

Digitalization of State Corporations and Companies with State Participation

A.V. Savoskin*, A.V. Kurdyumov, M.A. Zadorina, O.A. Kozhevnikov, and V.A. Meshcheryagina.

Ural State University of Economics, 620137 Yekaterinburg, Russia

Abstract. The article analyzes the legal acts regulating public relations in the field of digital transformation of state corporations in order to determine the priority organizational, economic and managerial directions of their development. At the same time, the research carried out is also relevant for organizations of other organizational and legal forms.

1 Introduction

The President of the Russian Federation in the Decree of July 21, 2020 No. 474 "On the national development goals of the Russian Federation for the period up to 2030" set the task "to ensure digital transformation" by 2030. The specified national development goal of Russia replaced the previously established goal of "ensuring the accelerated introduction of digital technologies in the economy and social sphere" ... It is not difficult to see that at present the task is set more than broadly. At the same time, it is in the digitalization of economic relations that the greatest progress has been observed (which, on the whole, is quite natural, since initially the emphasis was placed on this particular area).

Certainly, the solution to the task set by the head of state will require great efforts in various spheres of life. Without setting ourselves the goal of defining and disclosing all the areas of digital transformation in Russia, we would like to draw attention to the prospects for digitalization of state corporations and companies with state participation (hereinafter state companies) It is these subjects of civil relations that are most susceptible to the regulatory influence of the state (as its founder) and it is they that are an example of digitalization for other organizations (primarily private). In addition, it is state-owned companies that often create the necessary digitalization infrastructure. For example, a pilot project of Sberbank of the Russian Federation, which has been collecting biometric data since 2018. Moreover, it is the state-owned companies that can use targeted government funding to introduce new electronic technologies and funds into the organization of their activities.

At the same time, state-owned companies in Russia are faced with a non-trivial question: what does digital transformation mean and how should it be expressed? The complexity of the answer to this question lies in two circumstances. Firstly, in the Russian Federation there is no comprehensive federal law that would determine the directions of digital transformation, its stages, responsible persons, sources of funding, or at least

* Corresponding author: savoskinav@yandex.ru

legalize the used conceptual apparatus. Secondly, digitalization issues today are regulated by an extremely large number of scattered acts, many of which are not at all included in the traditional Russian system of sources of law. For example, the national program "Digital Economy of the Russian Federation" contains a very large array of provisions. This document was approved by the minutes of the meeting of the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects No. 7 dated June 4, 2019. At the same time, the Council under the President of the Russian Federation for Strategic Development and National Projects itself is not a government body and the legal force of its decisions is unclear (it is confirmed by the form of the act, namely, protocol).

Thus, the primary task is to understand the legal field of digital transformation, that is, those acts that determine something in the field of digitalization (primarily for state-owned companies). In modern conditions, such a list seems to be a value by itself.

We propose to include the following acts:

1. Decree of the President of the Russian Federation of May 9, 2017 No. 203 "On the Strategy for the Development of the Information Society of the Russian Federation for 2017-2030" and the lists of instructions of the President of the Russian Federation of January 24, 2020 No. Pr-113 and adopted in its development July 3, 2020 No. Pr-1068;
2. The national program "Digital Economy of the Russian Federation", approved by the minutes of the meeting of the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects No. 7 dated June 4, 2019;
3. Passport of the federal project "Digital Technologies", approved by the minutes of the meeting of the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life and Conditions for Doing Business No. 9 dated May 28, 2019;
4. Passport of the federal project "Information Security", approved by the minutes of the meeting of the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life and Conditions for Doing Business No. 9 dated May 28, 2019;
5. Passport of the federal project "Human Resources for the Digital Economy", approved by the minutes of the meeting of the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life and Conditions for Doing Business No. 9 dated May 28, 2019;
6. Decree of the Government of the Russian Federation of April 15, 2014 No. 313 "On approval of the state program of the Russian Federation" Information Society";
7. Decree of the Government of the Russian Federation of March 2, 2019 No. 234 "On the management system for the implementation of the national program" Digital Economy of the Russian Federation";
8. Decree of the Government of the Russian Federation of July 10, 2019 No. 878 "On measures to stimulate the production of radio-electronic products in the territory of the Russian Federation when purchasing goods, works, services to meet state and municipal needs, on amending the Decree of the Government of the Russian Federation of 16 September 2016 No. 925 and invalidation of some acts of the Government of the Russian Federation";
9. Decree of the Government of the Russian Federation of November 16, 2015 No. 1236 "On the establishment of a ban on the admission of software originating from

foreign countries for the purpose of procurement to meet state and municipal needs" and others.

