Protection of personal data in databases and computer programs

Alexey Borisov[1,*] and *Sayaana* Danilova[1]

[1]North-Eastern Federal University, 58 Belinsky str, Yakutsk, Republic of Sakha (Yakutia), Russia, 677027

Abstract. At the beginning of the article describes what restrictions caused the pandemic in 2020 caused by a new coronovirus infection the COVID-19. The article discusses the legitimacy of the processing of personal data using databases and programs, in particular, the problems of building, using and transmitting a database containing PD; storing PD in «cloud bases»; PD protection after database destruction. Comparative legal analysis of this institution in European and American legislation is carried out. In conclusion, it should be noted that the legislator understands the need to protect PD and is therefore taking appropriate measures to ensure the proper technical level of operators. At the end conclusions were drawn on this topic of the study.

1 Introduction

The COVID-19 pandemic in 2020 caused significant restrictions on citizens to stop the virus spreading, including restrictions on freedom of movement and the right to privacy. The restrictions affected a number of legal issues, in particular the use and protection of personal data (hereinafter referred as PD) that was processed in special databases and computer programs. For example, the Moscow City Health Department issued an order requiring residents who fell ill with a coronavirus infection to use the remote medical service TMIS (telemedicine information system) and special "Social Monitoring" software, i.e. the database and programs collecting the PD of the ill person.

There were many problems with the software, both on the technical side, such as geolocation when connecting to different towers from the same flat, and on the legal side, such as the consent to process personal data in the "Social Monitoring" software provided for the transfer of PD for 10 years, although the application itself was temporary and limited to quarantine periods; there was also the issue of PD protection, particularly storage security and its destruction after the end of the pandemic. It should be noted that consent was often given by individuals under threat of denial of health services or ill-health [2].

On the one hand, personal data may also be processed without the subject's consent in cases where it is necessary to protect life and health according to the Law “On Personal Data”, but the processing must be limited to that purpose, which is clearly not the case for the stated 10 years. It is possible that in the future this will lead to legal action to withdraw

* Corresponding author: tbbai@mail.ru

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

such consents by their subjects and to demand that the data processing cease. However, it should be noted that the institution of medical secrecy has been extended to the above relationship, which also aims to protect the data of a sick person, as the Constitutional Court of the Russian Federation pointed out in Ruling No 1176-O1 of July 16, 2013. This ensures that the data transmitted will not be used for unlawful purposes.

2 Problem statement

Let's talk about the legality of such PD processing, what requirements databases and programs must meet in the context of Russian and foreign legislation on this issue. The question of databases is discussed due to the fact that data storage is carried out with the help of databases in the age of digitalization. The legal definition of database is contained in paragraph 2, item 2, article 1260 of the Civil Code of the Russian Federation, which emphasizes that the basic element of protection in database is the systematization in a certain way, so that the materials included in it may be found and processed by a computer program. We can see a similar definition both in international acts and in the legislation of foreign countries [3].

Therefore, databases can be thought of as a complex object of intellectual property rights, a feature of which is the extension of its own protection regime to its constituent objects. In our case, these are PD, which are protected under the Federal Law of 27 July No. 152-FL "On Personal Data", which provides for a database with PD under the name "personal data information system". Recently, databases have gradually begun to take on a "cloud" appearance, so let's consider the characteristics of cloud services in details. Cloud services have appeared recently, so law and order, both Russian and foreign, have not provided a legal definition of them yet. However, the most comprehensive definition has been provided by the US National Institute of Standards and Technology.

Thus, "cloud service" is defined as "a model for providing convenient on-demand network access to a shared set of configurable computing resources that can be quickly deployed and released with minimal interaction with the service provider and minimal in-house management effort". So, cloud services can also be used as database, but no distinction will be made here between "cloud" and "classic" databases and software as most jurisdictions have absolutely identical requirements, which will be discussed below. The Russian legislator establishes a number of technical criteria for databases and programs which are prerequisite for processing PD.

These are contained in the bylaws of the executive branch of the Russian Federation. Such requirements may include anti-virus protection; intrusion prevention; "software environment restriction" (software startup management, software installation management, temporary file management), etc. There is also a differentiation of database protection requirements into four levels depending on the PD stored in them. In other words, it can be said that the legislator has taken the necessary measures to regulate the level of technical protection of databases. Moreover, one of the criteria can be identified as the technical capacity of the operator to ensure continuous access by law enforcement authorities to the databases containing the PD. This obligation is enshrined in the Rules approved by the Government [1].

