Legal Issues in the Digital Age. 2023. Vol. 4. No. 1.
Вопросы права в цифровую эпоху. 2023. Т. 4. № 1.

Research article
УДК: 342
DOI:10.17323/2713-2749.2023.1.53.76

The Scope of the Personal Data Concept in Russia

Kyrill A. Zyubanov
National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia, kazyubanov@hse.ru, ORCID: 0000-0002-6752-0516

Abstract

Personal data as an institution is gaining increasing attention on the part of both public authorities, business structures and private individuals as subjects of personal data. Meanwhile, an efficient and successful usage of the tools provided by this institution directly depends on whether the scope of the personal data concept can be unambiguously defined. The paper describes the main problems resulting from a lack of uniform approach, makes a case for a cross-jurisdictional approach to interpretation of the concept of personal data, and identifies four main criteria which can provide a basis for a procedure for assessing whether certain information amounts to personal data: information, relevance, definability and subject criteria. In assuming a single source of the institution's regulation across jurisdictions, the cross-jurisdictional approach to interpretation of the concept of personal data allows to follow the best international practices to define the scope of the personal data concept. In this paper, the cross-jurisdictional approach was successfully applied with respect to the European law and international law instruments. The information and subject criteria set the constraints on the assessment of whether information amounts to personal data from the perspective of object and subject, respectively. In assessing the relevance of information as personal data, the relevance and the definability criteria allow to account for the context in terms of content, purpose pursued and results achieved. The proposed criteria applicable to information, relevance, definability and subject, being universal, allow to unambiguously determine the scope of personal data concept at the level of regulation, enforcement and compliance, as well as exercise of rights envisaged by the regulation in question. The said criteria also contribute the development of uniform terminology in the research community to ensure comparability of research concerning personal data through an overarching approach to the scope of this concept.

Keywords

personal data, privacy, privacy protection, terminology, comparative analysis, information technologies, information law.

For citation: Zyubanov K. A. (2023) The Scope of the Personal Data Concept in Russia. *Legal Issues in the Digital Age,* vol. 4, no. 1, pp. 53–76 (in English) DOI: 10.17323/2713-2749.2023.1.53.76

Introduction

The number of life spheres and market segments directly depending on the amount and quality of data for successful and sustainable development is on the rise. In the 21th century, it is inconceivable to take a lead in any market or sector, be it telemedicine, targeted marketing, artificial intelligence (AI) model training for various purposes, robotics, pharmaceutics etc. without a sufficient amount of data. The social relationships arising in these life spheres and market segments increasingly become subject to all sorts of scientific research.

With the importance of data recognized worldwide, countries are adopting national strategies applicable to data[1] and artificial intelligence[2]. Soft law regulation is also progressing, with an AI Code of Conduct drafted and signed by Russia's major AI developers in 2021 to establish, in particular, the principles of using data (including personal data) for the purpose of developing AI solutions.

Russian business has also adopted a Code of Ethics for the Use of Data, a soft law regulation maintained by the Big Data Association (BDA) jointly with the Institute of Internet Development. The document entitled "An industry self-regulatory act"[3] lays down "the main principles of working with data"[4].

[1] See, for example, National Data Strategy. Policy paper. UK Government. Available at: URL: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy (accessed: 22.02.2023)

[2] See, for example, Presidential Decree No. 490 "On Developing Artificial Intelligence in Russia" of 10 October 2019 // SPS Consultant Plus.

[3] BDA. Code of Ethics for the Use of Data // Available at: URL: https://rubda.ru/deyatelnost/kodeks/ (accessed: 01.03.2023)

[4] Ibid.

Personal data — "any information relating to an identified or identifiable individual"[5] or "any information relating to directly or indirectly identified or identifiable natural person[6] — is among the most sensitive data types. The analysis of the elements of this concept will be provided further in the text.

In 2023, according to the UNCTAD, regulation of data protection (including personal data) was effective in 137 out of 194 countries[7]. According to other data, (personal) data protection laws were adopted as of March 2022 in 157 countries, with regulation in the majority of them being similar to that effective in Europe [Greenleaf G., 2022: 3]. In Russia, the *lex specialis* regulation of (personal) data is ensured by Federal Law No. 149-FZ "On Information, Information Technologies and Data Protection" of 27 July 2006 (Law 149-FZ) and Federal Law No. 152-FZ "On Personal Data" of 27 July 2006 (Law 152-FZ).

However, regulation is not the cause but the effect of growing transactions with data, with the amount of data on the rise along with the number of sources of such data[8].

Back in 2018, analysts projected[9] the total amount of data to grow fivefold by 2025 — from 33 zettabyte to 175 zettabyte worldwide[10]. Moreover, the 2018 forecasts could not take into account the COVID-19 pandemic which broke out in 2020 resulting in an exponential growth of data. Thus, according to experts, more than 64 zettabyte of data were created/repli-

---

[5] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data (Strasburg, 28 January 1981) // SPS Consultant Plus; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[6] Federal Law No. 152-FZ "On Personal Data" of 27 July 2006 [hereinafter Law 152-FZ], para 1, Article 3 // SPS Consultant Plus.

[7] UNCTAD, Data Protection and Privacy Legislation Worldwide // United Nations Conference on Trade and Development. Available at: URL: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed: 22.02.2023)

[8] "Personal data processing" should be understood as any action/transaction involving personal data (see para 3, Article 3, Law 152-FZ).

[9] IDC White Paper. The Digitization of the World. Available at: URL: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (accessed: 25.02.2023)

[10] 1 zettabyte equals 1 trillion gigabyte or 10^{21} byte.

cated in 2020[11] which is almost double the amount created or replicated before 2018.

