ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 113

Factors of Regional Extensive Development (FRED 2019)

Trust and Security in the Digital Economy

Kulova M.R.

Laboratory of Applied Sociology and
Conflict Studies, Vladikavkaz Scientific Center
kulova-m@inbox.ru

***Abstract* – The article discusses features of interaction of trust and security in the digital economy in the context of their impact on the changes in the digital environment. The development of the digital economy as an absolute economic imperative actualizes the issue due to its theoretical and practical relevance. The purpose is to study trust and security in the digital economy in their interconnection and develop proposals for the improvement of trust and security in the digital environment. It was found that the relationship and interdependence of trust and security is nonlinear due to the ambiguity of the concept "trust". An analysis of the results of the global study of the Digital Society Index 2019: Human Needs in a Digital World and statistical data on the digital economy of Russia showed an imbalance in the "trust-security" link, when a low level of trust in digital products is combined with a fairly developed system of information security. Relevant proposals have been formulated to balance trust and security in the digital economy. It is necessary to balance a model of digital development with a focus on ensuring confidence in the digital environment and maintain the active state policy in the field of information security. Limitations of this model for the development of the digital economy are ineffective institutions. Expanding the tools of control by civil society and involvement of people in the discussion of digital innovation, the implementation of programs aimed at teaching citizens information security when using digital products will contribute to the development of the digital economy.**

Key words – trust, security, digital economy, non-digital factors.

I. INTRODUCTION

The active use of digital technologies and services is no longer an innovation. It is reality for the entire civilized world. The development of the digital economy is becoming one of the global trends in economic processes. The formation and expansion of a digital space has explicit and implicit features and patterns. Non-digital factors of the digital economy, trust and security, and their dynamics determine the development paths of the digital economy.

The interconnection and interdependence of the categories *trust* and *security* forms the basic matrix of changes in the digital economy which actualizes the study of the characteristics of these categories and their impact on each other.

The Digital Society Index 2019 global study: Human Needsina Digital World records a decline in trust, or a lack of trust in digital technology. According to the researchers [1, p. 13], Russia is distinguished by a rather high level of citizens' access to digital technologies, and a low level of trust with the state-developed information security system.

The purpose is to study the categories *trust* and *security* in the digital economy in their interconnection and develop proposals for the growth of trust and security in the digital environment.

II. MATERIALS AND METHODS

To solve the tasks, we used general research methods: the comparative and statistical analysis, the secondary analysis of the results of the Digital Society Index 2019: Human Needs in a Digital World study in 24 countries involving 43,000 respondents.

III. RESULTS

It was found that the relationship and interdependence of the categories *trust* and *security* in the digital economy is non-linear due to the ambiguity of the content of the concept “trust.” An analysis of the results of the global study Digital Society Index 2019 and statistics on the digital economy of Russia showed an imbalance in the “trust-security” link, when a low level of trust in digital products is combined with a fairly developed information security system. Relevant proposals have been formulated to bring trust and security to an equilibrium state.

One of the basic determinants in society which determines the progress in the socio-economic development of the country and possibilities of self-realization of people is trust [2, p. 10]. Trust in the digital environment is becoming one of the main factors of the competitive ability of the digital economy.

The content of the concept “trust” in the digital economy is undergoing some changes in the context of the narrative of the digital economy. Despite the ambiguity, the term “digital economy” has two definitions. The first approach has a narrower interpretation, and the second one – a broader one. In the first case, it is a digital economy based on digital technologies, primarily electronic goods and services. The second approach suggests that the digital economy is an economic production using digital technology [3].

It is necessary to define the digital economy as an economic activity enshrined in the national program “Digital Economy of the Russian Federation” as production of digital data in order to build an information space in which citizens and society receive high-quality and reliable information, etc. [4].

T.V. Ershova identified digital and non-digital factors of the digital economy. According to the expert, digital factors cover the digital sector of the economy, digital infrastructure,

shared digital platforms and services, digitalization of the public sector and digital consumers represented by citizens. Non-digital factors include trust and security, state policies and strategic planning, relevant legislation and effective institutions, innovations in the field of digital economy and human capital [5].

Trust in the digital environment can be considered as a derivative of trust as a socio-philosophical category. According to A.A. Neofitova, a lack of trust is inherent in trust as an act of faith [6]. Trust is the expectation of reliability and predictability of the actions [6].

S.E. Gubanova explores the category “trust” as a basis for the harmonization of relations [7]. According to N.V. Pogukaeva, there are two main approaches to the concept "trust." On the one hand, trust is a product of a traditional society based on faith; on the other hand, trust is a product of rational thinking [8]. The combination of irrational and rational methods of interaction occurs through a culture of trust [9].

