Advances in Economics, Business and Management Research, volume 138
2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)

The Development of the Digital Economy and the Citizens' Right to Privacy

Malkerov V.B.

Ural state University of Economics, Yekaterinburg, Russia

ABSTRACT

The current digital progress in all the areas of various economic activities involves the processing of a much larger amount of data than it was ever necessary for any management decisions in the past. This tendency is mostly due to the rapidly increasing storage capacity, advanced ways of data processing and usage, as well as economic advantages; as better informed management decisions can be taken if a greater amount of data is processed. To reach a solution to a problem, various random data are specifically processed and considered. The feasibility of the solution reached depends on the amount of data processed, so anyone tends to acquire as much information as possible, even if the data have to be obtained illegally. The author considers the issues of legislation related to the protection of the citizen's right to private life provided that all interested parties have the capacity and the willingness to obtain the data. The current legislation related to the area discussed is studied and the drawbacks are highlighted. The author underlines possible risks for the development of the digital economy due to current legislation flaws.

Keywords: *digital economy, databases, legislation, privacy, individual digital profile*

1. INTRODUCTION

With the digitalisation of the economy, the modernization of the legislation, both Russian and international, becomes the fact of life and fosters the necessity of careful prediction of positive and negative tendencies in the socio-economic conditions locally as well as internationally. The maturing digital economy leads to powerful economic advances, and when the application of digital technologies to economic activities management is insufficient, this may constrain the overall economic development of the country and result in different negative consequences. It is apparent that the digital economy is reshaping the way many state and public institutions operate now; some of the existing institutions are going to be transformed or become extinct, while, other, new forms of institutions which cannot be even imaged now are going to emerge in the years ahead. The Internet and the application of information technology led to major changes in our everyday life. Nowadays, many employees successfully work from home, do their shopping online, get goods delivered to their houses, order and pay for services over the Internet. Human Resources are adapting to new ways of personnel hiring, with more and more people looking for jobs and human resources managers announcing vacancies online. [1] As a result of the maturing digital economy, the amount of data that has to be collected, processed and stored electronically on multiple servers is increasing rapidly, therefore, reasonable security measures should be set in motion to protect the data against unauthorised access and misuse. The challenges that organisations around the world are facing now include the potential harm to individuals, consequences of security breaches, possible pitfalls in data protection legislation, and possible implications they might have on the development of the digital economy.

2. RESEARCH METHODOLOGY

The present research was carried out using the comparative analysis method. The author explored the regulatory approaches applied by administrative bodies in the present and past acting within their respective information technology resources, and compared them with the approaches that are expected to be adopted by a greater range of administrative bodies in the future.

3. RESEARCH FINDINGS

In recent years a number of studies have been published which demonstrate that vast amounts of various media data, i.e., video footage, digitized medical data, aerial photography images, and other miscellaneous data generated by online activities and kept at cloud storages in numerous logical pools on multiple servers are steadily increasing with each passing year. [2] In this environment, should the security of personal data raise concerns or not? On the one hand, there are no apparent dangers of having fragments of your personal data stored digitally in different online storages. On the other hand, today, some