Apart from state-required identifiers (INN, OGRN, SNILS etc.), the data of individuals available to public authorities and/or businesses now include the data on communication devices used by individuals, their geolocation, purchase history, preferences of food, music and communication, as well as finger/voice prints, face geometry etc.

Moreover, the growth affects not just the amount of data but also the number of persons involved in data processing. Thus, the Federal Supervision Agency for Information Technologies and Communications (Roskomnadzor) reported back in July 2018 that "the number of personal data operators registered in the register [for personal data processing] is more than 397 thousand"[12] while as of 8 January 2022 personal data operator register ("PDOR") contained more than 434 thousand records of the registered operators[13].

The term "operator" is conceptually similar to the term "controller" used also in the European regulation that can be more familiar to the foreign explorers and practitioners. As estimated by Roskomnadzor, "there are over 6 million of organizations and private entrepreneurs [involved in personal data processing] in the territory of the Russian Federation"[14].

Research of related industries also demonstrates the range of IT penetration. A study conducted in August 2021 by Leichtman Research Group, an organization for analysis of the US broadcasting, media and recreation markets, showed that nearly 78 percent of families were signed to at least one streaming service. Such services process a significant amount of subscribers' personal data.

With the growth of personal data, increasing number of those who need such data for business, and the development speed of personal data law, the fundamental practical and doctrinal question is what personal data means.

---

[11] IDC. Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts, 2021. Available at: URL: https://www.idc.com/getdoc.jsp?containerId=prUS47560321 (accessed: 25.02.2023)

[12] Roskomnadzor. Registered personal data operators in excess of 397 thousand. Available at: URL: https://rkn.gov.ru/news/rsoc/news59260.htm (accessed: 01.04.2022)

[13] Roskomnadzor register of operators for personal data processing. Available at: URL: https://rkn.gov.ru/news/rsoc/news74048.htm (accessed: 25.02.2023)

[14] Roskomnadzor performance in 2021 for protection of rights and interests of individuals regarding personal data. Available at: URL: https://rkn.gov.ru/news/rsoc/news74048.htm (accessed: 25.02.2023)

In Russia, an entity processing personal data has to comply with numerous provisions of personal data law which normally require to considerably re-draft not only bylaws and agreements with customers and counterparties but also re-engineer corporate business processes and related information systems, with the cost of compliance to amount to millions or tens of millions depending on the scale and the extent of operations and specific industries.

For personal data subjects (individuals), the personal data law envisages a variety of rights and remedies including tools for control over one's personal data. In particular, a data subject has a right to know what kind of his personal data is processed by the organization in question, require to specify and update such data, and also prohibit such processing (except in cases provided by law). The remedies proposed by personal data regulation cannot be used unless subjects understand to what information they apply.

Understanding the personal data law is also crucially important for public authorities. In the context of separation of powers, the personal data law is simultaneously an object to be regulated by the legislative branch, enforced, and supervised by the executive branch, and interpreted and used for rendering justice by the judiciary branch.

Moreover, understanding the actual scope of personal data concept (hereinafter also referred to as the conceptual scope of personal data) as envisaged *de lege lata* is crucial for the execution of the above functions and duties. Where there is no such understanding of the personal data in law as a starting point, further progress in practice (legislative, enforcement) and theory (analysis, research) appears to be premature.

The relevance of that paper also comes from a lack of studies which would combine the latest theoretical framework with a practical form for solving both fundamental and applied issues. While normally focusing on narrower subjects, the available studies treat the concept of personal data *obiter dictum,* that is, incidentally [Saveliev A. I., 2018: 130], with the authors concluding on a need to either formally narrow down the concept of personal data [Burkova A. Yu., 2015: 21;]; [Naumov V.B., Arkhipov V.V., 2016: 190] or introduce "restrictive interpretation" [Miraev A.G., 2019: 80].

The above proposals to narrow down the conceptual scope of personal data through legislation or enforcement are barely acceptable since the underlying meaning, *raison d'etre* ("point of existence") of personal data concept and the regulation thereof do not assume nor accept restrictions.

Personal data is an institution designed to guarantee the exercise of the right to privacy, personal/family secret, and to provide data subjects with a minimum set of adequate data control tools optimally exercisable in the information society.

Nevertheless, there is one point in which these proposals elicit support: the concept of personal data needs to be transparent. This will be discussed further in the text.

Some authors point out that Russia's personal data law is catching up with that of Europe [Stepanov A. A., 2020: 93], a view possibly de facto correct from the perspective of the implementation speed of the relevant international law but wrong from a formally legal and historical standpoints since both the concept of personal data and the underlying legislation date back to 1995 when Federal Law No. 24-FZ "On Information, Information Technology and Data Protection" of 20 February 1995 (hereinafter Law 24-FZ) was approved. That Law preceded the currently effective regulation of personal data.

The branches of power perceive the conceptual scope of personal data each in a different way as reflected in the activities of their specific representatives. For example, in May 2022 the Council of Legislators under Russia's Federal Assembly accepted for consideration a draft law developed by the State Congress (Quriltai) of Bashkortostan, with "personal contact details" to be treated as a special category of personal data additionally protected by law[15].

In support of this proposal, it was stated that "[Law 152-FZ] does not have an exhaustive list of relevant details"[16] while "courts do not treat someone's phone number as personal data"[17]. Meanwhile, we believe the choice of tool to be wrong: the special personal data regime is not the primary criteria for treating information as personal data. The special category of personal data is a specific term compared to the general concept of personal data introduces higher requirements to the processing of such data considered more sensitive[18].