The famous sociologist P. Shtompka considered three dimensions of the category “trust”: trust as an attribute of culture, as a personality trait and as a characteristic of relationships. He described social conditions of the development of a culture of trust: structural opportunities that support the phenomenon of trust, and the desire and willingness to use them in order to increase the level of culture of trust. Shtompka formulated five binary oppositions, circumstances that give rise to a culture of trust and a culture of distrust: a stable social order – radical changes; norm-chaos consistency; transparency of the social system-secrecy; clarity; accountability of people and institutions – their irresponsibility. In addition, the culture of trust is influenced by the level of personal and social capital, as well as personal characteristics of people, such as optimism-pessimism, orientation to traditional values, orientation to modernist values, etc. [10].

In assessing the state of digital and non-digital factors, T.V. Ershova proceeds from the general notion of a satisfactory level of development of digital and non-digital factors. At the same time, the author assesses the practice of using digital technologies and electronic commerce as good, and trust, security, human capital and regulation as corresponding to a good level [11].

The research *Digital Society Index 2019: Human Needsina Digital World* identified a low trust level in the whole world and in Russia.

The key criteria of the Digital Society Index are dynamism, access to digital technologies and services (inclusion), and trust. In the 2018 global ranking of the world's digital economies, Russia ranked 10th out of 10. In 2019, Russia ranked 23rd out of 24 [1] between Japan and Brazil with a relatively good level of access to the digital environment (14th place), low development of the digital economy (22nd place) and a low level of trust (24th place). It should be noted that the low value of the trust criterion is correlated with the global trend – only 45 % of people put trust in business protecting their personal data.

Despite the fact that in Russia, the dynamism of the digital environment was not highly rated, positive trends in the development of digital infrastructure are observed in individual Russian regions. For example, in the North Caucasus Federal District, the number of fixed broadband Internet access subscribers per 100 people increased from 6 people in 2015 to 9 in 2018. The average Russian indicators were 18 and 22 people, respectively. The relevant indicators of the mobile Internet access amounted to 68 people in 2015, and 86 – in 2018. In 2018, as compared to 2015, the proportion of households with broadband Internet access increased from 71 to 73 %. In the North Caucasus Federal District, it increased from 62 to 65.4 % [12].

The authors of the study connect the problem of trust in the digital environment, the dynamism of the digital economy and access to its benefits with the way the digital economy satisfies human needs by analogy with the Maslow’s pyramid (Table 1).

TABLE I. SATISFACTION OF THE NEEDS OF THE DIGITAL ECONOMY

Ranking	Country	Basic needs, %	Psychological needs, %	Self-fulfillment needs, %	Social needs, %
1	China	69	27	62	76
2	India	67	27	69	74
3	Hungary	64	52	40	43
22	Russia	37	58	48	48
	Average world value	49	38	45	49

As can be seen from the Table 1, more than a third of respondents in Russia and half of respondents in other countries consider that the Internet satisfies their basic needs: an access to the digital infrastructure and trust in the use of personal data.

Just over half of the Russians and just over a third of respondents in other countries admit that their psychological needs are sufficient because digital technologies contribute to better health and personal well-being.

The opinions of respondents from Russia and other countries differ in assessing the level of satisfaction of social needs and self-fulfillment needs in the digital environment — slightly less than half of the respondents. Representatives of China and India (76 and 74 %) appreciate possibilities of the digital economy in meeting social needs and solving pressing social problems. The answers to the question about the level of satisfaction of self-fulfillment needs reflect their understanding of the right digital education, skills and opportunities for working in the digital economy

Trust in the digital economy is ensured by the mechanism of information security, one of the main directions of development of the digital economy. The national information security policy is outlined in the Information Security Doctrine which defines information security as a state of security of an individual, society and state in the context of constitutional rights and freedoms, quality of life [13]. S.V. Nuyanzin offers a slightly different interpretation of information security, describing it as a state of security both at the state level and at the level of the individual in the

information environment with the required amount of information, social usefulness and a right to access [14].

The content of the concept “security in the digital economy” is revealed in network security and data security management in order to ensure their availability, integrity and security, including trust in cloud services and authenticity of online transactions. The author proposes a solution to the problem of a lack of trust in digital technologies and services by providing greater protection of personal data and consumer rights, more efficient use of electronic documents and the use of safe and reliable applications [5].

According to A.A. Alpeev, it is necessary to distinguish between the concepts of information security and cybersecurity; instead of the concept "information security", it is necessary to use the concept of information security. The author defines cybersecurity as a security section that studies cyber objects, that is, objects with the participation of programmable tools, in order to formulate an effective policy for their protection [15].