Analysis of these and some other acts makes it possible to highlight the following areas of digital transformation of state corporations and companies with state participation.

1. Analysis of the current state and prospects of digital transformation of a state-owned company.
2. Development of goals for the digital transformation of a state-owned company.
3. Development of a roadmap for digital transformation of a state-owned company.
4. Improving the "quality" of the staff of the state company and the formation of a culture of digital transformation.

Of course, the proposed approach is generalized and approximate, but it gives a comprehensive idea not only of what exactly needs to be done. It also answers the question in what order to make changes. Let us analyze each direction.

2 Materials and methods

The research methodology consists of both general scientific research methods: analysis, synthesis, deduction and induction, abstraction, structural and functional method, and special methods of jurisprudence: formal legal method, method of legal construction, formal logical method, systemic method, technical and legal analysis, statistical method and others. Of particular importance is the method of economic relations between the assessment of the possible liquidity of the organization with the introduction of digital transformation of the production process and personnel management. The use of the above tools will make it possible to form an optimal model of the management process - the phased implementation of digitalization in the activities of a non-profit organization (for example, a state corporation).

3 Results and discussion

Analysis of the current condition of state-owned companies and the prospects for their digital transformation involves conducting analytics on the digital transformation of the industry, assessing the digital maturity of a state-owned company, researching key challenges and opportunities for digital transformation ", as well as risks and threats to information security in the course of digital transformation.

The complexity of the analysis lies in the fact that the state corporation, on the one hand, implements the social and economic goals set for it, but on the other hand, it also acts as an economic entity - it carries out entrepreneurial activity, makes a profit, invests funds [1].

It should be noted that the analysis of the digital transformation of the industry involves the study of changes in consumer behaviour, changes in the business models of industry players and the emergence of new online platforms and digital ecosystems, changes in technological vectors of digital transformation, changes in the quality of external conditions for digital transformation (for example, funding conditions, government support measures, educational programs). The digital maturity assessment provides an analysis of the key areas of digital transformation and key elements of the basic corporate conditions for digital transformation. The digital maturity assessment also includes the current level of use of modern digital technologies and software for digital transformation.

It is highly desirable to identify the key challenges and opportunities that digital transformation creates to improve the competitiveness and development of a state-owned company. Key challenges and opportunities take into account the changes that are taking

place in the industry due to digital transformation and affect the position of the state-owned company in the market. Key challenges and opportunities for the digital transformation of a state-owned company also include the current level and growth potential of the digital maturity of a state-owned company relative to the best Russian and international practices and digital transformation solutions, both common to all industries and specific to the industry. Key challenges and opportunities should form a sufficient rationale for the selection of strategic directions for digital transformation.

Identifying the risks and threats to information security that may arise during the implementation of digital transformation when introducing modern digital technologies into the activities of state-owned companies is a necessity today. When implementing digital transformation, state-owned companies will have to determine the risks (damage) and threats to information security associated with the introduction of modern information technologies.

When implementing digital transformation, state-owned companies should assess the risks (damage) and threats to information security, the implementation of which can lead to negative consequences for the activities of state-owned companies, including disruption of the functioning and leak of protected information. When assessing risks and threats to information security, the current level of use of modern digital technologies should be taken into account.

Information security risks and threats should form a sufficient substantiating basis for the choice of legal, organizational and technical measures to ensure information security during the implementation of digital transformation.

For state-owned companies that are subjects of the critical information infrastructure of the Russian Federation, the identification of risks and threats to information security should be carried out in accordance with the legislation of the Russian Federation on the security of the critical information infrastructure of the Russian Federation.