---

[15] Draft No. 8-111 "On Amending Article 10 of the Federal Law "On Personal Data" // Available at: URL: https://sozd.duma.gov.ru/bill/8-111 (accessed: 26.02.2023)

[16] Ibid. The explanatory note to the draft.

[17] Ibid.

[18] In Russia, special categories of personal data include those "concerning racial, ethnic origin, political views, religious or philosophic beliefs, health status, private life" (part 1, Article 10, Law 152-FZ).

The fact of proposing this tool to address the said problem points to a lack of uniform approach to the conceptual scope of personal data at the legislative level.

In its opinion to dismiss the draft, the Commission for Information Policies, IT and Investment of the Council of Legislators under the Federal Assembly, had referred, in particular, to Ministry of Communications Letter No. P11-15054-OG of 7 July 2017 explaining provisions of the federal law, something which shows, in combination with explanations of other regulatory and supervisory authorities, a lack of uniform approach at the executive level. Thus, as indicated in the Letter, while a subscriber's (telephone) number could be considered personal data, the Roskomnadzor in its numerous statements and answers to queries pointed out that a phone number can constitute personal data exclusively in combination with other information[19].

Likewise, there is no uniform approach to interpretation of conceptual scope of personal data at the judiciary level, i. e. in case law. Thus, specific decisions do not recognize the taxpayer identification number (TIN)[20] and family name with initials[21] as personal data. The immaturity and ambiguity of the Russian judicial practice is reflected at the doctrinal level as well [Saveliev A.I., 2021: 60]; [Stepanov A. A., 2020: 95]. However, a lack of uniform judicial practice seems to be the consequence of imperfect law and immature institution of personal date *per se* rather than a standalone phenomenon.

The above-described problem of the uncertain conceptual scope of personal data as reflected in the activities of each branch of power considerably hampers the exercise of rights by data subjects on the one side, compliance by data operators on the other side, and the application of legal provisions by competent authorities on the third side. If we apply the logical induction method to this point, it can be said that "personal data protection in Russia needs rethinking by all parties to this process" [Dmitrik N. A., 2020: 25].

One solution to the issue is to develop a uniform approach. This requires a methodological framework that would ensure consistent interpretation

[19] Including Answer to Query No. 88584-02-11/77 of 29 September 2021 // Author's personal contribution.

[20] Saint Petersburg City Court. Appellate decision of 3 February 2015. Case No. 2-3097/2014 // SPS Consultant Plus.

[21] Supreme Court of Tatarstan appellate decision of 24 October 2019 on case No. 2-5801/2019, 33-18168/2019 // SPS Consultant Plus.

of the conceptual scope of personal data for all of the above listed purposes (authorities, operators and individuals — data subjects).

Thus, this study is focused on the conceptual scope of personal data and its goal is to lay down a uniform approach to defining of that scope.

To achieve this goal as part of this study, it is necessary to identify the main approaches to defining the scope of this concept and to make proposals on how to improve the existing approaches and, finally, to develop a new, singular one for better operation of the institution of personal data in Russia.

The main methods used in the study included formal legal analysis of the legislation, enforcement and judicial practice, comparative analysis of approaches to the interpretation of conceptual scope of personal data in Russia and abroad, as well as historical method used as part of the analysis of the context in which the concept of personal data had emerged.

The Concept of Personal Data

To understand the conceptual scope of personal data, one should apply the historic method of research not to the history of this institution *per se* because this would extend the study beyond its purpose but to the origins of the definition of "personal data" as interpreted by both domestic and international researchers.

The Russian personal data law in its fundamental terminology follows the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108 (Convention 108). As such, Law 152-FZ was approved as part of the ratification procedure of Convention 108, being one of four drafts envisaged by Russian Government Instruction No. AZh-П4-3825[22].

As regards the definition of "personal data", Law 152-FZ was harmonized with Convention 108 as late as in 2011 when it was considerably amended[23] and the definition acquired its current form.

[22] Draft No. 217346-4 "On Ratification of the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data"; draft No. 217352-4 "On Personal Data"; draft No. 217354-4 "On Information, Information Technologies and Data Protection"; draft No. 217355-4 "On Amending Specific Regulations of the Russian Federation in connection with the adoption of the Federal Law "On Ratification of the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" and Federal Law "On Personal Data".

[23] Federal Law No. 261-FZ "On Amending the Federal Law "On Personal Data" of 25 July 2011 // SPS Consultant Plus.

In the European legislation, the main instrument governing personal data is Regulation No. 2016/679 of the European Parliament and of the Council of Europe "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" ("GDPR") also borrowed from Convention 108 an essentially identical definition but completed with a number of example to facilitate the understanding of its meaning.

Since Convention 108 and its protocols constitute a single instrument of international regulation, a cross-jurisdictional fundamental approach is applicable, in our view, to the conceptual scope of personal data, the cross-jurisdictional approach being the approach allowing for the use of foreign regulatory instruments as a means of interpretation also of the Russian personal data regulation. Despite numerous variations in more specific parts of this are of regulation, the concept of personal data is shared by many or even by a majority of jurisdictions just like the institution itself. This approach is adopted by the research community [Saveliev A.I., 2021: 62] and confirmed by the consistent stance of the Russian Federation in respect of Convention 108 and its protocols[24].

Before undertaking a more specific analysis, it is important to underline one element of the concept which is universal due to the nature of the institution itself as it facilitates the exercise of a number of human rights: only an individual could be a data subject enjoying all rights provided by personal data regulation — this constitutes what will be further referred to as the "subject criterion".

