automated decision-making options. It appears that the concept of automated decision-making proposed in China most accurately reflects the essence of profiling, since any digital traces are processed [16, p. 254; 17, p. 46], and not just personal data. Such an approach can provide a higher level of guarantee of individual rights, since the data subject will be aware of the fact of profiling. In China, when using automated decision-making algorithms for direct marketing purposes, the operator is obliged to offer processing options that are not based on individual characteristics or to refuse marketing.

3. Guarantees of human rights in digital profiling.

According to Article 22 of the EU General Data Protection Regulation, the data subject has the right not to be subject to profiling with a decision made solely by automated means if it produces legal effects or " similarly significantly affects him or her". It is possible to resort to corresponding algorithms in one of the following cases:

- they do not produce legal or similar significant effects for the data subject;
- explicit consent has been obtained;
- it is necessary for the entering into, or performance of, a contract;
- it is authorized by EU or EU Member State law. In Article 37 of the Federal Data Protection Act of Germany, processing is possible in connection with the performance of an insurance contract[2].

The automated process of processing personal data requires compliance with all principles of the General Data Protection Regulation, including transparency. Its implementation imposes an obligation to provide information in plain language in accordance with Articles 13 and 14, including on the existence of " automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". Separately, the provision of information on the existence of the right to object to profiling for marketing purposes is guaranteed. As Mochalov A.N. notes, "the wording of the GDPR does not have the necessary specificity and does not allow us to clearly say how the personal data controller must fulfill the corresponding obligation" [18, p. 81]. In the countries of the European Union, it is difficult to develop a practice for determining the procedure for applying this norm in terms of disclosing information about the logic of algorithms. In Austria, the court recognized that the principle of transparency entails the provision of information that allows a person to understand an automated decision, including disclosure of input data, parameters and variables used in the profiling process, the mathematical formula used to calculate the rating, an explanation of each profile category, as well as why the person was linked to a particular profile. However, failure to comply with the court decision, justified by the fact that the requested information constitutes a commercial secret, became the reason for an appeal to the European Court[3]. In a number of countries, a tendency is developing to interpret the content of the transparency principle differently depending on whether automated decision-making algorithms are used in the exercise of public authority or in commercial activities. In Sweden, when considering the issue of a bank’s activities, the court came to the conclusion that algorithmic formulas are not considered significant information [19, p. 21], while in the Trelleborg case, where algorithms were used to make a decision on the issuance of social assistance, it was stated that “the algorithm constituted an administrative document”, and without its openness, the plaintiffs cannot ensure the protection of their rights, that is, in relations with public authorities, the transparency of algorithms follows from the right to know [20]. Similarly, in the Hague District Court, the use of SyRI automated decision-making algorithms in the field of social security was recognized as illegal due to a violation of the principles of transparency and controllability. The need to protect commercial secrets is reflected in Article

[2] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097).

[3] Dun & Bradstreet Austria,Case C-203/22.

63 of the Preamble to the General Regulation, which emphasizes that the right to know about the algorithm of automated profiling and the consequences of such processing may not undermine commercial secrets. The conclusion on the balance of interests in automated decision-making for commercial purposes was formulated by the Federal Court of Justice of Germany with regard to the formula underlying the scoring[4].

Profiling also guarantees:

- receiving clear information about the right to object to profiling for direct marketing purposes and to object to profiling carried out for the purpose of achieving the public interest or the legitimate aims of the controller;
- a ban on purely automated decision-making using special categories of personal data;
- the right to demand intervention by the controller in the process of fully automated decision-making, to express one's position, and to challenge the decision if profiling is carried out on the basis of consent or for the purpose of concluding or performing a contract.

EU member states may provide additional guarantees of the data subject's rights in the case of access to fully automated decision-making systems. Malgieri notes that such guarantees have been reflected in a small number of countries and are of a "procedural" nature (Ireland), disclosing the requirements for the procedure for considering appeals and objections when using automated decision-making algorithms, or "proactive", eliminating gaps in the regulation of the GDPR [21] (the right to an explanation of algorithmic decisions based on the Code on Relations between the Public and the Administration of France).

In the United States, the procedure for processing personal information by federal executive bodies is regulated by the Privacy Act and The E-Government Act. Both acts have a number of shortcomings that hinder the effective protection of rights in the profiling process. The Privacy Act ensures the protection of only data that "reflect the characteristics and qualities of an individual", "therefore, an IP address, for example, is not subject to protection as a record, since it identifies the device, not the user" [22, p. 110]. Information is protected provided that it is part of the system of records and is retrieved through a person's identifier. The use of modern technologies makes it possible to process information and profile it without retrieving information through an identifier. The discrepancy between the law and modern realities is confirmed in the report of the US Government Accountability Office: among 25 agencies surveyed, the majority admitted that they did not use a personal identifier when collecting and processing information[5], thus depriving the subject of the information of the right to privacy.

