The System of Regulation of the Digital Environment in the Context of Globalization

Idris Iblaev*

Kadyrov Chechen State University, Sheripova Street 32, 364024, Grozny, Russia

Abstract. At present, the issue of business security is becoming extremely relevant, since the economic well-being of the regions and the entire state in particular depends on how developed and sustainable the activities of enterprises are. The security of entrepreneurial activity, first of all, can be characterized as the state of protection of business entities from external and internal threats. Of course, work at each enterprise in the areas of effective construction of an organizational structure, accounting and management accounting systems, risk management and anti-crisis management is being carried out, but very often in isolation from the real situation in the state economy. Hence, there are many problems in the economic security of enterprises. A comprehensive analysis is necessary in order to develop measures of managerial influences for the stable functioning of an economic entity in an unstable economic system. And the more thoroughly the assessment is carried out, the more reasonable and effective the measures taken will be.

1 Introduction

The onset of digitalization and the growing influence of digital platforms ("ecosystems") is accompanied by a fundamental change in the essence of labor, labor and economic relations in society. This phenomenon is called the "sharing economy" and also "uberization", after the American company Uber, the pioneer of this business model. Briefly, its essence can be stated as follows: the digital platform offers a certain service as an information intermediary, bringing together customers and service providers, both of which are "free economic agents", and the platform simply receives a commission for "pimping". Such are now taxi services, sharing cars, bicycles, scooters, renting apartments, Internet aggregators of goods, educational services, news, etc [1]. This model is dangerous for the rights of citizens in that, acquiring tremendous power over the market and its "free" economic agents, the digital platform - an information intermediary - relieves itself of all social obligations in order to increase profits. For example, by assigning ratings to taxi drivers, taking a significant commission from them, all the time tightening working conditions, increasing commission and requirements for working conditions, the intermediary platform is not responsible for them as for employees, does not have responsibility under the Labor Code of the Russian Federation, that is, it does not pays them vacations and sick leaves, has no obligations for maternity leave and other payments [2]. The employee using the platform

*Corresponding author: i.iblaev@yandex.ru

is formally an independent agent (for example, self-employed or individual entrepreneur). At the same time, in reality, he is, in fact, an employee who receives a relatively low salary, without any social protection provided for by the Labor Code, since formally he does not have an employer. He works with an irregular working day, without vacations, time off, overtime, ballots, two paid months upon dismissal and other social guarantees for the employee [3]. If an employee of such a system falls ill, does not go to the line, he instantly loses his earnings.

Before society and the state, the information intermediary, as is generally accepted when promoting the ideology of digitalization, justifies its existence with standard arguments of innovation and convenience. Indeed, taxis began to arrive very quickly, which means that from the point of view of digitalizers, this is a business model that is certainly useful for society and does not require special regulation [4]. Meanwhile, this model creates a rather serious social threat to the labor rights of citizens and the stability of society (recall that, for example, taxi drivers in taxi aggregators in Russia employ millions of people for whom this has become a profession, but they are not employees and are not protected by the Labor Code). Code). Moreover, over the past decade, several attempts have been made in Russia to introduce "uberized" medicine, in which a digital platform would bring doctors and patients together for a fee, also without answering for anything on the merits. These attempts will continue, because the uberization of markets gives huge profits to information intermediaries. The same attempts to "uberize", replace teachers with information intermediaries and "uberized" tutors are being made in relation to the education sector [5]. The lexicon of digitalizers is quite typical and revealing: in their policy statements they openly speak and write about the "unpackaged sectors" of education and medicine, referring to future huge profits for those who "unpack" (that is, in fact, privatize these industries first). In fact, uberization levels out, cancels the last hundred years of progress in improving social relations and protecting the rights of workers both under socialism and under capitalism, returning us to the times of wild capitalism of the 18th-19th centuries. The development of uberization and information intermediaries in the format of wild capitalism creates, produces social tension [6]. A "social bomb" is being planted under our society in the form of millions of citizens affected by their rights, controlled by artificial intelligence software and discriminated against by omnipotent information intermediaries for the sake of profits. This "bomb" may work in the near future if we do not begin to regulate and control the activities of information intermediaries as quickly and decisively as possible.