The development of goals for digital transformation of a state-owned company may include such areas of work as: creating a target business model, a system of goals and key performance indicators for digital transformation, determining strategic directions for the development of digital transformation and planning horizons for a digital transformation strategy.

If we rely on the achievements of economic theory and existing legal regulation, the target business model should include a description of the target business model of the state company in the context of digital transformation (or several business models if more than one model is planned to be used). When choosing a target business model, the current state and prospects of digital transformation of the industry, the level of digital readiness (maturity) of a state-owned company, key opportunities and challenges for the digital transformation of a state-owned company are taken into account.

The goals of digital transformation should be focused on increasing the competitiveness of a state-owned company, meet the criterion of economic efficiency and include an assessment of the contribution of digital transformation to the growth of profits or another similar indicator of a state-owned company, as well as an assessment of the necessary investments in digital transformation and an assessment of their payback, and should also be directed (according to the sphere of activities of a state company) to achieve "digital maturity" of key sectors of the economy and social sphere, including healthcare and education, as well as public administration in accordance with the Decree of the President of the Russian Federation of July 21, 2020 No. 474.

It is advisable for each state-owned company to decompose the system of key performance indicators of digital transformation, including three levels in it: the contribution of digital transformation to the strategic goals of the state-owned company (including increasing profits or a similar indicator, increasing revenue or a similar indicator,

reducing costs or a similar indicator; digital transformation of key areas of the state company - interaction with consumers, development and operation of products (for applicable industries), operations and supply chains supporting functions (human resources management, financial management, procurement management, management of buildings and offices, etc.); ensuring the basic corporate conditions for digital transformation - digital infrastructure and data management system, human resources, competencies and culture for digital transformation, digital transformation management model.

Target values for key performance indicators of digital transformation should be calculated based on the current performance of the state-owned company, its strategic goals, industry and cross-industry comparisons ("benchmarks").

State-owned companies should choose the strategic directions of digital transformation based on an integral assessment according to the criteria of the potential contribution of the direction to the achievement of the strategic goals of the state-owned company and the level of readiness of the state-owned company for the digital transformation of the direction. It is recommended to include, but not limited to, a new business model (several business models) and / or the development of additional sources of income, new digital products and services, customer relationship management, design and engineering, service maintenance, efficiency operations, supply chain management, human resources management, financial management, procurement management. To protect information which is subject to protection in accordance with the legislation of the Russian Federation, it is necessary to use the means of cryptographic protection of information certified by the FSB of Russia (for more details see the Decree of the Government of the Russian Federation of June 30, 2020 No. 963 "On the implementation of a pilot project on the use of Russian cryptographic algorithms and encryption tools in state information systems").

When planning a digital transformation strategy, it is recommended to distinguish three planning horizons: short-term - about 12 months: target values for key performance indicators are set with a detailed time frame for a year, key performance indicators for import substitution are set on a quarterly basis; medium-term horizon - 3-5 years; target values for key performance indicators are also determined with a breakdown by time for each year; the long-term horizon is 10 years.

Each next horizon must develop and expand the key results and priority areas of digital transformation of the previous horizon.

The development of a roadmap for the digital transformation of a state-owned company may include the following areas: development and implementation of initiatives to introduce digital solutions; development and implementation of initiatives to develop digital infrastructure; development of digital solutions providers; organizational measures in the framework of digital transformation"; measures for programmed import substitution; as well as measures to ensure information security within the framework of digital transformation.

When planning the implementation of digital solutions, a complete list of initiatives in the areas of digital transformation should be indicated, including the introduction of new business models and the development of additional sources of income, interaction with consumers, operations and supply chains that support functions (personnel management, financial management, procurement management, administrative economic department, legal service), as well as by business areas and divisions of the state company.

It is advisable to describe the approaches used to select initiatives. At the same time, a typical approach includes the formation of a complete list of initiatives (based on industry practices, applicable experience of other industries, proposals from suppliers, etc.) and the selection of initiatives for implementation (for example, compliance with the digital development strategy of a state company, the greatest effect for a state company, readiness of infrastructure).