large companies possess the software enabling them to process pieces of anonymous data in order to create a digital profile of a particular person. [3] Therefore, considering the current technological advances, our ability to create digital profiles will develop to a much greater extent and interested parties might get access to a huge amount of different personal data. Should it raise concerns? Indeed, in some cases, a person might be put into real danger if a crime is being plotted against them. And with the help of the digital profile, criminals have more tools to commit the crime. However, there is no need to consider any extreme examples, when we can illustrate the importance of the issue by stating that every citizen is a consumer of certain goods and services. Market economy means that companies are constantly searching for ways to increase their market share, to retain or enlarge revenues, to find new ways and methods of expanding their business activities. A company that sells more goods or serves more customers is considered to be more successful. And the quality of those goods or services is not the only criterion to evaluate the company performance. Other significant factors include marketing, thorough knowledge of the market, advertising campaigns effectiveness, good customer service, etc. Aggressive advertising is one of the growing concerns nowadays. Since the early nineties advertising has remained its strong presence on TV, the radio, in newspapers, and it is hard to imagine mass media without advertising. With every passing year, advertising becomes more and more aggressive. First, advertisements were glued to the inside walls of the lifts in large apartment buildings, then, they were placed in mailboxes, and, finally, they got enclosed into envelopes containing utility bills. The ever-growing use of mobile phones resulted in new advertising trends. Recently, Russian customers have experienced a considerable increase in the number of advertisement calls and spam texts delivered to their phones and offering different goods or services. Moreover, Russian mobile operators have started enabling various paid options by default, and quite often customers cannot disable those foisted options themselves or by dialling the company. So, customers have to visit the offices of their mobile operator where they are offered even more options based on the content viewed online, links clicked, and their purchase history. Apparently, companies keep on expanding and improving their advertising tools to extend their market share and sales. Therefore, an increasing number of companies is eager to learn more about their potential customers, their preferences and habits. Targeted advertising is becoming more people-based. If the date of the planned meter maintenance is approaching, then the customer gets the utility bill together with the advertisement for the company offering meter maintenance service. Middle-aged people usually get advertisements of dental clinics, and older people are offered medicine or health products. Databases containing consumer personal data have become a valuable commodity, and nowadays, they are routinely bought and sold. As a result, the number of people and companies prosecuted for disclosing or selling personal data has significantly increased. One of the examples is the judgment of Ordzhonikidze regional court of Ekaterinburg to case 1-405/12 of 25 July 2017. [4] The sentence was not related to the trade secrets disclosure, but the disclosure of personal information database to a third-party. Consumer data have been exploited for advertising purposes for years now. In the early nineties, the author of this article witnessed the first attempts of using disclosed personal data for advertising purposes. At that time, advertisements promoting garden seeds were mailed from Moscow to those Russian citizens who had invested in MMM investment fund. It can be assumed that the database with investors' personal data was somehow obtained by the organisers of that advertising campaign for seeds. As the postal charges of mailing paper advertisements throughout the whole country were significant, it is likely that in order to create a customer profile, a preliminary psychological study of a typical MMM investor had been carried out and that target market analysis demonstrated that MMM investors were potential customers for garden seeds. At present time, many Internet users state that they observe targeted advertising, as when they start searching for goods or services online, they are shown advertisements of these goods or services based on their browser history and their preferences. In other words, nowadays, each and every customer online activity is closely tracked, thoroughly analysed and stored in various online databases to be later used for targeted advertising. The advances in psychological science, the increased capacity of computer technology and the ability to combine pieces of fragmented information from diverse websites, and then process the data in order to study customer behaviour and create customer profiles, give reasons to believe that every citizen is considered a potential customer. The data are collected and analysed with the purpose of developing the best-fit targeted advertisements which are expected to offer customers goods and services perfectly matching their individual needs and wants. On the one hand, targeted advertising cannot be considered a negative development, while, on the other hand, the opportunities and the demand for the digital profile creation suggest the data obtained can be exploited in different ways, and it is not easy to predict the purposes the data are going to be used for. Many digital customer profiles created for promotion purposes are most likely to be exploited for political advertising, i.e., they can be used to appeal to citizens for votes or support or to affect preferences. Therefore, many political parties are interested in digital customer profiles creation. It is apparent, that citizens becoming aware of the fact that huge amounts of information about them can be easily obtained, processed and systematized get concerns about the ways the information can be used by interested parties which may result in an certain increase in anxiety disorders.

Recently, the digitalisation process has provided employers with a range of powerful tools. Human Resources specialists are now familiar with Big Data and Human Resource analytics and have started successfully applying them on a day-to-day basis. Big Data is a term

used to describe large amounts of data, and Human Resource analytics involves a mathematical analysis of the data available in order to forecast the course of a particular phenomenon. People Data involves applying digital technology to an analysis of a whole range of data about its employees available both from outside sources and inside the company in order to make measured management decisions. The benefits of using special software to process the information about employees have already been discussed in many scientific papers. [5] We can assume that for the purpose of the analysis huge amounts of data can be handled, as modern software enables us to collect and process fragmented data to obtain desired information. And the processed data can later be disclosed to any interested parties. Moreover, it should be noted that currently many employers actively adopt polygraph testing to obtain more information about their employees [13]. The reasons behind using polygraph tests can be different, although mostly these tests are used to protect assets and to prevent employees hired for top level management roles from exploiting the resources available in their own vested interest. Internal theft, fraud and embezzlement are among topical issues faced by a huge number of Russian companies, as in the nineteen nineties during the economic reform, many private companies were established using assets of state-owned enterprises. At the aforementioned period the majority of businesses were started that way. In most economically developed countries, polygraph tests have been used since the twentieth century. The mentality of the population and the socio-economic environment have largely influenced the application of polygraph tests. In some countries, like the USA, Canada, and France, no public bodies that prevent discrimination and protect human rights expressed concerns over using polygraph tests, meanwhile in Sweden, Switzerland, Germany, and Norway there were attempts to impose prohibitions on the use of polygraph tests, however, they are regularly administered in these countries at present [6]. Polygraph testing is considered to be effective, that is why it is applied widely. For example, the USA administer approximately one million polygraph tests a year, with nearly 30 per cent of the tests completed for private business sector. [7] Although polygraph tests are considered to be highly accurate, with accuracy rate estimated about 80 per cent, they are not totally reliable. However, in modern Russia polygraph testing is gaining popularity. In 2007, eighty employees of Kazan city administration were fired after being tested, and, in 2010, nearly 40 per cent of Moscow municipal government were suspended from working with government orders after similar testing. [9] Considering all the above, we can assume that with technology advances, new methods, improved equipment and better training for polygraph examiners, the number of polygraph tests is expected to increase significantly in Russia. Thus, even more digital data on an individual will be collected, stored, and merged with other available data to be used for profile creation which might result in misuse or exposure.