To effectively perform a proper analysis of the conceptual scope of personal data, it is of need to identify the core elements of this concept in a comparative legal context.

The shortest definition is given in Convention 108 where personal data means "any information related to an identified or identifiable individual".

The definition provided in the GDPR seems generally more specific: personal data means "any information concerning an identified or identifiable natural person" where "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identi-

[24] See Presidential Instruction No. 294-rp "On signing of the Protocol for amending the Convention for the protection of individuals with regard to automatic processing of personal data" of 10 October 2018 // SPS Consultant Plus.

fier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person".

Law 152-FZ apparently attempts to adapt the Convention 108 definition with a view to the legal, linguistic and semantic specifics: personal data is considered "any information related to a directly or indirectly identified or identifiable individual".

Instead of following one of the approaches of modern comparative studies in search of "legal institutions and provisions, different in their immediate content, [which] the authorities use to address the same social problems" [Syrykh V.M., 2012: 292], it would be more useful to assume the universality of the institution of personal data at least in the said sources and at least with regard to the definition of personal data. To establish this premise, we need to compare the fragments of three definitions of personal data and assess to what extent they are similar in terms of legal language and regulatory purpose.

The above comparison demonstrates minimum terminological differences *de jure*. Moreover, despite that this study also referred to the official translations of the said instruments into the Russian language, some differences are not found in the original texts. Thus, Convention 108 and GDPR contain definitions which differ in just one word: the former defines personal data as "any information relating to an identified or identifiable individual" while the latter as "any information relating to an identified or identifiable natural person", with explanation of who is "identifiable individual" also contained in the Explanatory Report[25] to the latest version of Convention 108 also endorsed by the Russian Federation.

The only point of possible controversy is what Table 1 describes as "definability criterion" since in spite of the originally (in the documents in English) identical definitions contained in both Convention 108 and GDPR, they clearly differ from the one contained in Law 152-FZ. However, as was stated above, we believe this difference to result from linguistic and semantic specifics rather than from diverging approaches to the conceptual scope of personal data.

The combination "identified or identifiable" exactly follows the logic behind the other definitions; meanwhile, the Russian definition adds "di-

[25] CETS. Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data § 17–18 // Council of Europe Treaty Series. No. 223.

Table 1. Comparison of the definitions of personal data contained in the Russian translations of the texts

Instrument	Information criterion	Relevance criterion	Definability criterion	Subject criterion
Convention 108	Any information	related	identified or identifiable	Individual
GDPR	Any information	concerning	identified or identifiable	Individual
Law 152-FZ	Any information	related	directly or indirectly identified or identifiable	Individual

rectly or indirectly" before the classical phrase "identified or identifiable". However, both Convention and GDPR include this element in their more specified approach to the definition of personal data: while Convention mentions it in the Explanatory Report[26] to the latest version to clarify the conceptual scope of "identifiable individual", the GDPR has it directly included into the text along with the phrase "directly or indirectly". As part of further analysis, this phrase is deemed to be covered by the scope of the relevance criterion in light of its nature and irrespective of the wording.

That is, if we imagine that all three definitions of personal data are used in English (original language for the both Convention 108 and GDPR, but not for Law 152-FZ), the differences could be removed altogether as demonstrated in Table 2 below.

Table 2. Comparison of the definitions of personal data in the English translations of the texts

Instrument	Criteria of information	Criteria of relevance	Criteria of definability	Criteria of subject
Convention 108	any information	relating to	an identified or identifiable	Individual
GDPR	any information	relating to	an identified or identifiable	natural person
Law 152-FZ author's t ranslation	any information	relating to	directly or indirectly identified or identifiable	natural person

[26] Ibid.

The above comparative legal analysis of the terminological framework of personal data regulation in Russia and abroad confirms again the possibility of cross-jurisdictional interpretation of the conceptual scope of personal data to define it on the basis of a uniform approach with a slight use of the Occam's razor principle, i. e. "entities must not be multiplied beyond necessity".

Two main approaches may be used to address the problem of uncertainty of the conceptual scope of personal data: a list-based and a criteria-based approach.

Under the list-based approach, the law should contain an exhaustive list of information types to be treated as personal data. This could potentially improve the legal certainty of personal data regulation *per se* while brutally undermining the extent of protection afforded to data subjects. Even with broader information categories replacing specific attributes (such as "contact details" instead of "mobile phone number"), the booming technological and information progress of the society will sooner or later result in new types of information outside the scope of personal data regulation but still allowing to identify and impact data subjects.

For this particular reason, it was stated already in the course of preparation of the European Parliament and Council of Europe Directive No. 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive No. 95/46), a pre-GDPR instrument for personal data regulation in Europe, that the definition of personal data should be as wide as possible to cover all information concerning or relating to an individual[27]. Later on, the European Data Protection Working Party noted that the definition of personal data contained in Directive 95/46 and similar to the above definitions should be applied "wide enough so that it can anticipate evolutions and catch all "shadow zones" within its scope"[28].

We believe the list-based approach to be potentially useful not for specifying the conceptual scope of personal data but for interpreting this concept exclusively in a non-exhaustive form (that is, with wordings such as "in particular", "including but not limited to" etc.). This approach, observed

[27] See COM (90) 314 final, 13.9.1990, p. 19 (commentary on Article 2); COM (92) 422 final, 28.10.1992, p. 10 (commentary on Article 2).