The E-Government Act expanded the range of information considered confidential: an "identifiable form" is understood as " any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means", thus, geographic marks and other descriptors fall under the scope. However, the law does not set limits on the processing of digital information: if the Privacy Act obliges to collect the largest layer of necessary information directly from the subject, then the E-Government Act allows collecting information about individuals from various sources, including by purchasing commercial databases and combining them

[4] BGH, Urteil vom 28.01.2014 — VI ZR 156/13, BGHZ 200, 38 Rn. 24ff

[5] Federal Law Should Be Updated to Address Changing Technology Landscape. Statement of Gregory C. Wilshusen, Director Information Security Issues, 2012. P. 7.

ISSN 2542-1514 (Print)

with government databases. In the event that agencies systematically supplement their databases with databases containing information in identifiable form obtained from commercial or publicly available sources, they are required to conduct a privacy impact assessment and post information about the purposes and scope of digital data processing on their website (with a wide range of exceptions where such disclosure is not required). Thus, the area of digital unidentifiable traces remains a gap in legal regulation, which allows information to be collected without control by the data subject. When combined with the databases of the executive authorities themselves, digital unidentifiable traces can ensure the identification of a person and allow the creation of new personal data. Analysts note cases of cooperation between executive authorities and commercial database aggregators for scanning websites and purchasing an application for geolocating smartphones [23].

US state laws impose additional obligations on data processors when profiling:

1. To conduct a data protection assessment of data processed for profiling purposes if there are risks of unlawful actions.

2. To provide an opt-out function for fully automated profiling if it leads to “legal or other significant effects”, which means decisions on the provision or refusal to provide financial or credit services, housing, insurance, health care, access to essential goods and services, education, employment, or criminal prosecution.

Unlike EU countries, US states do not require consent or provide for the possibility to object to profiling. No US state guarantees the right of the data subject to receive information about the use of profiling algorithms and the principles of their operation, about what new data may be created. The right to “know” implies disclosure of reliable information about what data and from what sources are subject to collection, the purposes of processing, the storage period and the categories of information transferred to third parties with an indication of the purposes, the content of the rights of the data subject and the procedure for their implementation, including the right to refuse the processing of personal data for profiling purposes. Thus, the principle of transparency is not implemented [18, pp. 84–85], and data subjects cannot control newly created information about them. State legislation on the protection of personal data does not apply to the activities of state authorities and local governments; the process of personal profiling carried out by the latter is beyond the control of the data subject.

In China, fully automated decision-making methods using personal data are not prohibited, consent is not required, however, if profiling has a significant impact on the rights and interests of an individual, he or she has the right to demand an explanation and reject the decision taken. In accordance with Article 24 of the Law on the Protection of Personal Data, automated processing of personal data must ensure transparency of decision-making, fairness and impartiality. The law does not disclose the content of the transparency principle in relation to automated processing, in connection with which the general provisions of Article 17 on the need to disclose information on the purposes and method, the type and retention period of the processed personal information, and the procedure for exercising rights by an individual should be applied. Reference to the processing method allows us to conclude that information must be provided on the fact of using automated forms of decision making, on the personal data that will be processed, and as noted by Wu and Lin, “basic information about the algorithm used” [24, p. 1187]. The content of the right to an explanation is disclosed by researchers in different ways, depending on who is the subject of data processing - government agencies or commercial organizations. In the first case, the right to know implies the right to an explanation of the reasons for making a particular decision, which requires disclosure of the algorithm itself. In the case of profiling for commercial purposes, a person has the right to request only "an explanation of the basic circumstances of the algorithm used" due to the fact that the algorithm itself may be protected by a commercial secret [24, p. 1190]. The Provisions on the Management of Algorithmic Recommendations in Internet Information Services[6] emphasizes the advisory nature of optimizing the transparency and explainability of search, sorting, and selection rules in order to avoid negative impact and prevent disagreements. In accordance with paragraph 14 of the Provisions, the provider of algorithmic recommendations is also obliged to provide noticeable information about the fact of using algorithms, the intended purposes, and the main operating mechanisms, which allows "to eliminate the risks of unjustified refusals <…> to provide the necessary information, such as the scope of the algorithm, the user of the service, the risk level of the algorithm, and others, on the basis that there are no clear legislative provisions in this regard" [25, p. 350].