Articles 21 and 23 of the Constitution of the Russian Federation state that people are guaranteed the right to personal and family secrets, as well as the inviolability of private life. Part 1 of Article 24 of the Constitution of the Russian Federation states that no collection, storage, use and dissemination of information about the private life of a person is allowed without their prior consent. These are the fundamentals of the Constitution applied to develop the legal procedure to protect the rights. Article 137 of the Criminal Code of the Russian Federation defines actions carried out in order to collect or disseminate data about a person's private life that reveals their personal or family secrets without their prior consent as criminal offence. Article 138 of the Criminal Code of the Russian Federation deals with the violation of the secrecy of correspondence, telephone conversations, postal, telegraphic or other messages. When compared, the term "trade secret" is rather accurately defined by the law enforcement, while the term "personal secret" has a rather complicated definition and, thus, results in certain difficulties in applying article 137 of the Criminal Code of the Russian Federation. The definition of the Constitutional Court of the Russian Federation dated 09.06. 2005 No. 248-0 is as follows "the term "private life" means an area of human activity that relates to an individual ... if it is not illegal in nature". As the result of the aforementioned difficulties in defining the term, the application of article 137 of the criminal Code of the Russian Federation on collecting or disseminating data about a person's private life remains the subject of concern and can only be used when the negative consequences of the data dissemination are indisputable. Let us consider the verdict of Krasnokameskii city court in Transbaikal Territory dated 26.06.2012 when a citizen was charged with blackmailing another person and threatening to disclose data on private life. [10]

As stated in article 152 of the Civil Code of the Russian Federation, civil law provides for the possibility to protect human rights against revealing any data that might contain defamatory information discrediting the honour and dignity of a citizen. According to this article, if the information disclosed contradicts the facts, then a citizen is entitled to petition for a retraction of the information denigrating honour or dignity. V.A. Mescheriagina underlines the fact that if the information discrediting the honour and the dignity of a citizen is disclosed, but that information does not contradict the facts, then "this citizen is deprived of the right of applying law to protect their rights". [11] It should be noted that Russian civil law has not been adapted to the conditions created by the digital economy yet. Let us consider Article 141.1 of the Civil Code of the Russian Federation which was adopted by the Federal Law on 18 March 2019 and defines the digital rights as "the contractual and other civil rights. The content of the digital rights and the conditions of their application are determined in compliance with the rules of the information system that acts in accordance with statutory criteria. The implementation, disposal, including by means of transfer, pledge, or encumbrance of digital

rights or disposal restriction are allowed in the information system without any third party. In real life the validity of a transaction might be questioned, it might require a specific procedure (for example, signing must be witnessed by a notary) and this procedure has not been defined clearly yet. It is necessary to note that currently the law only regulates the issue in general terms for it to be later resolved with the help of a judicial precedent.

The Labour Code of the Russian Federation has not been adopted to meet the requirements of the digital economy either. There are some provisions related to employees' personal data in Chapter 14 of the Labour Code of the Russian Federation that pose difficulties for the law enforcement practice. On the one hand, Article 86 of the Labour Code of the Russian Federation states that "an employer does not have the right to receive or process any employee personal data related to their membership in any public associations or their trade union activities, with the exception of those cases which are stipulated by the present Code or other Federal laws..." On the other hand, Article 374 of the Labour Code of the Russian Federation forbids firing trade union leaders at certain levels without prior consent of a higher trade union body. If this consent is refused by the higher trade union body, then the employer has the right to appeal in court. There are certain difficulties in complying with this law, as employers are forbidden to collect data on the union status of their employees, while, at the same time, they have to follow certain procedures when firing such employees. In fact, the contradictions in Article 86 and Article 394 of the Labour Code of the Russian Federation can be explained by a clause in the first of these two. It states that the data on the union status of their employees cannot be processed except in cases specified by law. We can assume that Article 394 of the Labour Code of the Russian Federation can be considered the case in question. However, there is no direct reference, which leads to various speculations and is often exploited by employees. Those employees who possess certain guarantees against being fired without a prior consent, do not inform their employers about their privilege and after being fired take legal action against their employers and make compensation claims. There have been a number of similar cases, in which not only trade union leaders, but other employees have been reported to taking advantage of their privileges (pregnant women and new mothers among them). During the trial, the defendants may state that the claimants abuse their rights to a certain privilege, only it is really ardours to prove that the claimants exploit their rights. Therefore, the Labour Code of the Russian Federation has some apparent inconsistencies which are related to personal data storage and processing and which can lead to obvious obstacles in applying laws in the digital economy.

