UNAUTHORIZED ACCESS TO THE REGISTER OF DATA ON THE POPULATION OF THE COUNTRY AS A THREAT TO INFORMATION SECURITY

Anna Zueva, Financial University under the Government of the Russian Federation
Mariya Troyanskaya, Orenburg State University
Andrey Brodunov, Moscow Witte University
Ainura Zhakhmetova LN, Gumilyov Eurasian National University
Iurii Rychagov, Lomonosov Moscow State University
Darya Musatova, Lomonosov Moscow State University
Angela Mottaeva, Moscow State University of Civil Engineering
Svetlana Anzorova, Synergy University
Madina Kharesova, al-Farabi Kazakh National University

ABSTRACT

At the moment, due to the widespread development of technologies and informatization of the activities of state bodies, the introduction and use of unified registers of data on the population is more than ever a relevant tool that contributes to the transformation of the state into an information state of a post–industrial type. The register allows you to obtain complete and reliable information about citizens, increases the efficiency and quality of public services provided to the population and has a positive impact on the development of budget policy by providing more information for making socially significant financial government decisions. This article is devoted to topical issues related to the use of the population register by the state in the process of governing the country. The article provides an economic justification for the advantages of having a register in the structure of the state apparatus, looks into the issues related to security maintenance while storing and processing the data from the register, and for clarity provides examples of cyber-attacks on government databases. After a thorough analysis and study of problematics of this field, the authors proposed measures to minimize the possible risks associated with the leakage of data from the register, as well as measures to ensure the security of the population register and to prevent hacker attacks on the information systems of the state, in particular for the purpose of stealing personal data of citizens.

Keywords: Population Register, Database, Personal Data, Cyber–Attack, Hacking, Information Security.

INTRODUCTION

In the modern world, the collection, storage, processing and updating of information about persons living in the country is one of the important components that allows the state to fully realize the rights of citizens in the spheres of social security, health care, education, taxation, as well as contributing to the high–quality provision of state and municipal services (Andrichenko, 2012; Karpenko, 2018; Maisigova, 2021; Moldashbayeva, 2021; Morkovkin, 2019; Nazarenko, 2018; Goigova, 2021; Niyazbekova, 2021). As experts in the field of information law rightly point out, it is impossible to fully implement any sectoral and functionally defined tasks of the state, competently carry out reforms or implement important projects without fully having information about the size, composition and necessary parameters of the population (Bachilo, 2006; Karandaev, 2007; Federal Law, 2020; Ayuk, 2016).

MATERIALS AND METHODS

In the process of writing this article, the following methods were used: methods of analyzing the literature, analyzing regulatory documents, comparing the experience of different states in the observable area, specific legal and comparative legal methods.

RESULTS

Economic value of keeping population registers. In the economic sphere, population registers serve as a tool to enable the state to plan budgetary funds. Based on the data provided by the population register, the state can accurately calculate the amount of funds required to allocate for the needs of certain segments of the population (unemployment benefits, various payments to families with children), it is more competent to implement tax policy, taking into account the characteristics of the population living on that or another territory. Also, the register data makes it possible to speed up the process of making socially significant decisions in the economic sphere due to the promptness of obtaining data by the relevant departments responsible for the development of draft laws, orders and decrees on financial issues. Due to population registers, the state will be able to better implement fiscal policy. Because of the fragmentation of the databases of various departments, mistakes often occur in the process of writing off the debts of citizens in favor of the state, as a result of which funds are collected from the wrong person from whom they should have been written off («wrong person/defendant»). The problem of data duplication in state information systems occurs due to the fact that departmental information systems for registering the population in countries that do not use the register are created without proper coordination between them, on the basis of principles independently determined by each department, technologies for collecting, storing and transferring personal data information, formats and protocols of interaction, non–unified information and linguistic means. As a result of such erroneous write–offs, the process of collecting funds to the state budget is delayed, which may be one of the reasons for its deficit, which can also be eliminated by the population register.