One of the most authoritative studies of cybersecurity in the world is the ranking of the International Telecommunication Union – the UN Global Cybersecurity Index. The ranking methodology provides for the assessment of five main criteria: the legislative framework in the field of cybersecurity, the technological base, the organizational basis, international cooperation and potential in the form of capacity growth, training for the development of the sphere.

In 2017, Russia ranked 10th in the cybersecurity ranking with 0.788 points, in 2018 – 26th with 0.836 points. Despite the deterioration of positions in the 2018 ranking, the cybersecurity index increased from 0.788 points in 2017 to 0.836 points. The improvement was due to the fact that the drafters of the ranking noted the adoption of measures to combat fraud in the use of electronic payment systems.

Figure 1 shows Russia's position in the ICT development ranking — 45th place, e-government development ranking — 32nd and cybersecurity ranking — 26th [16].

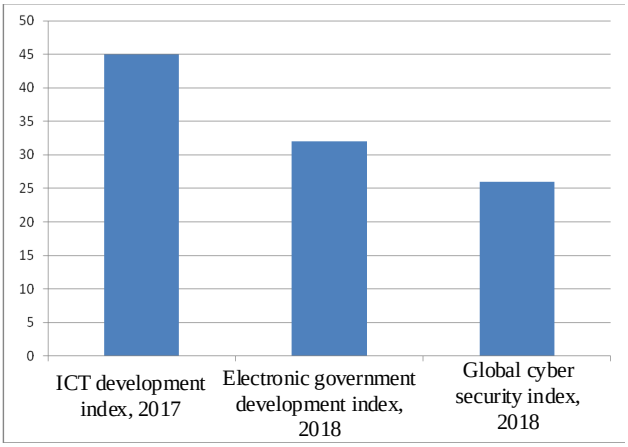

Fig. 1. Russia's place in international digital economy development rankings

The correlation and scoring of individual criteria of the global cybersecurity index for countries that ranked 1st (Great Britain), 2nd (the United States), 3rd (France) and 26th (Russia 2) are shown in Figure 2.

The legislative aspects of cybersecurity and its regulation in Russia are at the same high level of development as in the leading countries. Regarding the technical and organizational aspects, national skills in building a cybersecurity system and international relations, the lag behind the leading countries makes it necessary to implement systemic measures in these areas of cybersecurity in order to improve the overall position of Russia in the ranking.

The statistical data show that to protect information, organizations use updated antivirus programs – 87.8 % of companies, electronic digital signature means – 83.7 %, technical means of user authentication – 64 %, means of detecting intrusions into computers – 45 % and less. In total, 5.7 % are in demand, in particular, biometric means of user authentication. The population mainly uses anti-virus information protection tools [16, p. 203].

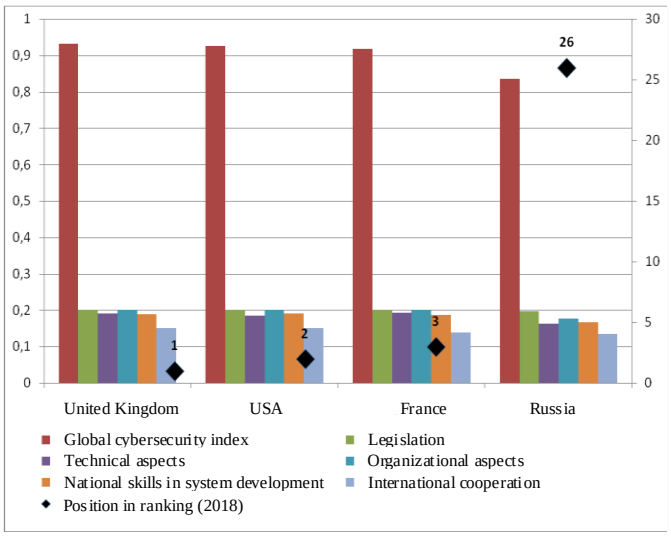

Fig. 2. Global Cybersecurity Index

Nevertheless, one of the main problems of information security in the digital environment is a low level of information security culture. The lack of understanding of serious risks of loss of economic information and the involvement of company employees in data leakage indicates the absence of a relevant culture of economic information [17].