[28] Opinion 4/2007 On the concept of personal data. WP 136, 20 June 2007. Article 29 Data Protection Working Party. P. 5.

in the GDPR, was to some extent also present in Law 152-FZ before 2011. However, it can be used only at later development stages of personal data regulation because, if used at earlier stages, it could be perceived as the main approach, only to hamper the understanding of the conceptual scope of personal data.

In doctrine, the criteria-based approach enjoys wider support than the list-based approach. Thus, it has been asserted that "attempts to come up with sample lists of information to be treated as personal data… are doomed to failure because the personal data concept does not assume any list to be made" [Rozhkova M. et al., 2021: 130]; other authors argue that the list-based approach is impractical due to "a wide variety of relationships related to the processing of personal data and their rapid evolution characterized by the emergence of new data subjects and processing technologies" [Saveliev A.I., 2021: 70] and due to "the overall trend… towards a generalizing institution of personal data" [Bachilo I.L. et al., 2006: 19]. In this study, preference is made for the criteria-based approach as well.

Once the criteria-based approach to address the problem of uncertainty of the conceptual scope of personal data has been chosen as preferential, we need to assess each of the identified elements of this concept for uniform understanding of its scope.

a) "Any information"

"Personal data means any information…" as an element of the concept of personal data is at the heart of a majority of personal data regulations currently in effect. This element is not so much a criteria for establishing whether information amounts to personal data, but rather an indicator of the concept itself. It also serves to designate the legislator's will to "devise a wide concept of personal data and… apply a broader approach to its interpretation"[29].

In the Russian regulatory context, "information" should be understood as "details (messages, data)[30] irrespective of the form they are presented"[31]. Based on this definition, it can be concluded that personal data may be presented in any form (including text, graphics, photo, sound) and on any

[29] Ibid. P. 6.

[30] Whatever the effort, the translation here fails to be accurate for there is information is defined through its contextual synonym in the Russian regulatory framework information.

[31] Para 1, Article 2, Law 149-FZ.

media (including paper, flash card, computer memory)[32]. Also, it is of no importance whether this information is objective or subjective, or whether it is true or not — these criteria were left aside in designing the concept of personal data.

Nevertheless, even such a wide concept of "any information" specified not only in Russian regulatory instruments but also internationally allows to conclude that data should be somehow presented. Based on this approach, information not presented in any definite (including oral) form — assuming it is possible to confirm the information thus presented — is not to be protected as personal data.

b) "Relating to"

"Personal data means any information relating to…". The general approach to this element which can be called a "relevance criterion" suggests that personal data is information "about an individual"[33].

Meanwhile, as the analysis will demonstrate, the information to be protected as personal data may equally relate to objects, events, phenomena, and processes in the first place and only then to individuals[34].

An example of "classical" personal data relating to information "about an individual" is a combination of surname, first name and patronymic of a person or details of his/her income. Personal data relating to objects can be exemplified by an IMEI code of a mobile phone or IP address of a personal computer since these are technical details of devices or their operational artifacts in the first place.

A widespread approach to the understanding of the criteria of relevance with logical tools covering all possible cases of "relating" information to someone or something assumes the use of "content–purpose–result" triad[35] to describe the nature of such "relevance" depending on a particular case. One of the aspects of the triad — content of information, processing purpose or processing result — should be present for the criteria of relevance to be observed[36], making the triad a set of alternative tests.

---

[32] Opinion 4/2007 On the concept of personal data... P. 7–8.

[33] Ibid. P. 9.

[34] Ibid.

[35] Ibid.

[36] Ibid. P. 10.

The aspect of content serves to assess whether information can be qualified as personal data where information by its nature concerns, relates to or describes an individual. Moreover, in assessing the content of information one should, in our view, assume a literal interpretation of the said criteria.

The typical examples of information relating by its content to personal data would then be passport details or results of medical analysis that relate to an individual "by default". Where this aspect is used, no account is made of either the purpose of processing or the extent it affects the data subject.

An exception from this aspect's application can readily be made for the data called "synthetic data" however we maintain that the issue of the interplay of the two concepts the second one being the personal data concept shall be subject to separate research. Yet, even for the "synthetic data" case does certainly fall within the scope of the following two aspects.

The "purpose of processing" is an independent aspect of assessing relevance to personal data irrespective of whether the content of such information concerns, relates to or describes an individual. The criteria of relevance will be satisfied with regard to purpose where the purpose of processing this or another information is to impact an individual in any way regardless of the extent or the scale of such impact.

A typical example of situations with the purpose as a main aspect is processing of information on operations with specific elements of a web interface, as well as on navigating from one web page to another when this information serves to identify the user among others (for example, by displaying to him/her a targeted advertisement).

Another example is corporate monitoring of the use of office equipment by workers: while the information on what documents were printed out relates to the documents in the first place, the purpose can be to identify unduly performance of job duties.

The "result" of personal data processing can also constitute a predominant aspect in assessing the relevance of information to personal data regardless of the content and purpose of such processing. This aspect serves as an additional filter designed to mitigate the risk of narrowing the scope of personal data regulation without good reason. According to the result criteria, personal data is information that, while not related to an individual by its content and not processed with the purpose of impacting a data subject in first place, will generate a result capable of affecting the rights, liberties and legitimate interests of a data subject.

Despite that this aspect is described as a kind of "filter", examples of its use are quite frequent to include monitoring of company vehicles for fuel consumption to timely identify fuel pump malfunctions or monitoring of taxis' position in order to optimize itineraries and reduce waiting time etc. While this information relates to cars and serves a technical purpose, it can be used to assess driver performance and make decisions affecting their employment.

Thus, information will be deemed relating to an individual if this follows from its content, purpose or result of processing. It is again noteworthy that these aspects should be understood as alternative rather than cumulative: any of them, if present, will suffice.