In the United States of America, there is a special project called «E–Vital», which is a system of interdepartmental electronic interaction between various federal, regional and local authorities, as well as providing for the creation of a unified technology for collecting, processing, storing and using data about citizens of the country. The main goal of this project is the ability to provide full and transparent identification of the person, the creation of a tool that allows you to solve the problems of accounting and identification of citizens living in the country, at all levels of government. As official reports regarding the implementation of this project show, thanks to the detection of various cases of fraud and the elimination of cases of erroneous social payments, the US budget manages to save tens and even hundreds of millions of dollars (Karandaev, 2007: Federal Law, 2020; Ayuk, 2016; Andress, n.d.; Bunevich, 2017). According to experts from the UN Statistical Bureau, population registration systems operate in more than 60 countries, that is, in every third country in the world (Federal Law, 2020; Ayuk, 2016; Andress, n.d.; Bunevich, 2017; Ivanova, 2020; Gavrilova, 2019; Gavrilova, 2021; Karpenko, 2018). Despite this, in many countries, including large ones, there is no register. For clarity, you can look at Table 1, which presents a random sample of countries that have a population register in the structure of their government agencies' instruments and countries that do not have a population register.

Table 1
PRESENCE OF A NATIONAL POPULATION REGISTER

Presence of a national population register

Country	Yes	No
Austria	x	
Bulgaria	x	
Croatia	x	
Cyprus	x	
Czech Republic	x	
Denmark	x	
Estonia	x	
Finland	x	
Germany	x	
Greece	x	
Hungary	x	
Italy	x	
Latvia	x	
Lithuania	x	
Luxembourg	x	
Netherlands	x	
Poland	x	
Portugal	x	
Slovenia	x	
Spain	x	
Sweden	x	
Mexico*	x	
Namibia*	x	
Israel	x	
France		x
Ireland*		x
Malta		x
United Kingdom*		x
Canada**		x
New Zealand*		x
Georgia		x

In Russia, the Federal Law «On the Unified Federal Information Register Containing Information on the Population of the Russian Federation» was adopted only in July 2020. At the same time, the law provides for a transitional period of five years, as a result of which the functioning of the register should be fully implemented only from January 2026 (Federal Law, 2020). At the same time, even before the adoption of the law, public opinion was divided: some supported the idea of introducing a register, others opposed the adoption of this law, expressing various concerns, especially regarding the protection of personal data. What kind of danger can the register carry? Let's consider possible problems further.

Potential Information Security Risks when using registers

Undoubtedly, the first fear associated with the functioning in the state of a unified database containing a large amount of information about a person's personal data and his various identifiers is the threat of their leakage. We are talking not only about possible hacker attacks and criminal data theft, which will be discussed in more detail below, but also about the possible unauthorized familiarization, use and transfer of information by employees of government agencies who have access to the register. This fear, for example, was repeatedly expressed by the deputies of the legislative assembly of the Russian Federation during the discussion of the law «On a single federal information register containing information about the population of the Russian Federation». Thus, the risk of corruption is added to the risk of personal data leakage. Another problematic point is the issue of citizens' confidence in the government, in whose hands the entire array of personal information about people living in the country will be concentrated. Often among the population, fears of chipping of the population are expressed, sometimes an analogy is drawn with the regime of concentration camps, the provisions of the International Military Tribunal of the Nuremberg Trials of 1945–1946 are cited, which stated that the assignment of a person to life depersonalized numbers (in the case of the register – a unique identifying personality number – ID) testifies to the belittling of the dignity of the individual, which is prohibited by the legislation of almost all countries (Troyanskaya, 2021; Patashkova, 2021; Vodopyanova, 2017; Baigireyeva, 2020; Baidalinova, 2020; Igaliyeva, 2020; Reutov, 2021; Niyazbekova, 2020).

Also, from the point of view of information security, it is considered dangerous and not entirely correct to store all data in one place. It seems obvious that the creation of a unified database of information about citizens cannot but arouse the increased interest of cybercriminals, because any record of this register contains more information than information about citizens in separate departmental databases. This significantly reduces the cost and complexity of unauthorized access to citizens' data. Moreover, today all over the world there is no technical possibility of 100 % security guarantee of any information system. Thus, the state knowingly creates a system that is guaranteed to be vulnerable and susceptible to data leaks, while containing valuable personal data of citizens.

Examples of cyber-attacks on Government Databases

Despite the flourishing of information technologies and the development of data protection methods, from time to time there are cases that make us doubt the security of modern systems for processing and storing personal data, including government systems. Technological progress also carries negative consequences, including the widespread development of cybercrime. Increasingly, the information systems of databases of various government departments are becoming the object of attacks by cybercriminals. The purpose of these crimes is to gain access to unique confidential information about citizens for the purpose of its subsequent use in other criminal activities or sale.