It is recommended for each initiative to give a brief description, including a description of the business problem to be solved, a description of the solution being implemented (digital technologies used), a description of 5-10 key milestones in the implementation of the initiative and determine the time frame for reaching each milestone, identify the responsible unit, other divisions of the parent company and individual subsidiaries and dependent societies.

Initiatives for the development of digital infrastructure should include a description of the requirements for the IT infrastructure, IT architecture, the state company's data management system, the information security system and tools for developing digital solutions (code storage, development support libraries, etc.). Based on the requirements for the digital infrastructure and analysis of its current state, a list of initiatives for its development is formed with a brief description of each initiative (including 5-10 key milestones in the implementation of the initiative and the timing of each milestone, the scope of work, the responsible department, operational KPIs, costs).

Initiatives for the development of digital solutions providers "should include identifying the resources that will be involved in the development and implementation of digital solutions (own resources or external suppliers), assessing the scope of work for external suppliers, establishing approaches to working with suppliers (long-term work with a limited number of suppliers and development of their competencies or selection of a supplier for each task, etc.), programs and procedures for working with start-up projects, a list of supplier development initiatives with a brief description of each initiative (including 5-10 key milestones in the implementation of the initiative and the timing of achieving each milestone, responsible unit).

“Organizational activities within the framework of digital transformation should include planned changes in the organizational structure of a state-owned company in connection with digital transformation, the creation of digital competence centers, the creation of the position of the head of digital transformation (RCT, CDO / CDTO (Chief Digital Officer / Chief Digital Transformation Officer), the formation of its division (digital transformation office) , description of functions, job responsibilities and authorities. Simultaneously, it is desirable to develop and approve a list of organizational activities within the digital transformation with a brief description of each event (including 5-10 key milestones in the implementation of the event and the timing of each milestone, responsible unit)

Import substitution measures are an obligatory part of the digitalization strategy of any state-owned company; they include a list of measures aimed at ensuring the transition of the state-owned company to the predominant use of Russian software and radio-electronic products of Russian origin. State-owned companies are also obliged to take measures to ensure information security within the framework of digital transformation, which includes activities aimed at implementing legal, organizational, technical and other measures to ensure information security. At the same time, the choice of legal, organizational, technical and other measures for ensuring information security should be aimed at preventing negative consequences for the activities of state-owned companies, including preventing disruption of the functioning of the information infrastructure of state-owned companies and leak of protected information.

At the level of local legal acts, state-owned companies are instructed to establish a list of measures aimed at the implementation of legal, organizational, technical and other measures to ensure information security in the framework of digital transformation with a brief description of each measure (including key milestones in the implementation of the measure and the timing of achieving each milestone, the responsible unit). The responsible department for the implementation of measures to ensure information security within the

framework of digital transformation is the information security department of a state-owned company.

For state-owned companies that are subjects of the critical information infrastructure of the Russian Federation, the implementation of measures to ensure information security within the framework of digital transformation is carried out in accordance with the legislation of the Russian Federation on the security of the critical information infrastructure of the Russian Federation.

Improving the "quality" of the staff of a state-owned company and the formation of a culture of digital transformation involves activities in such areas as: developing a model of digital competencies and staffing the digital transformation of a state-owned company; assessment of the need for personnel with special competence; training in digital skills and the development of digital competencies for employees of a state company; digital workforce management; planning and holding measures to develop digital culture and information security culture of a state company.

Modeling digital competencies and staffing the digital transformation of a state-owned company includes: a description of a digital competency model (or an initiative to implement a digital competency model); enumeration of specialties in demand in the digital economy, with their description in terms of the digital competence model; calculating the need for personnel based on a portfolio of digital transformation initiatives, taking into account the company's strategy for choosing suppliers of digital solutions or implementing digital solutions on its own ("sourcing model"); attracting personnel for the implementation of measures for the digital transformation of a state company (hiring, developing its own personnel, etc.).

