EGOV-CeDEM-ePart

New Prospects for the Use of Cloud Computing by Control and Supervisory Bodies in Russia

Mikhail Bundin*, Aleksei Martynov**

*4, Ashkhabadskaya st., Nizhny Novgorod, 603105 Russia, mbundin@mail.ru
**4, Ashkhabadskaya st., Nizhny Novgorod, 603105 Russia, avm@unn.ru

Abstract: There is an international tendency to intensify the processes of adaptation of new (end-to-end) information technologies in the field of public administration, including cloud computing. One of the most recent imitative is to create one and only online platform for public audits and inspections – a standard cloud solution integrated with other State information systems. Despite a certain immaturity/incompleteness of this solution it remains a key direction for further innovation of control and supervisory system in Russia.

Keywords: E-government, State Control, Cloud Technologies

Acknowledgement: The reported study was funded by RFBR according to the research project No. 20-011-00584.

1. New Russian Cloud Solution for e-Government

An important point on the way to the digital economy is the reduction of administrative barriers. Russia in the framework of Reform of Control and Supervisory Activities announced creation of a standard cloud solution for control and supervisory activities (hereinafter - SCS CSA) (Resolution of Russian Government #482, 2018). It is assumed that this "standard solution" will be an automated system for supporting inspections, containing a complete and up-to-date description of administrative procedures, templates and forms of documents, decision-making models, which will eliminate an excessive degree of discretion and directly affect the growth of the quality index. The SCS CSA is designed: to use risk-based approach; to evaluate efficiency of state and municipal control; to systemize mandatory requirements; to support information interaction between state control (supervision) bodies and others participants as well as audited persons; to carry out measures for the implementation of state and municipal control. It was launched in 2019 and in 2020, a new version (version 2.0) of SCS CSA has been introduced in a demo version on the Portal of Control and Supervisory Activities of Russia (www.knd.gov.ru).

2. Recent International Practice

The use of cloud solutions by modern governments is becoming a global trend (Gasser, 2014). The *United States* can be considered one of the few countries that have been actively promoting the use of cloud solutions. In 2019, a new version of Federal Cloud Computing Strategywas announced - "Smart Cloud"(The 2019 Federal Cloud Computing Strategy, 2019). The strategy envisions a long-term model for the safe transition of federal agencies to the use of cloud technologies in order to further reduce costs, improve security and speed of service delivery. An important role in introducing technological innovations in the public administration system at the federal level is played by the Federal Risk and Authorization Management Program (FedRAMP), the essence of which is expert risk assessment and standardization in the implementation of cloud services by federal agencies. In fact, any decision to use cloud solutions that involves the use of federal data must be verified under a special program procedure.

The *European Union* in 2020 developed new strategy for data (A European strategy for data, 2020), which containes significant provisions concerning the further implementation of cloud computing technologies in the public sector. In particular, the document noted the still low level of "use" of cloud solutions in the public sector, which could potentially lead to a decrease in the efficiency of providing public services. As a solution, the Strategy involves several steps aimed at developing an appropriate legal framework for the creation of pan-European data pools, further steps to develop partnerships between the public sector and providers of digital services. A special role in the document was assigned to the creation of a legal framework for the creation of data clouds and cloud services for the system of public procurement and law enforcement.

Since 2015, *China* has developed a number of policy and strategic documents on the implementation of cloud computing technologies in the public sector. According to them, cloud computing service platforms and data centers that provide services to the party and the government should be located in China, and confidential information should not be transmitted, processed or stored outside the state. A security or confidentiality agreement may be entered into by the departments and the service provider. However, enterprises that are related to state secrets or official secrets are prohibited from using cloud services (Murphy, 2019). One of the Chinese IT-leader Huawei is now actively promoting the "one cloud + one lake + one platform" strategy. This strategy helps speed up data integration and exchange between different government information systems (Xin, 2020, p. 13).

3. Conclusions

Based on current foreign practices' analysis it is possible to highlight some issues for further improving the legal framework for the use of cloud solutions in control and supervisory activities in Russia:

- to develop competitive environment for cloud solution providers, including import substitution, priority for Russian developers, and the criteria for admission of foreign suppliers;

- to formulate in detail and correct form the general and specific requirements for cloud solutions admission in the public sector, including through the public procurement system;
- to improve provisions on IoT & information security, privacy (Mackay, 2012, p. 679);
- to envisage provisions on training staff and personnel to work with cloud solutions.

References

A European strategy for data. (2020). EUR-Lex.europa.eu, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

Gasser, U., & O'Brien, D. (2014). Governments and Cloud Computing: Roles, Approaches, and Policy Considerations. Berkman Center Research Publication, 2014-6. DOI: 10.2139/ssrn.2410270

Mackay, M., & Baker T., & Al-Yasiri A. (2012). Security-oriented cloud computing platform for critical infrastructures. Computer Law & Security Review, 28(6), 679–686. DOI: 10.1016/j.clsr.2012.07.007

Murphy, M., & Dang F. (2019). Cloud computing in China. Lexology, 21.03.2019. https://www.lexology.com/library/detail.aspx?g=998fe1a0-6634-41e7-a670-19ca406709e5

Resolution of the Government of the Russian Federation of 21.04.2018 # 482 "On the State Information System" Standard cloud solution for automation of control (supervisory) activities", http://publication.pravo.gov.ru/Document/View/0001201804250009.

The 2019 Federal Cloud Computing Strategy. (2019). the Whitehouse, https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf

Xin, W. (2020). e-Government: Contributing to a Digital China. ICT Insight, 25, 12-13.

About the Authors

Mikhail Bundin

Mikhail Bundin works as Assistant Professor for the of administrative and financial law chair at Lobachevsky State University of Nizhny Novgorod. In 2018 he obtained his PhD degree in law of informatics at the Institute of Legislation and Comparative Law under the Government of the Russian Federation. He speaks Russian, English, French.

Aleksei Martynov

Aleksei Martynov works as head for the of administrative and financial law chair at Lobachevsky State University of Nizhny Novgorod. He is full professor and one of the leading experts in the field of administrative law and procedure, regulation of state control and supervision in Russia, since 2016 - Head of PhD Council in administrative law & procedure. He speaks Russian, English.