In September 2021, the Argentine government was exposed to a hacker attack, as a result of which attackers were able to break into government databases and steal personal data of citizens (Karandaev, 2007: Federal Law, 2020; Ayuk, 2016; Andress, n.d.; Bunevich, 2017; Ivanova, 2020; Gavrilova, 2019; Gavrilova, 2021; Karpenko, 2018; Troyanskaya, 2021; Goigova, 2021; Niyazbekova, 2021; Nurpeisova, 2021; Patashkova, 2021; Vodopyanova, 2017; Baigireyeva, 2020; Baidalinova, 2020; Igaliyeva, 2020; Reutov, 2021; Niyazbekova, 2020). Identity cards (DNI – Documento Nacional de Identidad) of more than 46 million people, including information about name, citizenship, identity photo, signature, date and place of birth, home address and even a citizen's thumbprint were not only posted on the Internet, but were also put up for sale by cybercriminals. Interestingly, it was only in October that the data breach was discovered, thanks to the fact that a Twitter user under the nickname AnibalLeaks published photographs of ID cards of 44 Argentinean celebrities, including the personal data of the world famous football player Lionel Messi, several famous Argentine journalists and public figures, and even the data of the country's president – Alberto Fernandez. A few days later, the same Twitter user posted an announcement offering to provide personal information about anyone in the country. Personal data was stolen from Argentina's National Registry of Persons – RENAPER (Registro Nacional de las Personas). The operator of this register and the department responsible for the safety of the data contained in it in Argentina is the country's Ministry of the Interior. The reaction from the Ministry followed only a few days after all these publications. In a press release, the Argentine Ministry of Internal Affairs confirmed the data leak, but noted that they had not noticed any irregularities in the operation of the RENAPER system, the structure was working properly and there were no traces of hacking (Karandaev, 2007: Federal Law, 2020; Ayuk, 2016; Andress, n.d.; Bunevich, 2017; Ivanova, 2020; Gavrilova, 2019; Gavrilova, 2021; Karpenko, 2018; Troyanskaya, 2021; Goigova, 2021;

Niyazbekova, 2021; Nurpeisova, 2021; Patashkova, 2021; Vodopyanova, 2017; Baigireyeva, 2020; Baidalinova, 2020; Igaliyeva, 2020; Reutov, 2021; Niyazbekova, 2020).

In June 2015, the US Administration publicly announced a hacker attack on the data storage systems of the US Office of Personnel Management (OPM), which is operated by the data center of the Department of the Interior (Karandaev, 2007: Federal Law, 2020; Ayuk, 2016; Andress, n.d.; Bunevich, 2017; Ivanova, 2020; Gavrilova, 2019; Gavrilova, 2021; Karpenko, 2018; Troyanskaya, 2021; Goigova, 2021; Niyazbekova, 2021; Nurpeisova, 2021; Patashkova, 2021; Vodopyanova, 2017; Baigireyeva, 2020; Baidalinova, 2020; Igaliyeva, 2020; Reutov, 2021; Niyazbekova, 2020). As a result of criminal actions, personal data of more than 4 million current and former civil servants were stolen. After this incident, US Secretary of Homeland Security, Jay Johnson, announced the need to create a nationwide warning system about hacking of computer networks and toughen criminal penalties for committing crimes in cyberspace. The fact that such data leaks still occur, and the structures responsible for the safety of data cannot even detect the theft of data themselves, once again convinces us that by creating a population register to improve the life of the state and citizens, the risk of information security in relation to personal citizen data remains inevitable.

DISCUSSION

The population register is a database containing such information about citizens of a certain state as full name, age, sex, place of residence, citizenship and many other personal data. These lists of information are quite extensive. They include, for example, information about identity documents, including details of the start and end date of their validity, cancellation and issuance of documents with violations; information about the status of a person (citizen, refugee, migrant, etc.) and information about his relatives; information on military registration; about education and academic degrees; on registration with the tax authorities (including TIN, data on registration as an individual entrepreneur, the type of activity of the enterprise, etc.); about the details of insurance and civil records of the citizen. Of course, by gaining access to such a database, fraudsters get a fairly wide room for maneuver in terms of committing crimes. In view of this circumstance, it is quite reasonable to believe that the population register will be subject to a huge number of cyber-attacks. Thus, it is imperative to ensure that the population register is enhanced against encroachment. Let's consider some types of database protection, which, in our opinion, are the most effective and have a very high potential for preventing unauthorized access to population registers.

