The Bayes model for the protection of human interests

Anna Zharova[1,2], Vladimir Elin[2,3], Mikhail Levashov[2]
[1]Criminal Law Department, Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia
[2]Information Security Department, Financial University under the Government of the Russian Federation, Moscow, Russia
[3]Information Security Department, Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia

Article Info

Article history:

Received Dec 9, 2022
Revised Mar 13, 2023
Accepted Apr 7, 2023

Keywords:

Bayesian model
Digital profile
Human rights
Information security
Privacy

ABSTRACT

This article is aimed at solving a number of issues related to the problems, risks, and threats arising from the profiling of human activity. In this study, the Bayesian method was used, to determine the quantitative and qualitative characteristics of personal data for ensuring the security of this data by dint of reducing the redundancy of data processed by artificial intelligence (AI). A thought experiment to test the possibility of reducing the redundancy of personal data processed by AI allows us to conclude that using the Bayesian method allows to protect human rights to privacy. With this approach, instead of the method associated with the collection and accumulation of the most sensitive categories of personal data, we proposed a method that is associated with obtaining probabilistic estimates of the values of the parameters of these data by conducting statistical studies of the specified personal data without their collection and accumulation. The probabilistic estimates of the parameters of some sensitive personal data obtained in this way can replace their exact values and can be used by AI in the criteria for filtering personal data subjects, including for the purpose of making a decision.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Anna Zharova
Criminal Law Department, Institute of State and Law of the Russian Academy of Sciences
Znamenka 10 str., 119019, Moscow, Russian Federation
Email: anna_jarova@mail.ru

1. INTRODUCTION

People are becoming increasingly dependent on technology, not only in industrial relations but also at the individual level. Data about a person accumulated in information and communication technologies (ICT) is used by predictive modeling systems with elements of artificial intelligence (AI) [1]. AI sorts, analyzes, and builds connections between unstructured and disparate information, predicting human activities. Such actions affect individual interests since, on the basis of their results, AI can later make decisions. The analysis of personal data is carried out on an ongoing basis in order to make legally significant decisions [2], for example, the analysis of documents submitted for the purpose of obtaining a loan [3]. The use of AI has made it possible to significantly increase the amount of information processed, which requires reliable, non-redundant data, and relevant information. Such profiling and decision making based on AI predictions, having implications for individuals, can be interpreted as interference in a person's private sphere.

This article is aimed at solving a number of issues related to such problems as risks and threats arising from the profiling of human activity [2], [4]–[7] and lack of confidence in the algorithms of the decision-making system, and ensuring the necessity and sufficiency of the data being processed. The urgency of this problem is associated with the legal requirements for operators processing data on reducing personal data use and on the use of a specific list of personal data agreed in advance with the subject of personal data. These requirements are defined in both European [8], [9] and Russian legislation [10], [11]. In this regard, the authors of the article made an attempt to solve this complex social problem [12] using mathematical methods. The choice was made in favor of the Bayes methodology, since this method, unlike others, allows the model to be represented in the form of certain probabilities [13]. Using Bayes' theorem, we can find new information and measure the probability of occurrence of related events, this allows us to get closer to the classical estimate, and to combine existing a priori ideas about an object with sample information [14].

The authors do not pretend to be the final result, but only offer one of the possible options for solving a social problem using a mathematical method. In addition, a full-fledged solution, including the method proposed in the article, requires additional research and experiments. The value of our article lies in an attempt to bring up for discussion the idea of using the Bayesian calculation method to solve the problem of reducing personal data and thereby to provide ensuring the security of personal data, as well as implementing legal requirements for their targeted processing. The data were personal data related to age, region of residence in Russia, and the category of processed data (general and special). To conduct an analysis from a scientific and regulatory point of view, this article reviewed the literature, regulatory documents, and models for ensuring legal requirements are fulfilled by businesses.

The article consists of 5 sections. The introduction describes the main problems that the article addresses. Section 2 presents the research method. Section 3 reveals the regulation of using AI technology. Section 4 reveals the technological and instrumental solutions proposed for countering the risks and threats arising from the processing of personal data by decision-support and decision-making systems. The conclusion summarizes the results of the study.