4. Conclusion

Approaches to regulating personal profiling differ significantly in the practice of foreign countries, while several trends can be identified:

- the formation of a broad concept of profiling, which allows the processing of most digital traces to be introduced into the legal field;

- differentiation of approaches to the implementation of the transparency principle depending on the purposes of profiling. In the EU and China, the use of automated decision-making algorithms imposes on public authorities an obligation to disclose the formula, ensure controllability of the data processing process, while the algorithm used for commercial purposes can be protected by secrecy. This approach seems justified, since the transparency of individual decision-making by government bodies is of particular importance for the individual. No less important is ensuring fair and transparent profiling by the private sector while maintaining a balance of interests of the parties, which involves the disclosure of complete and reliable information about the fact of profiling, the information processed, the purposes, and possible consequences, including the likelihood of generating new information about the individual, which requires precise and balanced wording. The presence of mandatory and recommended disclosure elements of profiling information in China seems to be quite an interesting approach, but the proposed wording lacks the necessary level of formal certainty, and therefore can be interpreted differently in practice. The most unfavorable is the legal regulation of profiling in the United States, since there are no special requirements for ensuring transparency of profiling in the activities of government agencies, which allows the latter to collect and form an unlimited amount of information about an individual. State legislation regulating profiling for commercial purposes also tends to upset the balance in favor of business: in most states, disclosure of the fact of profiling, its purposes and the information processed is necessary only when using an exclusively automated decision-making model, thus, even minor human participation in this process deprives an individual of the right to receive information

[6] Provisions on the Management of Algorithmic Recommendations in Internet Information Services, 2021.

ISSN 2542-1514 (Print)

about the fact of profiling, and also releases the data operator from the obligation to assess the risks of using algorithms.

- - the development of different approaches to the need to obtain consent for the use of fully automated decision-making algorithms for profiling purposes: in the United States and China, it is possible to refuse profiling (object to the application of the decision) if legal or other significant consequences for the individual arise, while in the European Union, as a general rule, it is necessary to obtain the individual's consent if the relevant consequences occur. It appears that the approach of European countries more carefully ensures a balance of interests of the parties to the legal relationship, which is also due to other grounds for profiling (for example, in the public interest), which are absent from the national legislation of the United States and China.

REFERENCES

1. Ramadan R.A. Big Data Tools – An Overview. *International Journal of Computer & Software Engineering*, 2017, vol. 2, art. 125. DOI: 10.15344/2456-4451/2017/125.

2. Teslenko I.B., Gubernatorov A.M., Digilina O.B., Krylov V.E. *Big Data*, Teaching aid. Vladimir, Vladimir State University named after Alexander and Nikolay Stoletovs publ., 2021. 123 p. (In Russ.).

3. Hildebrandt M., Gutwirth S. (eds.). *Profiling the European citizen: Cross-disciplinary perspectives*. Dordrecht, Springer Publ., 2008. 373 p. DOI: 10.1007/978-1-4020-6914-7.

4. Bakhteev D.V., Lednev I.V. The concept and characteristics of forensic profiling of the personality and behavior of an unknown offender. *Yuridicheskaya nauka i pravookhranitel'naya praktika = Legal Science and Law Enforcement Practice*, 2020, no. 3 (53), pp. 110–118. (In Russ.).

5. Petherick W., Brooks N. Reframing criminal profiling: a guide for integrated practice. *Psychiatry, Psychology and Law*, 2021, vol. 28, iss. 5, pp. 694–710. DOI: 10.1080/13218719.2020.1837030.

6. Ilina T. Approaching to Digital Profiling in the Financial Market. *Journal of Corporate Finance Research*, 2020, vol. 14, iss. 4, pp. 47–60.

7. Vinogradova E.V., Polyakova T.A., Minbaleev A.V. Digital profile: the concept, regulatory mechanisms and enforcement problems. *Pravoprimenenie = Law Enforcement Review*, 2021, vol. 5, iss. 4, pp. 5–19. DOI: 10.52468/2542-1514.2021.5(4).5-19.

8. Zharova A.K., Elin V.M., Minbaleev A.V. *The paradigm of digital profiling of human activity: risks, threats, crimes*, Monograph. Moscow, RUSAINS, 2022. 239 p. (In Russ.).

9. Mendoza I., Bygrave L.A. The Right Not to be Subject to Automated Decisions Based on Profiling, in: Synodinou T.E., Jougleux P., Markou C., Prastitou T. (eds.). *EU Internet Law*, Cham, Springer Publ., 2017, pp. 77–98. DOI: 10.1007/978-3-319-64955-9_4.