First of all, it is restricting access to population registers by a circle of persons. It is important to note that such a restriction should be based on obtaining a special qualification, which implies passing the procedure for admission to work with registers established by law and checking the employee's personal file. It is also important to follow the procedure for accessing the register, which provides that employees have a personal login and password. The authenticity of the user must be confirmed by his identification or recognition of the user by his identifier – login and password. Authentication, confirmation of the validity of an identifier is implemented, for example, by a secret expression. Next, user authorization is required. According to the differentiation of access rights, the user is provided only with the data to which he has the right. Passwords, with their main advantage – simplicity and familiarity – when used correctly, can provide a level of security acceptable to many companies. The reliability of password protection is based on the following requirements: the password must be a combination of letters, numbers or special characters; the password must be at least six characters long; passwords should be changed frequently and kept confidential, and passwords should be subject to a strict retention policy. It is also possible to reduce the risk of unauthorized access by using two–factor authentication.

Secondly, we admit the possibility of using data encryption. This ensures the storage of information in an «unreadable» form. It is possible to illegally enter the database not only by using the usual means of access in the system, but also by connecting to a communication channel, in fact, move part of the database. The use of cryptographic means of hiding information will prevent this threat. For this purpose, data encryption is used, i.e. storage and transmission of confidential data in encrypted form. The encryption process consists in transforming the original data (plain text) into a new representation using a special algorithm that hides the content of the original information. The encrypted text with a secret encryption key is stored in the database and transmitted over the communication channel. It should be noted that in this case, despite a sufficiently high level of protection against unauthorized access, the level of performance of data storage systems decreases due to its increasing complexity.

Thirdly, of course, before implementation and start–up, the population register should be tested for vulnerability and, based on the testing results, the population registers should be improved.

Fourthly, we believe that the current legislation in some states does not fully cover the full range of crimes committed in cyberspace, as a result of which it is necessary to amend the legislation providing for certain elements of crimes, including unauthorized access to databases with such a high significance.

In case of admission of unauthorized access to the population register, we propose to create an emergency notification system about hacking of computer networks of databases of departmental structures. This system will minimize the negative consequences and eliminate the source of the problem as soon as possible, as well as initiate an investigation against the persons involved in the hacking.

CONCLUSION

Therefore, despite the positive aspects of the register, which make it possible to improve the budgetary process in the country and the quality of public services provided to the population, the register remains vulnerable in terms of the security of the data stored in it from various cyber attacks. Possible ways to overcome this problem are proposed by us in this article. In order to overcome the distrust on the part of citizens towards the register system and to protect information systems, new ways of protecting databases should be developed in the future.

REFERENCES

Andrichenko, L.V. (2012). Information registers as an effective means of collecting and monitoring population data. *Journal of Russian Law, 8*(188), 16-40.

Andress, J., & Winterfeld, S. (n.d). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.

Ayuk, J.A., Bystryakov, A.Y., & Karpenko, O.A. (2016). Financing sustainable development of small and medium enterprises in Cameroon. International Journal of Environmental and Science Education.

Baigireyeva, Z., Niyazbekova Sh., Kicha D., & Misigova, L. (2021). Analysis of the influence of ecology on human resources management in the healthcare system. *Journal of Environmental Management and Tourism, 7*(55), 1980-1996.

Baidalinova, A.S., Niyazbekova, S.U., Baigireyeva Z., & Myrkanova, A. (2021), household food security in Kazakhstan. Popkova E.G., Sergi B.S. (eds) "Smart Technologies" for Society, State and Economy. Lecture Notes in Networks and Systems. Springer, Cham.

Bachilo, I.L. (2006). An important step in the regulation of information rights of citizens. Laws of Russia: experience, analysis, practice.

Bulletin of national academy of sciences of the Republic of Kazakhstan. 2(390), 160-168.

Bunevich K.G., & Niyazbekova, Sh.U. (2017). Analysis of the socio–economic development of the city of Astana. *Economics and Management, 3*(22), 24 31.

Federal Law No. 168–FZ of June (2020). On the Unified Federal Information Register containing information about the population of the Russian Federation.

Gavrilova, E.N. (2019). Investment banking as a direction of banking activity: the essence, features and problems of development. *Economics and Management, 4*(31), 81 86.