2. RESEARCH METHOD

The work uses an empirical research method focused on ensuring the security of personal data processing using AI. In the analysis, methods of computer law, mathematical modeling, abstraction, and a thought experiment were used. The literature shows the most pressing research problems related to data security arise from the use of AI.

In order to eliminate the problem of redundancy of personal data, the authors used a statistical method, since the amount of information used to transmit or store data begins to exceed the information entropy of data accumulated by internet technologies. A large volume of personal data gives rise to adverse consequences in the form of anomalies (a set of problems) associated with illegal access to information, deletion of data, and their anomalous identification. In addition, the complexity of technological processes does not exclude the need to comply with the requirements of European and Russian legislation on the use of a specific list of personal data agreed in advance with the subject of personal data. In this regard, for statistical calculations, anonymized personal data was used, for the processing of which it is not required to obtain the consent of the subject of personal data. As a source of statistical information, we used open data posted on the website of the Federal Service for Technical and Export Control of Russia [15]. To build a theoretical model for reducing the redundancy of personal data when processed by AI, the most appropriate method for working with indirect and inaccurate data would be to conduct a mental experiment using a statistical method of technical diagnostics based on the generalized Bayesian formula, which allows the probability of an event in the presence of indirect and inaccurate data that must be determined [5], [6], [16]–[18].

3. RELATED WORK

In our article, a position of ensuring information security of a person through ensuring the security of his digital profile is considered. This problem is relevant since the implementation of human rights to privacy, personal and family secrets depends on information technologies (IT) models. This is studied in different positions; these are organizational, technological, and legal. However, now this problem is still little studied. We would like to note several scientific works in which solutions to the problem of ensuring human information security when using IT [19]. For example, organizations are encouraged to ensure the privacy of their employees using the PDGuard framework. Following a security-by-design approach, PDGuard shifts the challenge of managing personal data from the insurmountable challenge of controlling processes, operations, people, and the large software stack to auditing applications that use structure [20]. In another study, the authors suggest using structured threat information expression (STIX) technology. From their point of view, STIX allows to measure and visualize cyber threats and get a holistic view of cyber incidents [21]. The threat of confidentiality is associated with the fact that the sources of possible attacks are often hidden in the implementation details or even in the logic of the protocol, and not in the cryptographic guarantees of the encryption algorithms used. Information security of the IT user, authors proposed to be ensured by correcting defective procedures, taking into account confidentiality [22].

Ensuring confidentiality by data minimization was discussed in the analytical review [22]. The author of review concluded that at the moment there is no communication protocol that would provide a satisfactory level of accurate assessment and identification of the data required for processing [23]. In this connection, the authors proposed to use a common formal basis for the analysis and comparison of communication protocols. Determining the requirements for the security of personal data for the entire life cycle of technologies is a key requirement [5], and the Bayesian methodology [24] and the method differentiated confidentiality [25] were studied for the analysis of personal data in the social network [26], [27].

The presented works demonstrate a wide coverage of the problem of ensuring human information security and various methods of ensuring it, depending on the information technologies used. The scatter of the research topics presented allows us to conclude that solving this problem is a difficult task, relevant for many information technologies. In the process of finding solutions, various models are proposed, but each has its advantages and disadvantages. However, the person and ensuring their privacy during digitalization should remain at the center of the discussion.

4. RESULTS AND DISCUSSION

Information about individuals can be given in different ways. For example, a personal profile is created based on the semantic analysis of photos posted on the internet [6]. In the absence of the consent of the individuals, AI processes all possible information about them [28], [29]. The knowledge representation model is formed from rules and precedent. Rules are a way of presenting the basic knowledge of the subject area, which explain the occurrence of certain phenomena, making it possible to predict the development of a situation, allowing individual objects of the real world to be connected and display a decision-making model [30]–[32]. Logically ordered knowledge in the field of personal data security can be presented in the form of rules for:

- The allocation of personal data information systems;
- The classification of personal data information systems;
- Determining security threats;
- Determining the relevance of the threats;
- Choosing measures to protect personal data;
- Building a knowledge base;
- Evaluating efficiency and analyzing risks.