10. Alimov D.A. Transformation of the idea of subjective rights and freedoms in the conditions of digital reality, in: *Prava cheloveka v usloviyakh tsifrovoi transformatsii obshchestva i gosudarstva*, collected articles, Rostov-on-Don, Taganrog, Southern Federal University Publ., 2021, pp. 9–11. (In Russ.).

11. Menshikov Ya. Advantages of Automatic Data Collection in the Internet over Manual Data Collection. *Universum: tekhnicheskie nauki*, 2022, no. 10 (103), available at: https://7universum.com/ru/tech/archive/item/14383. (In Russ.).

12. Mochalov A.N. Digital Profile: Main Risks for Constitutional Human Rights in the face of Legal Uncertainty. *Lex Russica*, 2021, vol. 74, iss. 9, pp. 88–101. DOI: 10.17803/1729-5920.2021.178.9.088-101. (In Russ.).

13. Purificato E., Boratto L., De Luca E.W. *User Modelling and User Profiling: A Comprehensive Survey*, Preprint. February 21, 2024. 71 p. Available at: https://arxiv.org/pdf/2402.09660.

14. Corte L.D. Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, 2019, vol. 10, iss. 1, available at: https://ejlt.org/index.php/ejlt/article/view/672.

15. Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y. *Defining Profiling*, Working paper. December 11, 2013. 40 p. DOI: 10.2139/ssrn.2366564.

16. Adnan M., Rosi L., Veluru S., Mouseli M., Longley P.A., Rajarajan M. Using Digital Traces for User Profiling: The Uncertainty of Identity Toolset, in: *SIN '14*, The 7th International Conference on Security of Information and Networks, New York, ACM Publ., 2014, pp. 254–260. DOI: 10.1145/2659651.2659741.

17. Petrov A.A. Russian Matrix of the Digital Profile of the Russian. *Natsional'naya assotsiatsiya uchenykh*, 2020, no. 52, pp. 39–52. DOI: 10.31618/nas.2413-5291.2020.1.52.144. (In Russ.).

18. Mochalov A.N. Transparency of Algorithms as a Legal Principle of Automated Processing of Human Data. *Yuridicheskie issledovaniya*, 2023, no. 12, pp. 77–88. DOI: 10.25136/2409-7136.2023.12.69452. (In Russ.).

19. Barros Vale S., Zanfir-Fortuna G. *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*. Future of Privacy Forum Publ., 2022. 60 p. Available at: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

20. Foss-Solbrekk K. Searchlights across the black box: Trade secrecy versus access to information. *Computer Law & Security Review*, 2023, vol. 50, art. 105811. DOI: 10.1016/j.clsr.2023.105811.

21. 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, iss. 5, art. 105327. DOI:

10.1016/j.clsr.2019.05.002.

22. Salikov M.S. (ed.). *The right to access the Internet, anonymity and identification of users (constitutional legal problems)*. Yekaterinburg, Ural Polytechnic Institute Publ., 2020. 167 p. (In Russ.).

23. Lee N.T., Chin-Rothman C. Police surveillance and facial recognition: Why data privacy is imperative for communities of color. *Brookings*, April 12, 2022, available at: https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

24. Lin H., Wu H. A Right to an Explanation of Algorithmic Decision-Making in China. *Hong Kong Law Journal*, 2022, vol. 52, iss. 3, pp. 1163–1192.

25. Kharitonova Yu.S. Legal Means of Providing the Principle of Transparency of the Artificial Intelligence. *Journal of Digital Technologies and Law*, 2023, vol. 1, iss. 2, pp. 337–358. DOI: 10.21202/jdtl.2023.14.

INFORMATION ABOUT AUTHOR

Svetlana S. Kuznetsova – PhD in Law, Associate Professor; Associate Professor, Department of Constitutional Law
Ural State Law University named after V.F. Yakovlev
21, Komsomol'skaya ul., Yekaterinburg, 620137, Russia
E-mail: kss001@usla.ru
ORCID: 0000-0003-2426-8055
RSCI SPIN-code: 3387-9420; AuthorID: 804404

BIBLIOGRAPHIC DESCRIPTION

Kuznetsova S.S. Legal regulation of digital profiling of a person in the practice of foreign countries. *Pravoprimenenie = Law Enforcement Review*, 2024, vol. 8, no. 4, pp. 63–72. DOI: 10.52468/2542-1514.2024.8(4).63-72. (In Russ.).