The Supreme Court of the Russian Federation has recognized this provision as fully in force, so an operator who evades this obligation is liable in accordance with Article 13.11 of the CAO RF. The European legislator in the GDPR has also provided for certain functions for databases and programs, the failure to perform which results in the prohibition of PD processing. For example, this is the ability to pseudonymize and cryptographically protect PD; the ability to guarantee permanent confidentiality. There is a certification institute, and there is collaboration with technical universities on these matters. And UK legislation is

moving faster than the European legislation and introducing new, more advanced conditions for technical protection of PD. Thus, we can say that the level of admissibility of databases in Europe is comparable to that of the Russian Federation.

3 Findings

Let's consider the specifics of creating databases containing PD. In terms of intellectual property law, there is no difference between creating databases for different purposes. Thus, database can be created by an author for himself/herself; under a contract for a customer; in the performance of his/her official duties by an employer as a work of service; and under a government contract (Figure 1).

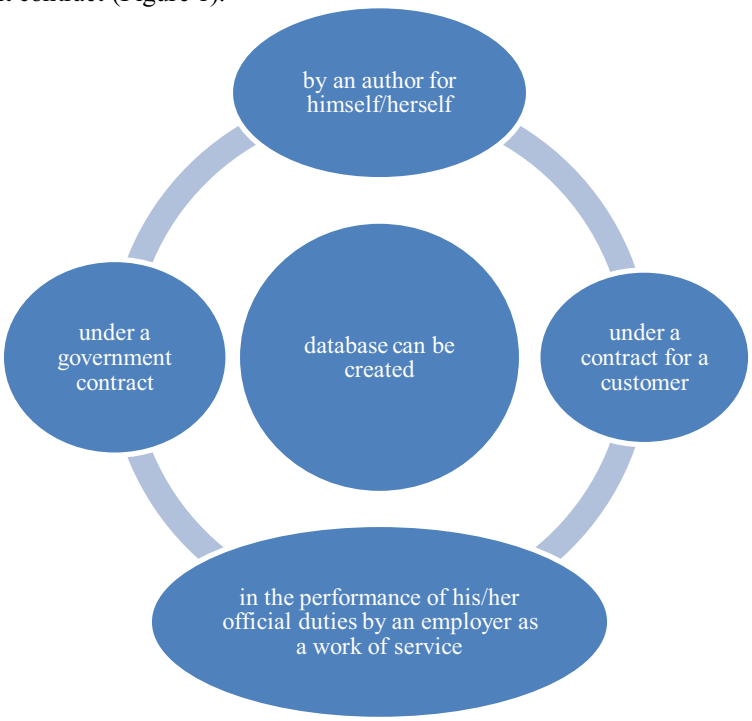

Fig. 1. Database to create.

In each of these cases, the author of the database will own not only the copyright on the selection or arrangement of the material he has made, which is irrelevant to the PD, but also the exclusive right of the database maker. Its peculiarity lies in the fact that the producer of the database, which requires substantial costs, can extract the materials and use them in any way he wishes. According to point 2 of Article 1334 of the Civil Code, this right is recognized irrespective of the exclusive right to the database, so it would seem possible to speak of a possible leakage of PD from the database, but to prevent this situation, the institution of consent to the processing of PD, which must contain a list of all persons who can get access to data; condition of withdrawal of consent to processing at the initiative of the subject (for example, when the consent was given based on false information or when personal data began to be processed in violation of the law), as well as the possibility of terminating the misuse of the data on the subject's application [4].

Let's talk about the legal regime of databases containing personal data. Considering this issue from the perspective of intellectual property law, there are no differences in the scope of intellectual rights in the database itself, as in any case the author will have the copyright

on the object in question and the right holder will have an exclusive right. However, if we compare the scope of rights to the objects included in the database, we see some differences. For example, the use of PD included in a database must be strictly limited to the purposes of processing, consent and the rules of the Law "On Personal Data", and this scope cannot be extended due to the imperative nature of the rules. At the same time, if other objects, such as works of literature, are included in the database, the protection regime acquires a different character as it is based on the dispositive norms of the Civil Code of the Russian Federation.

The database compiler is obviously bound by the need to obtain consent to use the work, but such consent may confer more rights on the compiler than consent to process PD. For example, a license agreement may be concluded between the database compiler and the author of the work to transfer the exclusive right, which significantly "free the hands" of the database owner with respect to use the work. Let's consider the main provisions on PD protection. Judicial practice in the European and Russian legal systems has developed its own approaches to the protection of personal data. Some court positions will be discussed below. Article 7 of the Law "On Personal Data" prohibits the transfer of PD to third parties without the consent of the subject. However, in practice there are cases of violations of this norm, for example when databases become the subject of purchase and sale between interested parties. There is an extensive practice of prosecution under Article 13.11 of the CAO RF for such violations, with administrative fines running into millions of rubles.