The simplest rules are in the form of a production model:

$$\text{«}\,IF\ \text{“A”}, THEN\ \text{“B”»}: R =< A1, A2, \ldots, An;\ B > \tag{1}$$

where *A1, …, An* are prerequisites for the rule to work, and *B* is the conclusion. The rule is triggered if all the prerequisites are met. Each prerequisite, *Ai*, is a simple “attribute-value” expression constructed using terms from domain ontology. The aggregate of personal data about the subject acts as attributes for decision-making.

It is believed that the technologies for collecting and processing information cannot be developed so that they could, at the stage of data collection, determine exactly which information is needed to make a decision. This is the reason for the collection of redundant personal data. The authors propose using a statistical method to determine the sufficiency of information. The method is based on a simple Bayesian formula: if there is a state D_i and a simple attribute k_j that occurs in this state, then the probability of the joint occurrence of events (the presence of the state D_i and the attribute k_j in the object) is determined by (2):

$$P(D_i \wedge k_j\ ) \ = P(D_i)\ P(k_i//D_i) \ = \ P(k_j)\, P(D_i/k_j) \tag{2}$$

where $P(D_i)$ is the probability of the state D_i, determined from static data. $P(k_j/D_i)$ is conditional probability of the appearance of the feature k_j provided that the object is in the state D_i; $P(k_j)$ is the probability of an object appearing k_j in all objects, regardless of the state of the object. $P(D_i/k_j)$ is conditional probability that an object has a state D_i provided that the sign appears k_j.

So, if N objects were previously examined and N_i the objects had the state D_i, then the probability is $P(D_i)$ state appearances D_i can be estimated by relative frequency:

$$P(D_i\ ) \approx \ N_i\ /\mathrm{N} \tag{3}$$

Similarly, if in N_{ij} objects with the state D_i a sign appeared k_j, then:

$$P\ (k_j/D_i) \approx N_{ij}/N_i \tag{4}$$

Suppose that out of the total N objects feature k_j was found in objects N_j, then:

$$P(k_j) \approx \frac{N_j}{\mathrm{N}} \tag{5}$$

Probability of condition D_i can be defined if there is an attribute k_j:

$$P(D_i/k_j) = P(D_i)\ \frac{\mathrm{P}(k_j/D_i)}{\mathrm{P}(k_j)} \tag{6}$$

At the same time, we do not fix the k_j attribute itself in relation to a specific subject of personal data. For example, such a sign may be a tendency to illegal human activity. A person does not provide such information within the framework of consent to the processing of personal data, this may be due to both the requirement of legislation and the unwillingness of the subject himself. However, understanding a person's propensity for a certain activity can be important for making a decision. Due to the requirement of the legislation that it is necessary to obtain written consent to the processing of sensitive personal data, we propose to solve this problem by applying a model that takes into account the requirement of the law and works with the relative frequencies of the appearance of a critical sign that affects decision-making.

In fact, the model we propose allows us to take into account the information traces left by a person on the internet. Information traces can be obtained from various available external sources, for example, social networks (without fixing the specific persons to whom the specified attribute belongs). The relative frequency of the appearance of the k_j sign in the personal data subject, whose consent to the processing of certain (insensitive) personal data we have received, will allow the decision-maker to decide on a specific decision.

The values on the right side of expression (6) can be estimated as follows. $P\ (k_j)$ allows us to determine the relative frequency of occurrence of a critical sign that affects decision-making. $P\ (k_j/D_i)$ is evaluated in the same way, but only those persons who have the state of D_i are selected in the assessed set of personal data subjects. And only for them the relative frequency of the appearance of the k_j. sign is calculated.

These relative frequencies (or sample probabilities) are used by AI to solve various problems. At the same time, the degree of proximity of the relative frequencies of events to their probabilities can be obtained based on the well-known [33] Bieneme-Chebyshev inequality. Let the unknown probability of the sign $P\ (k_j/D_i)$ is equal to q. Then this inequality can be written as (7):

$$P\ \{|\frac{N_{ij}}{Ni} - q| > e\} < q(1-q)/ne^2 < 1/4ne^2 \tag{7}$$

where n is the number of subjects that have the state i, e is an arbitrary arbitrarily small number. If in this expression, for example, choose e=0.1, then the right part of the expression (7) is equal to 25/n. That is, at n=\250, the probability of deviation of the relative frequency of the event in question from its theoretical probability will be no more than 0.1.