Training in digital skills and the development of digital competencies for employees of a state company involves the development of educational programs and an assessment of the number of employees of a state company for training in competencies and technologies that are in demand in the digital economy.

Educational programs (courses) of a state company can be conducted using the state company's own resources or on the basis of third-party educational institutions. It is advisable to provide separate training programs for managers of a state company.

The list of competencies and technologies that personnel are trained in should include knowledge and skills in the field of information security. The list of knowledge and skills in the field of information security should be coordinated with the information security measures.

Special attention should be paid to the management of employees of digital specialties: peculiarities of recruiting personnel; creation of working conditions (for example, special working hours and working conditions in the office); taking into account the peculiarities of career planning (for example, expert career paths); taking into account the peculiarities of motivation (for example, strengthening the connection between the remuneration of employees of a state company and the results of digital transformation initiatives); specifics of skills development programs and other factors.

Planning and conducting measures for the development of a digital culture and information security culture of a state-owned company includes such initiatives as the introduction of customer-oriented approaches in work, practices of work in conditions of constantly changing requirements and design thinking, the introduction of a product-oriented approach in work, services feedback for employees of a state company, as well as compliance with organizational measures to protect information and the requirements of the legislation of the Russian Federation, including the use of certified information security tools.

4 Conclusions

Based on the foregoing, a conclusion should be drawn about the special legal nature of state-owned companies, which combines the features of a legal entity with state participation, but in its economic essence, represents a different form of ownership (public-private). In other words, state corporations, in fact, must act on an equal footing with other market participants and cannot have any privileges, with the exception of the privileges provided for non-profit organizations in general, on the other hand, from the standpoint of legal regulation (the presence of separate federal laws regulating their activities), they certainly become more "visual" for understanding the state concept of digital transformation implementation.

Having performed a formal legal analysis of regulations in the field of digital transformation of state-owned companies, it is possible to build a model of the management process - the phased introduction of digitalization into the activities of a non-profit organization, which, as a result, can increase its economic liquidity.

This model consists of four main stages: analysis of the current state and prospects of digital transformation of a state-owned company; setting goals for digital transformation of a state-owned company; development of a roadmap for digital transformation of a state-owned company; improving the "quality" of the staff of the state company and the formation of a digital transformation culture.

The basis for the formation of an optimal digital transformation model of an organization is to conduct analytical activities to study the dynamics of supply and demand with the emergence of new online platforms and digital ecosystems, changes in the technological vectors of digital transformation, changes in the quality of external conditions for digital transformation. At the same time, an important area is the assessment of risks and threats to information security, which will form an optimal basis for choosing legal, organizational and technical measures to ensure information security during the implementation of digital transformation.

The choice of legal, organizational, technical and other measures for ensuring information security should be aimed at preventing negative consequences for the activities of state-owned companies, including preventing disruption of the functioning of the information infrastructure of state-owned companies and leak of protected information.

Acknowledgment

The article is prepared with the financial support of the Russian Federal Property Fund within the project No. 19-010-00886 (2018). The comprehensive economic and legal study of improving the competitiveness of the agro-industrial complex of the Russian Federation in the context of the development and integration of information-digital systems.

References

1. S.G. Kirdina, Academic Bulletin, **2**, 184 (2015)
2. K.S. Stepanov, Saratov Bulletin state socio-economic university, **1**, 36 (2016)
3. J. Kuis, Z. Kruzmetra, D. Bite, *Economic Science for Rural Development*, **15**, 88 (2008)
4. M. Yu. Malkina, TERRA ECONOMICUS, **3**, 23 (2010)
5. S. A. Tertishny, *Effect of ownership transformations in the Russian economy on formation of a national model of public corporation management*, 192 (2011)
6. D. A. Parfenova, Via scientiarum, **2**, 43 (2019)

7. M. Demidov, *Development of the legal framework for the functioning of state financial control in the Russian Federation*, 4, 98 (2017)
8. V.D. Kolychev, I.O. Belkin, R.S. Udovidchenkov, *Specificity and effectiveness of programs for the development of managerial competencies of the personnel reserve*, 11 (2019)