Gavrilova E.N., & Danaeva K.L. (2021). The banking sector of Russia: the current state and development trends. *Economics and Management, 1*(36), 7 14.

Goigova, M.G., Kurmankulova R.Z., Anzorova S.P., Yessymkhanova Z.K., & Niyazbekova S.U. (2021). Digital transformation of government procurement on the level of state governance. Studies in Systems, Decision and Control. Springer, Cham.

Hacker steals government id database for Argentina's entire population (2021). Retrieved from https://therecord.media/hacker–steals–government–id–database–for–argentinas–entire–population, last accessed 2021/11/15.

Ivanova, O.S., & Niyazbekova, Sh. (2020). Development of fintech and big data in the financial sphere: features, problems, opportunities. *Economics and Management, 1*(32), 30 36.

Igaliyeva, L., Niyazbekova, S., Serikova, M., Kenzhegaliyeva, Z., Mussirov, G., Zueva, A., Tyurina, Y.G., & Maisigova, L.A. (2020). Towards environmental security via energy efficiency: A case study. *Entrepreneurship and Sustainability, 7*(4), 3488-3499.

Karandaev G.N., & Gryzlov A.A. (2007). Economic justification creation of a system of personal accounting of the population of the Russian Federation.

Karpenko, O.A., Blokhina, T.K., Savenkova, E.V., & Rybakova, O.V. (2018). Case study of financing of innovative projects and exogenous shocks Management and Production Engineering Review.

Maisigova L.A., Niyazbekova Sh., Isayeva B.K., & Dzholdosheva T.Y. (2021) Features of relations between government authorities, business, and civil society in the digital economy. Studies in Systems, Decision and Control, vol 314. Springer, Cham.

Moldashbayeva L., Niyazbekova Sh., S. Kerimkhulle, N. Dzholdoshev, T. Dzholdosheva and M. Serikova. "Green" bonds – a tool for financing "green" projects in countries. E3S Web Conf., 244 (2021) 10060 DOI: https://doi.org/10.1051/e3sconf/202124410060

Morkovkin, D.E, Stroev, P.V., & Shaposhnikov, A.I. (2019). Financial support of regions as a tool to equalize budgetary security of the constituent entities of the Russian Federation. *Finance: Theory and Practice, 23*(4), 57-68.

Nazarenko, O.V., & Niyazbekova, Sh.U. (2021). Current state and prospects for the development of the oil and gas sector of the Republic of Kazakhstan. *Economics and Management, 4*(27), 7 14.

Niyazbekova, Sh., Grekov, I.E., Blokhina, T.K., Mussirov, G., Aetdinova, R., Suleimenova, B.B., Bunevich, K.G., & Burkaltseva, D.D. (2020). Macroeconomic analysis of the securities market of the Republic of Armenia. *Bulletin of national academy of sciences of the Republic OF Kazakhstan, 1*(383), 156-162.

Niyazbekova, S.U., Ivanova, O.S., Suleimenova, B., Yerzhanova, S.K., & Berstembayeva R.K. (2021). Oil and gas investment opportunities for companies in modern conditions.

Nurpeisova, A.A., Smailova, L.K., Akimova, B.Z., Borisova, E.V., & Niyazbekova, S.U. (2021). Condition and prospects of innovative development of the economy in Kazakhstan.

Patashkova, Y., Niyazbekova Sh., Kerimkhulle, S., Serikova, M., & Troyanskaya, M. (2021). Dynamics of Bitcoin trading on the Binance cryptocurrency exchange. *Economic Annals–XXI, 187*(1 2), 177 188

Reutov, V., Jallal, A., Sviridov, O., Korobeynikova, O., Blazhevich, O., Bondar, A., Niyazbekova, Sh., & Kamyshova, A. (2021). Analysis of the agro industrial complex of Crimea: food security of the region.

The order of registration of the population: domestic and foreign experience: mater. international. Seminars held with the support of the OSCE/ODIHR. Retrieved from http://www. osce.org/node/40135.

Troyanskaya, M., Niyazbekova, Sh., Serik Toygambayev, V., Rozhkov, A.Z., Elena, A., & Olga, I. (2021). Instruments for financing and investing the "green" economy in the country's environmental projects. *E3S Web of Conferences, 244*(2021), 10054.

Vodopyanova, E.V. (2017). Peculiarities of interaction of scientific and educational technologies. *Educational resources and technologies*, *1*(18), 38.