Thus, we can limit the amount of sensitive personal data collected by a particular person, sometimes completely refusing to process such data, using only calculated probabilistic estimates of the parameters of this data. By this method, we reduce the amount of personal data collected, thereby reducing their redundancy. Let's consider the possibility of practical application of this method in the analysis of personal data of the subject on which the AI should make a management decision. This may be a decision on a financial issue (granting a loan, the interest rate on it, the conditions for providing a bank card), on the issue of concluding a contract (hiring, buying/ selling goods or services), and so on.

For example, the subject provided his personal data: full name, age, region of residence, marital status and other information. But for AI to make a more informed decision, it is necessary to use special categories of personal data, which, in accordance with the law, the subject has the right not to provide. In this case, the AI evaluates the parameters of distributions associated with the possession of certain values of special categories of personal data by the desired subject. To evaluate these parameters, the AI searches for other (special) personal data from all sources, for example, in social networks, among subjects who have known (provided) personal data close to the subject under study, and builds a probabilistic model of whether the analyzed subject has these special personal data and their parameters, which may appear in unreliable subjects. Among the many individuals found by AI, whose parameters can be compared with the analyzed subject, the AI using (2)-(6) evaluates the values of the parameters of distributions of special categories of personal data, without fixing or storing them. At the same time, the AI evaluates only the relative frequencies of the necessary parameters, without collecting them. In the future, the AI taking into account the construction of confidence intervals for the parameters of the above distributions, can apply the obtained frequencies to make a control decision.

Using this method eliminates the need to collect unnecessary personal data when processing them using automated decision-making systems based on AI [26]. The method is applicable in the absence of a unified approach to managing a person's digital profile and is organized in such a way that ICT users have the right to consent or not to process personal data [30] and determine the value of information about themselves. At the same time, the logic of this algorithm can be disclosed to the subjects of personal data, implementing the requirement of the law on transparency of collected data and their processing. The model we offer analyzes personal data, but does not save it.

5. CONCLUSION

The issue of ensuring IoT security is given considerable attention in relation to all the participants in information processes. A number of significant problems have been identified, and the following solutions were identified: developing a system of industry regulation for the use of cyber-physical systems and requirements to identify participants in information interaction; determining the requirements for participants in the IoT and for the registration of equipment used in the IoT; developing a model of information security threats for IoT devices and systems; creating technology for handling information security incidents in the IoT; developing mechanisms for determining the degree of compliance with the requirements of Russian and international legislation, as well as industry, national, and international standards in information security; drafting security standards for IoT devices for subjects, processes, and technologies.

To ensure effective IoT security, it is necessary to consolidate the rules for disclosing data on IoT devices, the rules for their connection, and determine the requirements for the safe operation of networked devices. This paper presents a theoretical model for reducing the redundancy of collected personal data. The use of Bayesian methods in the operation of the support and decision-making system makes it possible to optimize the parameters of the personal data collected depending on the characteristics of the subjects. This approach simplifies the formation of a knowledge representation model. The methodology for calculating the quantitative and qualitative characteristics of personal data has been determined, using the example of selected 1,000 subjects of personal data, for 100 of which special categories of personal data were processed.

ACKNOWLEDGEMENTS

The article was prepared on the results of research carried out at the expense of budgetary funds under the state assignment of the Financial University.

REFERENCES

[1] X. Hu, B. Neupane, L. Flores, P. Sibal, and M. Rivera Lam, *Steering AI and advanced ICTs for knowledge societies: a rights, openness, access, and multi-stakeholder perspective (in Russian)*, *UNESCO*, 2020. Accessed: Mar 13, 2023. [Online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000374014?posInSet=1&queryId=N-EXPLORE-f4357445-8475-4526-b9ae-c29e5225b6b5

[2] K. Martin, "Ethical implications and accountability of algorithms," *Journal of Business Ethics*, vol. 160, no. 4, pp. 835–850, Dec. 2019, doi: 10.1007/s10551-018-3921-3.