However, some experts believe that fines for legal entities in the amount of $1 to 16 million are not significant (by comparison, the European legislator in the GDPR calculates fines for identical violations in the tens of millions of dollars). It seems that this position is the most correct, because the importance of the institute of personal data in the digital world can hardly be overestimated and the lack of preventive effect of the rule may lead to adverse consequences, for example to elementary advertising calls of a personalized nature. The Law "On Personal Data" provides for the transfer of databases containing PD only if these data have undergone depersonalization procedures [5].

The transfer takes place by means of a licensing agreement, and either all or part of the database may be transferred. However, this is only possible for statistical or research purposes, so the following problems may arise when transferring an impersonal database. Firstly, both parties to the licensing agreement must not only have a research purpose, but must also be able to prove this purpose, as the burden of proof will be on them in the event of a dispute. Secondly, in the absence of this purpose, consent to the processing of anonymized data from the data subject must be obtained. Next, consider the issue of protection from the perspective of the subject whose rights have been infringed.

If the unlawful processing of personal data caused material damage to the data subject, e.g. a loan was fraudulently issued to the data subject or the data was used to make personalized advertising call and the subject was deceived about an expensive product, then the subject is entitled to recover damages under Article 15 of the Civil Code of the Russian Federation based on the concept of pure economic loss. If the subject has suffered moral damage (in the above examples this may well happen), in this case the subject may claim compensation for moral damage under Article 151 of the Civil Code of the RF [6].

However, there is also a way to protect against further misuse of data. For example, under Article 21(3) of the Law "On Personal Data", the operator is obliged to stop the unlawful processing of personal data and to ensure the destruction of personal data if a breach is detected. This obligation is prescribed by law, but can also be imposed on the operator by a court decision, e.g. by requiring the destruction of the database or the deletion of a particular person from the PD database.

The basis for such a decision may be, for example, the unlawful obtaining of personal data by threat, deception or misrepresentation. The enforceability of this requirement is worth touching upon. On the one hand, the court may apply an astreinte based on Article 174 par.

4 of the APC RF or Article 206 par. 3 of the CPC RF to enforce the decision; the operator has to report to the respective state authorities on removal of data; law enforcement authorities on the basis of the mentioned decision of the Supreme Court of the RF have access to databases with PD and may check execution of the court decision. But on the other hand, in the era of digitalization an unscrupulous operator may remove personal data from one database and move it to another or may make a paper version of the database that would be problematic to prove. Therefore, it is very difficult to guarantee the enforcement of a court decision in this situation, so it appears that it can only be enforced in a formal way.

4 Conclusion

To summarize, the incredibly rapid technological advances are also affecting the protection of human rights, among which personal data has a significant place. The impact of digital developments primarily affects the technical protection of data from cybercriminals, as not all operators are able to adequately protect citizens' PD, but many jurisdictions have established appropriate criteria for databases and programs related to the processing of PD. In conclusion, it should be noted that the legislator understands the need to protect PD and is therefore taking appropriate measures to ensure the proper technical level of operators in the Russian Federation.

However, some of the government's actions in the area of personal data are troubling. These include both the situation with the issuance of 'digital passes' and obtaining consent to transfer PD for a ten-year period, and the decision of the Supreme Court of the Russian Federation to ensure permanent access to databases by the security services. While it is difficult to say what this is for, the worst scenario seems to be excessive control of citizens, which would be facilitated by the digital storage of PD in databases [7].

Acknowledgement

I, Sayaana Savvichna Danilova, want to express my sincere gratitude to my scientific supervisor, Alexey Ivanovich Borisov, for his help in finding the sources of literature that became the basis for writing this scientific article.

References

1. V.V. Anischenko, Information Science **3,** 116-25 (2018)
2. L.K. Babenko, F.B. Burtyka, O.B. Makarevich, A.V. Trepacheva, Izvestia of Southern Federal University. Technical Sciences **5,** 77-88 (2018)
3. T.V. Alshanskaya, Information systems and technologies: management and security **2,** 81-6 (2019)
4. V.A. Kamayev, V.V. Natrov, Izvestia of Volgograd State Technical University **1(27),** 74-6 (2017)
5. A.M. Krishtofik, Information Protection **1,** 111-3 (2019)
6. A.I. Nikonov, Vestnik of Nizhny Novgorod State University of Engineering and Economics **1,** 48-55 (2018)
7. V.I. Pogorelov, Information and security **4,** 66-70 (2019)