2 Research Methodology

The main players in the market for big user data and its use are now not states, but private digital data operators (platforms, "ecosystems", IT services): search engines, browsers, social networks, instant messengers, video and photo hosting, advertising systems, mobile operators, app stores and online media [7]. It is they who accumulate the largest volumes of user data, have huge audiences, and also own the most powerful technologies for analyzing and using this data. Not only do government agencies fail to develop their collection and analysis tools at the same pace, but they also do not have a comparable audience, so they are often the solicitors and recipients of this data from private digital platforms [8]. At the same time, the wider the range of digital services of the platform - or "ecosystem" - the higher its ability to aggregate and jointly analyze heterogeneous data about users. Bringing together data on search queries, emails, site visits, purchases, media consumption, communication in social networks allows you to create the most complete user profile and then manipulate its product demand, media consumption, picture of the day, as well as the circle of communication and political views, use it for propaganda purposes , fraud,

blackmail and other criminal activities. Ecosystems tend to monopolize the data market. Only a few of the largest players in our digital market have or strive to have such a wide range of services: Google, Meta (Facebook), Yandex, Mail.ru, Sberbank, four federal mobile operators. And where some element of the line of services and data from it is not enough for some major player, he enters into alliances or makes acquisitions. As a result, these "ecosystems" accumulate not only huge amounts of very valuable data, but also receive the most powerful economic, ideological and geopolitical leverage on the population of Russia and almost any other country in the world.

3 Results and Discussions

The largest global digital platforms and ecosystems operating in our country – Google, Meta (Facebook), Twitter, Instagram, TikTok – already have budgets and a "net population" larger than most UN member countries [9].

These platforms, being transnational in nature, have corporate interests, a policy of promotion in foreign markets, which is largely determined by the decisions of their management and the jurisdiction of the country of origin of the company, and not by the laws of those countries where they operate. Huge incomes and technological power allow them to feel confident even in disputes with the state apparatus of most countries of the world. In fact, this is a new type of "digital states" with its own special digital sovereignty, superimposed on top of the sovereignties of traditional states of the real world [17]. This is a rather alarming trend, since such digital states are practically not subject to international law in any way and, in fact, have no restrictions other than their internal corporate goals, objectives and interests, as well as the requirements and rules of the government of the country of origin, that is, in the vast majority cases, the US government. Some national states are now developing ways to "land" digital giants in their jurisdictions, in particular, such a law on "landing" (that is, on the creation of legal entities in local jurisdiction) was also adopted in the Russian Federation in 2021 [10]. However, this is a rather weak and, moreover, purely economic mechanism (especially for countries that at best belong to the third category of local markets among digital giants), which will not be able to significantly affect the ideological and outreach work of digital foreign agents on the territory of third countries. The current practice in many countries of fining the largest violating companies (first of all, Google, Twitter, Meta (Facebook) for refusing to remove illegal content and non-transparent internal corporate censorship, so far shows rather weak effectiveness if the measures of financial impact are not supported by technological ways to slow down the work of platforms or their blocking [11].

The main risks of accelerated digitalization by digital platforms and "ecosystems", described above, are aggravated for our country by the fact that most of these "ecosystems" are not domestic, but foreign, mostly American [16]. Their widespread use, including by representatives of the public sector for work needs, creates a direct threat to the digital "colonization" of Russia in the interests of the United States. American digital platforms now have more than 50% of user accounts in social networks, about 50% of search queries, more than 90% of messenger accounts, more than 95% of video views, more than 50% of ad impressions on the Russian-language Internet (Runet) [12]. You need to understand that the developer - the one who creates the technology and / or platform - always remains its true owner, regardless of the form in which the developer sells the technology or provides it for use [15]. All so-called "information intermediaries", that is, search engines, social networks, photo and video hosting sites, independently determine which news feed and messages to show to the account owner, what to allow him to write and when to block him, that is, they are the actual owners of both the account and the content , which is produced by the user on it. The history of the 2019-2020 US election campaign, including the

blocking of the incumbent and his supporters by digital platforms and hosting services in January 2020, has clearly demonstrated the true owners of this media space [14]. In essence, the American global IT corporations, controlled by the US Democratic Party, now have a "controlling stake in Runet." The digital sphere of Russia as a whole is even more a digital colony of the West: the vast majority of operating systems and office applications on private devices of Russians and in organizations are developed in the USA; enterprise management uses predominantly Western systems; management of Russian discrete and continuous production (metallurgy, chemical production, oil production, gas pipelines, etc.), some other critical infrastructure - is carried out almost exclusively with the help of Western systems [13]. The acceleration of digitalization paradoxically leads not to a decrease in this colonial digital dependence, but to its strengthening, because under the flag of accelerating digital transformation in Russia, there is an increasing borrowing and implementation of ready-made Western technologies and platforms in government agencies, sectors of the national economy and private business. In this regard, it should be noted that 90–95% of all "artificial intelligence systems" currently being created in Russia and presented as domestic developments are based on publicly available open solutions (the so-called neural frameworks) of Google and Facebook, and not on domestic software solutions.