[3] K. Ghaffari, M. Lagzian, M. Kazemi, and G. Malekzadeh, "A comprehensive framework for internet of things development," *Journal of Enterprise Information Management*, vol. 33, no. 1, pp. 23–50, Nov. 2019, doi: 10.1108/JEIM-02-2019-0060.

[4] A. Zharova, "The protect mobile user data in Russia," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3184–3192, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3184-3192.

[5] H.-C. Tsai, B.-W. Chen, J.-F. Wang, and A. Paul, "Enhanced long-range personal identification based on multimodal information of human features," *Multimedia Tools and Applications*, vol. 73, no. 1, pp. 291–307, Nov. 2014, doi: 10.1007/s11042-013-1606-6.

[6] P. Sandhaus and S. Boll, "Semantic analysis and retrieval in personal and social photo collections," *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 5–33, Jan. 2011, doi: 10.1007/s11042-010-0673-1.

[7] A. Parrott and L. Warshaw, "Industry 4.0 and the digital twin," *Deloitte Insights*, 2017. https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html (accessed Mar. 13, 2023).

[8] "Regulation (EU) 2016/679," *ogdpr.eu*, 2016. https://ogdpr.eu/en/gdpr-2016-679 (accessed Mar. 13, 2023).

[9] "Directive (EU) 2016/680," *ogdpr.eu*, 2016. https://ogdpr.eu/en/gdpr-2016-680 (accessed Mar. 13, 2023).

[10] "On the security of the critical information infrastructure of the Russian Federation (in Russian)," Resolution of the Government of the Russian Federation, 2018. Accessed: Mar 13, 2023. [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001201802130006

[11] V. V. Maslennikov *et al.*, “Assessment of Forecast of Social and Economic Development of the Russian Federation for 2019–2024 (September, 2019),” *Finance: Theory and Practice*, Vol. 23, No. 5, 2019. Accessed Jun. 21, 2023. [Online]. Available: https://financetp.fa.ru/jour/article/view/909/612?locale=en_US

[12] Z. Anna and E. Vladimir, “State regulation of the IoT in the Russian federation: fundamentals and challenges,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4542–4549, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4542-4549.

[13] J. M. Castelo Gómez, J. Carrillo Mondéjar, J. Roldán Gómez, and J. L. Martínez Martínez, “A context-centered methodology for IoT forensic investigations,” *International Journal of Information Security*, vol. 20, no. 5, pp. 647–673, Oct. 2021, doi: 10.1007/s10207-020-00523-6.

[14] N. Kewsuwun and S. Kajornkasirat, “A sentiment analysis model of Agritech startup on Facebook comments using naive Bayes classifier,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 2829–2838, Jun. 2022, doi: 10.11591/ijece.v12i3.pp2829-2838.

[15] “The basic model of threats to the security of personal data during their processing in personal data information systems,” *FSTEC*, 2008. Accessed Jun. 21, 2023. [Online]. Available: https: https://normativ.kontur.ru/document?moduleId=1&documentId=204882

[16] Á. Erdélyi, T. Winkler, and B. Rinner, “Privacy protection vs. utility in visual data,” *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2285–2312, Jan. 2018, doi: 10.1007/s11042-016-4337-7.

[17] I. Kayes and A. Iamnitchi, “Privacy and security in online social networks: a survey,” *Online Social Networks and Media*, vol. 3–4, pp. 1–21, Oct. 2017, doi: 10.1016/j.osnem.2017.09.001.

[18] A. Zharova, “Ensuring the information security of information communication technology users in Russia,” *International Journal of Cyber Criminology*, vol. 13, no. 2, pp. 255–269, 2019, doi: 10.5281/zenodo.3698141.

[19] Y. I. Alzoubi, A. Al-Ahmad, and A. Jaradat, “Fog computing security and privacy issues, open challenges, and blockchain solution: an overview,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5081–5088, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5081-5088.

[20] D. Mitropoulos, T. Sotiropoulos, N. Koutsovasilis, and D. Spinellis, “PDGuard: an architecture for the control and secure processing of personal data,” *International Journal of Information Security*, vol. 19, no. 4, pp. 479–498, Aug. 2020, doi: 10.1007/s10207-019-00468-5.