While this approach may seem unreasonably broad, one should bear in mind that the institution of personal data is designed to protect the rights, liberties and legitimate interests of data subjects, and thus should undoubtedly demonstrate "a substantial degree of flexibility, so as to strike the appropriate balance between protection of the data subject's rights and the legitimate interests of data controllers third parties and the public interest"[37], to be achieved through regulation applicable to all possible cases of personal data processing rather than artificial narrowing of the regulatory scope. The paragraph above shall be considered one of the most core elements of the case the author attempts to make.

Moreover, the adoption of such approach by specific representatives of the executive authorities is confirmed by the Roskomnadzor's position whereby "the principle of identifying individuals by their full name from the whole stock of data is not the only possible criteria to relate processed information to personal data"[38].

Since the so-called inference economy is currently gaining momentum [Solow-Niederman A., 2022: 117], with some authors, in view of the capabilities of big data technologies to make conclusions on specific persons, even asserting that "in the age of inference almost all data are sensitive" [Solove D., 2023: 18], a restrictive interpretation of the conceptual scope of personal data can obstruct the exercise of data subjects' rights even more than its uncertainty.

[37] Ibid. P. 5.

[38] Roskomnadzor letter No. 08AP-6054 "On consideration of the Treasury of Russia's query" of 20 January 2017 // SPS Consultant Plus.

c)"Identified or identifiable natural person"

"Personal data means any information relating to an identified or identifiable individual". Once we have determined what personal data means (any information) and how it is related to specific individuals (relevance criterion), we need to clear out the meaning of such elements of this concept as "defined natural person" and "definable natural person".

In this study, the use of the terms "defined" and "definable" instead of, for example, "identified" and "identifiable" does not mean that the author makes any difference between the definitions of Law 152-FZ and GDPR/ Convention 108 has been described in the analysis above. This terminology allows to make abstraction of unreasonable over-utilization of terminological frameworks proper to specific branches of law that contain legal definitions of the term "identification"[39].

These elements obviously differ in the "identifying potential" of information [Saveliev A.I., 2021: 61] in each particular case, that is, how fully and exactly it can relate to a natural person.

This criterion — to be called the "definability criterion" — is the most difficult to grasp due to subjectivity and dependence on both particular attributes contained in information and the processing context in each specific case. Nevertheless, we should attempt to systematize and clarify this concept, otherwise the purpose of the study will not be achieved.

This criterion is essentially evaluative not *per se* but with regard to the extent a natural person to whom information is related is *specific* and *distinguished* from the group he/she is part of. That is, the definability criterion is largely a measure of the relevance criterion.

Thus, an individual — data subject — will be deemed "defined" where he/she is singled out of the group he/she is part of (for example, users of the same online service) in the specific personal data processing procedure. That is, for sending a personal message to a web service user with a proposal to test a new version of the service, the administrator will distinguish the user on the basis of the available data and thus will process his/her personal data. In similar terms, someone receiving a marketing SMS with

[39] See, for example, Federal Law No. 115-FZ "On the Prevention of Legalization (Laundering) of Criminal Proceeds and Financing of Terrorism" of 7 August 2001 // SPS ConsultantPlus.

a personal proposal to visit a beauty parlor recently opened next door will be deemed "defined".

It is noteworthy that the above examples have a full triad of the relevance criterion: content of information is highly indicative of an individual (account with a web service, mobile phone number), purpose of processing envisages interaction with a data subject (respectively, service test or beauty parlor invitation) while the result implies a direct impact on the data subject (respectively, via a web service message or SMS).

It is argued that a "defined" individual can be only the one whose full name (if any) is known, but this approach appears unreasonably restrictive because it falls short of the regulatory purpose. Moreover, this argument contradicts the basic understanding that "the phrase on indirect definability of an individual on the basis of such data added to the definition will trigger a wider approach to interpretation of the concept of personal data" [Saveliev A.I., 2020: 85; 2021: 65]. A data subject could be "defined" beyond doubt using a variety of attributes not explicitly related to his/her name including, for example, a mobile phone number which allows to call someone directly without even knowing his/her name. This position is adopted in both European[40] and national[41] enforcement practices.

As for situations where an individual is deemed definable rather than defined, one should adopt a more comprehensive approach than the one which clearly distinguishes an individual within a group as was possible with a defined individual. Under the basic approach, a "definable" individual is the one who can be "defined" based on the concept of defined individual as distinguished from the group he/she is part of; but the accuracy of such definition is lower than in respect of a "defined individual".

To systemically and consistently approach the cases where an individual is deemed "definable" with information relating to him/her deemed personal data, it is needed to return to the criteria-based approach. As was stated above, definability criterion largely becomes a measure of the relevance criterion; however the opposite is also true since the triad explicating the relevance criterion can provide that of definability with tools for interpreting the concept of "definable individual".

[40] Judgment of the European Court of Justice C-101/2001of 06.11.2003 (Lindqvist), §27.

[41] Roskomnadzor letter No. 08AP-6054 "On consideration of the Treasury of Russia's query" of 20 January 2017 // SPS Consultant Plus.

Thus, a "definable" individual will be the one who, while probably not being clearly distinguished in the group he/she is part of, will exhibit information ("any information") allowing to individualize him/her or single out of the group or else to at least narrow down the group (for example, when it is possible to identify how specific data relate to a particular family or household).