4. THE DISCUSSION OF THE FINDINGS

Modern technologies, business and political organisations require different personal data, which can be of some minor importance, like health related data, family life, habits and preferences to create a digital profile. The data are collected to be later used for various commercial purposes, and for targeted advertising, in particular. Therefore, citizens experience a great deal of difficulties attempting to protect their rights and to make organisations totally comply with Article 24 of the Constitution of the Russian Federation. With the advances in the information technology application, this trend is going to develop even further, which, in turn, may result in increased anxiety. We have to admit, that, currently, modern areas of law related to the regulations in the economic sphere (criminal, civil, and labour) are not prepared to handle the increased demands of the economy digitalisation. Taking into account the current economic environment in Russia, we can assume that one more leverage might appear and be exploited by the law enforcement. Citizens' frustration with the increased intrusion in their private life and tampering with their personal data might lead to the tightening in applying Article 137 of the Criminal Code of the Russian Federation. Other countries might experience similar issues. Our world is rapidly changing, and we are constantly adapting to new ways, welcoming challenges. According to Wiliam Mougayar "these new areas will include banking without banks, gambling without the house's edge, title transfers without central authorities stamping them, registrations without government officials overseeing them" [12]. That is why careful forecasting taking into account all the possible outcomes is crucial.

5. CONCLUSION

The following preventive measures have to be urgently considered in order to avoid the escalating social tension:

- A legal framework that can restrict the design and production of individually targeted advertisements in order to derail the increased interest in personal data has to be introduced.
- Patterns in law application, Articles 137 and 138 of the Criminal Code of the Russian Federation, in particular, should be closely monitored to prevent any exploitation of power by authorities due to the increase in the digital technology application.
- Civil, Labour, and other legal areas have to be adapted to the new emerging realities of the digital economy in order to identify and correct any possible contradictions or flaws in the current legislation.

REFERENCES

[1] Roshchin S. Yu., Solntsev S. A. How companies look for workers: empirical estimates for Russian enterprises // Ros. journal management. - 2017. - T. 15, No. 2. - P. 173–192. - DOI: 10.21638 / 11701 / spbu.2017.2017.203.

[2] Volkova Yu. S. Big data in the modern world // Concept. 2016.Vol. 11.p. 1171–1175

[3] Belaya O. V., Kononenko D. B., Semchenkova M. N. Legal regulation of startups in the field of Big data (big data) // Business. Education. Right. Bulletin of the Volgograd Institute of Business. 2018.No 1 (42). p. 174−180

[4] http://sud-praktika.ru/precedent/366904.html

[5] Vorobev L. A., Panasenko G. N. Opportunities and prospects for the development of technologies based on Big Data in HR // Human Resource Management - the basis for the development of an innovative economy. - 2015. - No. 6. - p. 67–75.

[6] Anoshin K.V. Shigirdanova I.Yu. The attitude of citizens towards the use of polygraph technology in public authorities. Materials Afanasyev readings. 2018. No2 (23). S.11-25. p. 12

[7] Samofalova V.V., Posokhov S.E. Polygraph today: application problems. Central Scientific Herald. 2018.V.3. No. 10S (51S) P..22-24 p. 22

[8] Kuznetsov A.A., Rogozhina V.V. Polygraph - from history to the present day. Bulletin of modern research. 2018. №11.8 (26) p. 55-57 p. 56

[9] Patova E.M. Anti-corruption mechanisms in the implementation of the personnel policy of state bodies and local authorities // Journal of Russian Law. 2016. N 12. p. 114-122.

[10] http://oukrf.ru/st137

[11] Meshcheryagina V.A. The right to oblivion as the new competence of the constitutional right to privacy. Problems of interaction between public and private law in the regulation of the digitalization of economic relations. Materials of the third international scientific-practical conference. Yekaterinburg Ural State Economic University 2019 p.44

[12] Mogayar W. Blockchain for business / translated from English D. Shalaeva. M .: Eksmo, 2018.p. 183

[13] Novgorodov P. A. Otsenka stoimosti intellektual'nogo kapitala vuza: metodiches- kiy aspect [Valuation of higher education institution's intellectual capital: The issue of method- ology]. Izvestiya Uralskogo gosudarstvennogo ekonomicheskogo universiteta = Journal of the Ural State University of Economics, 2019, vol. 20, no. 1, pp. 78–94. DOI: 10.29141/2073-1019-201920-1-6.