According to the results of the Digital Society Index 2019 study, it is clear that the lack of trust in digital products and the risks of information security affect the change in the behavior of Internet users. Respondents (44 %) reduce the amount of data posted on the Internet, use ad blocking programs (27 % of respondents), reduce the time spent on the Internet (21 % of respondents), delete accounts in social networks (14 % of respondents). The main reason for the distrust is the leakage of personal data. [1]. Russian respondents show a lower level of trust in companies and government bodies regarding confidentiality of their personal

data. If in the world, about 45 % of respondents believe in the protection of their personal data, in Russia, only 30 % believe in it.

Thus, at a high level of access to digital services and technologies, there is a relatively low level of trust in the use of personal data by businesses and the government. It is paradoxical when there is an effective cyber security system and no trust. An analysis of the factors affecting the content of the concept "trust" shows that a lack of trust in digital technologies is caused by ineffective institutions.

IV. Conclusion

Trust and security are interrelated categories, but their relationship is non-linear due to the multidimensional nature of trust as an attribute of culture, personality traits and characteristics of relationships, rational and irrational principles. A relatively low level of trust in digital products is combined with acceptable indicators of information security in Russia.

To ensure the priority development of the digital economy, a more balanced model of digital development is required. It should be focused on the methods for increasing trust in the digital environment and an active state policy in the field of information security. Limitations of the model are inefficient institutions.

The expansion of control tools by civil society and the more active involvement of people in the discussion about digital innovations, introduction of training programs for Internet users will contribute to the development of the digital economy in Russia.

References

[1] Digital Society Index 2019: Human Needs in a Digital World. Retrieved from: https://www.oxfordeconomics.com/recent-releases/digital-society-index-2019-human-needs-in-a-digital-world.

[2] F. Fukyama, Trust: Human Nature and the Reconstitution of Social Order. London: Free Press, 1996, 368 p.

[3] T.V. Ershova, Yu.E. Khokhlov, S.B. Shaposhnik, "Methodology for assessing the level of development of the digital economy as a tool for managing digital transformation processes", Eleventh international conference "Management of the development of large-scale systems". Retrieved from: https://iotas.ru/files/documents/wg/хохлов.pdf.

[4] National program "Digital Economy of the Russian Federation". Retrieved from: https://sudact.ru/law/rasporiazhenie-pravitelstva-rf-ot-28072017-n-1632-r/programma-tsifrovaia-ekonomika-rossiiskoi-federatsii/

[5] T.V. Ershova, Trust and security in the digital economy. Retrieved from: https://digital.msu.ru/wp-content/uploads/2018-03-06-Доверие-и-безопасность_Ершова-v.2.pdf

[6] A.A. Neofitova, "Trust as a category of sociological analysis", Bulletin of the Russian State Humanitarian University. Philosophy. Sociology. Art History, vol. 4, no. 6, pp. 69–74, 2016.

[7] S.E. Gubanova, "Trust as the basis for harmonizing the interaction of business structures in the digital economy", Bulletin of the Volga University named after V.N. Tatishchev, no. 1, pp. 134–141, 2018.

[8] N.V. Pogukaeva, "Trust in the context of the information society", Bulletin of the Siberian Science, vol. 1, no. 16, pp. 40–43, 2015.

[9] I.B. Ardashkin, "Confidence in science and religion: on the issue of establishing a culture of trust", Bulletin of Tomsk State University, vol. 2-13, no. 370, pp. 56–60.

[10] N.V. Freik, P. Shtompka, "Trust: Sociological Theory", Sociological Review, no. 3, pp. 30–41, 2002.

[11] T.V. Ershova, Digital economy: approaches and experience of Russia. Retrieved from: https://digital.msu.ru/wp-content/uploads/2018-03-23-Plenary_Ershova-v2pdf.

[12] M.A. Sabelnikov, G.I. Abdrakhmanov, L.M. Gokhberg, O.Yu. Dudorova et al., Information society: the main characteristics of the regions of the Russian Federation. Moscow, NRU HSE, 2018, 216 p.

[13] Information Security Doctrine of the Russian Federation, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

[14] S.V. Nuyanzin, "Information security of an individual and some organizational and legal measures to ensure it", Jurisprudence and law enforcement practice, no. 2, pp. 77–85, 2018.

[15] A.A. Alpeev, "Security terminology: cybersecurity, information security", Cybersecurity Issues, no. 5, pp. 39–41, 2014.

[16] G.I. Abdrakhmanova, K.O. Vishnevsky, L.M. Gokhberg et al., Indicators of the digital economy: statistical. Moscow: HSE, 2019, 248 p.

[17] F.A. Khochueva, T.P. Shugunov, A.Z. Zhukov, Ch.H. Ingushev, "Information Security Through the Prism of the Digital Economy," Modern High-Tech Technologies, no. 11, part 1, pp. 65–71, 2018.