Meanwhile, once a uniform methodology is not there, this approach does not allow to come up with a sustainable test for applicability of this conceptual element of personal data. The reason is dependence of an individual's "definability" on the processing context[42] rightly euphemized in law by the purpose of processing [Dmitrik N.A., 2020: 31]. The context does not only assume specific description of a place (circumstances) *per se* but also particular political, social and cultural expectations from the place (circumstances) [Nissenbaum H., 2004: 119].

We believe it possible to re-use the "content–purpose–result" triad of the relevance criterion to adequately take into account the dependence of "definability" on the processing context but in accounting for a number of peculiarities of such re-use characteristic of the definability criterion as such. The three aspects of the triad should be also understood as alternative and not necessarily cumulative.

In this case, the content aspect as a qualifying factor should be provided with additional tools to determine whether the information is associated with a specific individual rather than a "natural person" in principle. This could be done through an analysis of the means [Saveliev A. I., 2021: 63] used to process the information. Thus, the content of information will be deemed relating to the "definable individual" where in view of the required time, effort and other resources and the means reasonably likely[43] to be used[44] such information may be "associated" with a particular person in-

[42] See, for example, CETS 223 Explanatory Report. P. 3; Opinion 4/2007 On the concept of personal data. WP 136, 20 June 2007. Article 29 Data Protection Working Party. P. 13.

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter — GDPR), Recital 26 // EUR-Lex European Union Law. Available at: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (accessed: 04.03.2023)

[44] The study supports an argument that one should take into account not only the means available to someone who analyzes whether the personal data regime is applicable to certain information but also legitimately available means including those in possession of third parties, see. GDPR. Recital 26; Patrick Breyer v. Bundesrepublik Deutschland, ECJ, Case C-582/14, 19 October 2016, § 41.

cluding where his/her name and other attributes clearly identifying an individual cannot be indicated.

A.I. Saveliev pointed out a classic case of applicability of this criterion — associating traffic meta-data (in particular, details of established connections with timing and duration, numbers or IP addresses of the communicating devices) with personal data [Saveliev A.I., 2021: 72] as they may be used to determine political, religious, sexual and other preferences and opinions of a data subject as well as other data[45].

Adding to the list of examples, D. Solove indicates that religious opinions could be determined by the data on taste preferences and visited religious/political events identified on the basis of location data [Solove D., 2023: 22].

As equally relevant for "defined" and "definable" individuals, it is worth noting that when we refer to "defining" as a procedure which, depending on the degree of completion, leads to different conceptual elements of personal data we speak not only about "civic or legal identity"[46] but also about any means which allow to "individualize or single out"[47] a person within a group including anything allowing to treat such individual in a special way.

The aspects of purpose and result should be applied without specification. Thus, information will be deemed relating to a "definable individual" where the purpose or result of processing is to "individualize or single out" an individual within a group, narrow this group down, or use a "special interaction model" in his respect[48].

A defined individual will thus be the one clearly distinguished in the group he/she is part of, while a definable individual the one with respect to whom the information is at hand to be used to single him/her out of the

[45] Mayer J. et al. Evaluating the Privacy Properties of Telephone Metadata. Stanford University. 1 March 2016. Available at: URL: http://www.pnas.org/content/113/20/5536 (accessed: 30.05.2021)

[46] CETS 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // Council of Europe Treaty Series (hereinafter — CETS 223 Explanatory Report). Available at: URL: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (accessed: 03.03.2023)

[47] Ibid.

[48] A.I. Saveliev provides a good original translation of a term "treat differently" contained in CETS 223 Explanatory Report, see. CETS 223 Explanatory Report, p. 3; Saveliev A. I. Article-by-Article Commentary of the Federal Law on Personal Data for Research and Practical Purposes, comment to Article 3. Moscow, 2021.

group or narrow down the group or processed in a way (with a view to the purpose and/or result of such processing) as to impact such individual regardless of the extent of definition (including when all of the above is done in respect of a family or household).

One can also conclude that where the aspects of purpose and/or result from the "content — purpose — result" triad are considered applicable at the stage of the assessment under the relevance criterion, no specific assessment under the definability criterion will be necessary. Once other criteria are observed, such data should be deemed personal data.

Conclusion

The amount of processed personal data is invariably growing worldwide just like the number of data subjects, those involved in data processing and the methods they apply. Regulation of personal data processing is inextricably linked with guarantees of one of the crucial and vulnerable human rights in the 21th century, the right to privacy, personal and family secret. Thus, any drawback, shortcoming and even linguistic inaccuracy can result in major issues both for public authorities, companies required to comply with relevant provisions, and data subjects.

The personal data law in Russia, while rapidly progressing, is arguably not consistent enough. This results in a regulatory framework at the same time widely applicable, subject to increasing public supervision (control) and raising a growing number of questions for those whom it targets (personal data operators). In particular, there is no uniform approach to the definition of the scope of the personal data concept, nor there is a methodological framework to support the development of such approach for public authorities, personal data operators and data subjects (individuals).

However, this problem is solvable, with a uniform approach to the definition of conceptual scope of personal data being developed on the basis of the existing regulation, major doctrinal approaches to the study of the institution of personal data and, particularly, the conceptual scope of personal data with reliance on cross-jurisdictional application of fundamental approaches to the problem in question.

Based on the identified conceptual elements of personal data, criteria were proposed to significantly reduce the risk of ambiguous interpretation both in the legislative process and at the level of executive and judiciary authorities, and to ensure overall understanding of the basic terminology

of the institution of personal data within the research community. Thus, of 4 basic criteria being proposed, each was provided with an original or updated methodology of relevance for both practice and research.

The first criteria, that of information, restricts the conceptual scope from the perspective of the nature of content: personal data could be only something which is information.