[21] R. Fattahi, R. Tavakkoli-Moghaddam, M. Khalilzadeh, N. Shahsavari-Pour, and R. Soltani, “A novel FMEA model based on fuzzy multiple-criteria decision-making methods for risk assessment,” *Journal of Enterprise Information Management*, vol. 33, no. 5, pp. 881–904, Dec. 2020, doi: 10.1108/JEIM-09-2019-0282.

[22] “Analytical review of big data market (in Russian),” *Moscow Exchange*. 2015. https://habr.com/ru/company/moex/blog/256747/ (accessed Aug. 16, 2023).

[23] P. Mavriki and M. Karyda, “Automated data-driven profiling: threats for group privacy,” *Information and Computer Security*, vol. 28, no. 2, pp. 183–197, Nov. 2019, doi: 10.1108/ICS-04-2019-0048.

[24] I. Deeva, P. D. Andriushchenko, A. V. Kalyuzhnaya, and A. V. Boukhanovsky, “Bayesian networks-based personal data synthesis,” in *Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good*, Sep. 2020, pp. 6–11, doi: 10.1145/3411170.3411243.

[25] J. Zhang, G. Cormode, C. M. Procopiuc, D. Srivastava, and X. Xiao, “PrivBayes: private data release via Bayesian,” in *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data*, Jun. 2014, pp. 1423–1434, doi: 10.1145/2588555.2588573.

[26] “Methodology for determining the current threats to the security of personal data during their processing in personal data information systems (in Russian),” FSTEC, 2021. Accessed: Jun. 21, 2023. [Online]. Available: https://zlonov.ru/assets/laws/Методика%20ФСТЭК%20России%20от%2005.02.2021.pdf

[27] X. Ding, H. Zhang, C. Ma, X. Zhang, and K. Zhong, “User identification across multiple social networks based on naive Bayes model,” *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–12, 2022, doi: 10.1109/TNNLS.2022.3202709.

[28] A. K. Zharova and V. M. Elin, “The use of big data: a russian perspective of personal data security,” *Computer Law and Security Review*, vol. 33, no. 4, pp. 482–501, Aug. 2017, doi: 10.1016/j.clsr.2017.03.025.

[29] R. Liss, “Criminal law in a world of states,” *Michigan Journal of International Law*, 2022, doi: 10.36642/mjil.43.2.criminal.

[30] T. Silva and J. Ma, “Expert profiling for collaborative innovation: big data perspective,” *Information Discovery and Delivery*, vol. 45, no. 4, pp. 169–180, Nov. 2017, doi: 10.1108/IDD-03-2017-0021.

[31] A. V. Kuyanova and A. E. Yuritsin, “Organizational-legal and tactical fundamentals of police activity on protection of public order and public safety,” *The Topical Issues of Public Law*. pp. 75–81, 2014.

[32] M. Almorsy, J. Grundy, and A. S. Ibrahim, “Automated software architecture security risk analysis using formalized signatures,” in *2013 35th International Conference on Software Engineering (ICSE)*, May 2013, pp. 662–671, doi: 10.1109/ICSE.2013.6606612.

[33] D. Dugué, *Treatise on theoretical and applied statistics: random analysis—random algebra*, (in French), Masson, Paris, 1958, Cambridge University Press, 2016.

BIOGRAPHIES OF AUTHORS

Anna Zharova holds a Doctor of Law in field information security. She is currently Director of the HSE Cyberspace Research Center, Russia, also Professor of Financial University under the Government of the Russian Federation and a research RAS. She is Editor-in-Chief of the Journal of Digital Technologies and Law. She can be contacted at email: anna_jarova@mail.ru.

Vladimir Elin holds a Candidate of Technical Sciences. In 1989, received the degree engineer in the field of aerospace. He is a currently an Associate Professor at the Department Information Security of the Financial University under the Government of the Russian Federation, also Kikot Moscow University of the Ministry of Internal Affairs of Russia. Author of a number of books and scientific research. He can be contacted at email: elin_vm@mail.ru.

Mikhail Levashov holds a Candidate of Physical and Mathematical Sciences. Currently, he is a professor at the Financial University, an expert of the Skolkovo Foundation. He can be contacted at email: michael.levashov@mail.ru.