4 Conclusions

In the context of the rapid development of the digital environment in our country, there is still no targeted legislation (although there is already an amendment to Article 71 of the Constitution of the Russian Federation, which fixes the issues of protecting citizens' data under federal jurisdiction). There is an obvious backlog and imperfection of the legislation regulating the digital environment, including in the field of protecting the rights of citizens in the new digital environment. Today, the most acute problems include, in particular, the lack of a set of rules that ensure the voluntary use of digital technologies by citizens when interacting with the state, as well as the large-scale collection of personal data in centralized federal-level databases.

In recent years, facts of coercion to the electronic form of state and municipal services have also become widespread, to sign consent to the processing of personal data in cases where this is not required for the implementation of state or municipal functions. Serious objections in society are caused by the norms of legal acts related to uncontested digitalization in the field of public administration in general and specific areas of life in particular. This section below provides an overview of the destructive tendencies of law enforcement practice in the Russian Federation, which limits the information sovereignty of a person and threatens privacy.

References

1. D. V. Shepelev, Digitalization and law: current state and prospects for mutual influence, **16(3)**, 109–113 (2020).
2. D. V. Shepeleva, The evolution of state financial control, **12(192)**, 30 (2020).
3. D. V. Shepeleva, State audit in the Russian Federation: features of implementation, **5(4)**, 178 (2020).
4. T. Menzel, T. Teubner, Green Energy Platform Economics (2020).
5. L. Barnewold, B. G. Lottermoser, Identification of Digital Technologies and Digitalisation Trends in the Mining Industry, **30**, 747-757 (2020).

6. R. Kh. Ilyasov, Spline modeling and analysis of relationships in the economy with the possible presence of regression switching points, **11(4)**, 165-175 (2018).
7. M. Barzaeva, R. Ilyasov, Sustainable development of the global labor market in the context of the transformation of the industrial complex of the digital economy, 152-164 (2022).
8. A. V. Makarova, Actual problems of cybercrime investigation in the Russian Federation, 149-153 (2021).
9. G. V. Vorontsova, G. V. Chepurko, R. M. Ligidov, T. A. Nalchadzhi, I. M. Podkolzina, Problems and perspectives of development of the world financial system in the conditions of globalization, **57**, 862-870 (2019).
10. Y. E. Klishina, I. I. Glotova, O. N. Uglitskikh, E. P. Tomilina, I. M. Podkolzina, Peculiarities of the financial policy of non-profit organizations in the macroeconomic unstable environment. Espacios, **38(34)**, 34 (2017).
11. A. Lawler, End Game for Oil? OPEC Prepares for an Age of Dwindling Demand. Reuters (2021).
12. I. V. Taranova, I. M. Podkolzina, F. M. Uzdenova, O. S. Dubskaya, A. V. Temirkanova, Methodology for assessing bankruptcy risks and financial sustainability management in regional agricultural organizations, **206**, 239-245 (2021).
13. A. S. Salamova, O. Dzhioeva, Green transformation of the global economy in the context of sustainable development, 152-159 (2023).
14. A. S. Salamova, Global networked economy as a factor for sustainable development, 03053 (2020).
15. V. Sebestyén, E. Domokos, J. Abonyi, Focal Points for Sustainable Development Strategies: Text Mining-Based Comparative Analysis of Voluntary National Reviews. Journal of Environmental Management, **263** (2020).
16. S. G. Shmatko, L. V. Agarkova, T. G. Gurnovich, I. M. Podkolzina, Problems of increasing the quality of raw material for wine in the stavropol region, **7(2)**, 725-730 (2016).
17. I. M. Podkolzina, A. I. Belousov, F. M. Uzdenova, L. V. Romanko, O. A. Chernikova, Forms of financial fraud and ways to minimize risks, Modern Global Economic System: Evolutional Development vs. Revolutionary Leap. Institute of Scientific Communications Conference, 2197-2205 (2021).
18. I. M. Podkolzina, I. V. Taranova, K. T. Paytaeva, S. V. Revunov, T. F. Abrosimova, Innovative approaches in financial support for regional economic security, 549-558 (2021).
19. T. U. Elbuzdukaeva, A. M. Gelagaeva, A. M. Sugaipova, Migration processes in the chechen republic at the turn of xx century, 2690-2696 (2019).