The second criteria, that of relevance, does the same by requiring to identify a link between the information subject to analysis and an individual. Formal and functional at the same time, it is explicated by the "content–purpose–result" triad. Information will satisfy this criteria where it is essentially relevant to an individual (at this stage, regardless of the extent of the individual's definability) and processed to impact a data subject or in such a way as to affect his/her rights, liberties or legitimate interests.

The third — last but one — criterion, that of definability, is the most difficult to grasp as a conceptual element of personal data relating to the extent an individual is definable. An individual can be "defined" or "definable" depending on the extent of completeness of the "identification" procedure and definiteness of its result. As such, a "defined individual" is the one distinguished in the group he/she is part of (for example, by reference to passport details or other attributes clearly associated with him/her). Also, an individual can be "definable", with the "content — purpose — result" triad re-applied to explicate this aspect of the definability criterion. The aspect of content was modified to determine the relevance to a specific individual rather than generally to a natural person using the means which "reasonably likely" can be used to identify a specific person. Two other aspects of the triad — purpose and result — do not change.

As a matter of conclusion, where information and its processing satisfy the requirements of purpose and/or result, no specific assessment under the definability criterion will be necessary.

The fourth criterion, that of subject, allows to identify the main *beneficiary* of regulation who cannot be other than the individual to whom the information under analysis is related. This, however, does not mean that information relating to a legal entity cannot constitute personal data of a natural person (for example, the entity's business name can be specified as the place of employment).

The above criteria, being universal, can be applied by both public authorities and business entities to resolve controversies in the process of im-

plementation of functions and duties, as well as by data subjects to protect their rights, and in the field of research.

Despite that this approach can be criticized for too broad interpretation of the conceptual scope of personal data, we believe that the solution to problems of business entities arising from restricted access to data and various constraints for their use in business processes should arise from within the regulation, i. e. not avoiding or circumventing it by means of restrictive interpretation.

Meanwhile, it is worth pointing out that broader interpretation does not pose a danger but rather provides an incentive for the regulatory and functional enhancement for the legislative, executive and judiciary branches of power.

References

1. Bachilo I.L. et al. (2006) Personal data in the structure of information resources. Principles of regulation. Minsk: Bellitfond, 474 p. (in Russ.)

2. Burkova A.Yu. (2015) Defining the concept of personal data. *Pravo i ekonomika*=Law and Economics, no. 4, pp. 20–24 (in Russ.)

3. Dmitrik N.A. (2020) The history, meaning and prospects of the institution of personal data. *Vestnik grazhdanskogo prava*=Bulletin of Civil Law, no. 3, pp. 43–82 (in Russ.)

4. Greenleaf G. (2021) Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. 169 Privacy Laws & Business International Report. UNSW Law Research Paper No. 21-60 Available at: URL: SSRN: https://ssrn.com/abstract=3836348 (accessed: 03.03.2023)

5. Greenleaf G. (2022) Now 157 Countries: Twelve Data Privacy Laws in 2021/22. 176 Privacy Laws & Business International Report. UNSW Law Research, Available at: URL: SSRN: https://ssrn.com/abstract=4137418 (accessed: 10.03.2023)

6. Mayer J. et al. (2016) Evaluating the Privacy Properties of Telephone Metadata. Stanford University. 1 March 2016. Available at: URL: http://www.pnas.org/content/113/20/5536 (accessed: 03.03.2023)

7. Miraev A.G. (2019)The concept of personal data in Russia and European Union. *Yuridicheskaya nauka*=Legal Science, no. 5, pp. 72–83 (in Russ.)

8. Naumov V.B., Arkhipov V.V. (2016) The concept of personal data: interpretation in the context of information and communication technologies

progress. *Rossiyskiy juridicheskiy zhurnal*=Russian Law Journal, no. 2, pp. 186–196 (in Russ.)

9. Nissenbaum H. (2004) Privacy as contextual integrity. *Washington Law Review*, vol. 79, issue 1, pp. 119–158.

10. Rozhkova M. et al. (2021) *Personal and non-personal data. Legal aspects of digital technologies used in business operations.* Moscow: Statut, pp. 127–133 (in Russ.)

11. Saveliev A.I. (2020) The civil law aspects of data regulation in the context of attempts to build a digital economy. *Vestnik grazhdanskogo prava*=Bulletin of Civil War, no. 1, pp. 60–92 (in Russ.)

12. Saveliev A.I. (2021) The article-by-article commentary to the law on personal data. Moscow: Statut, 258 p. (in Russ.)

13. Saveliev A.I. (2018) Big data regulation and privacy protection in a new economic reality. *Zakon*=Law, no. 5, pp. 122–144 (in Russ.)

14. Solove D. (2022) Data is what data does: regulating use, harm, and risk instead of sensitive data. Available at: URL: SSRN: https://ssrn.com/abstract=4322198 (accessed: 03.03.2023)

15. Solow-Niederman A. (2021) Information Privacy and the Inference Economy. Available at: URL: SSRN: https://ssrn.com/abstract=3921003 (accessed: 10.03.2023)

16. Stepanov A.A. (2020) The content of personal date in the legislation of Russia and European Union. *Obrazovaniye i pravo*=Education and Law, no. 9, pp. 92–99 (in Russ.)

17. Syrykh V.M. (2012) The history and methodology of jurisprudence: a manual. Moscow: Norma, 464 p. (in Russ.)

Information about the author:

K.A. Zyubanov — Postgraduate Student.

The article was submitted to the editorial office 02.02.2023; approved after reviewing 28.02.2023; accepted for publication 03.03.2023.