GDPR implementation as the main reason for the regional fragmentation in the online mediasphere

Mikhail Smolenskiy[1,2] and *Nikolay* Levshin[2*]

[1]Don State Technical University, Gagarin sq., 1, Rostov-on-Don, 344003, Russia
[2]Rostov State Transport University, Rostovskogo Strelkovogo Polka Narodnogo Opolcheniya sq., 2, Rostov-on-Don, 344038, Russia

Abstract. The EU's General Data Protection Regulation (GDPR) applies not only to the territory of the European Union, but also to all information systems containing data of EU's citizens around the world.Misusing or carelessly handling personal data bring fines of up to 20 million euros or 4% of the annual turnover of the offending company. This article analyzes the main trends in the global implementation of the GDPR. Authors considered and analyzed results of personal data protection measures in nineteen regions: The USA, Canada, China, France, Germany, India, Kazakhstan, Nigeria, Russia, South Korea and Thailand, as well as the European Union and a handful of other. This allowedidentifying a direct pattern between the global tightening of EU's citizenspersonal data protection and the fragmentation of the global mediasphere into separate national segments.As a result of the study, the authors conclude thatGDPRhas finally slowed down the globalization of the online mediasphere, playing a main role in its regional fragmentation.

1 Introduction

Modern technologies allow to transmit information from one end of our planet to another in seconds, addressing it to billions of different recipients. And, since distributing information through television and radio channels seems to be quite expensive, computer networks have become the true embodiment of modern ideas about the freedom of information exchange.

The capabilities of computer networks brought the mediasphere to a fundamentally new level. Thanks to the ubiquitous spread of the Internet, publishers were able to expand their audiences virtually unhindered beyond the borders of the state in which they were originally registered.

Entry into foreign markets no longer required large financial investments from publishers. Due to the absence of the need to distribute physical media, publishers could avoid the costs that entailed the export of media abroad or the rental of local facilities for their production[1]. All this created optimal conditions for the mediasphere globalization.

*Corresponding author: info.law.expert@yandex.com

However, in the real world, the borders between states have not gone anywhere.States seek to protect the data of their citizens. The general trend is the desireto prevent the spread of citizen's personal data beyond geographic boundaries of its state of origin. This inevitably creates legal problems for the functioning of global information systems [2-4].

The negative consequences of GDPR implementation become increasingly obvious as global data-intensive technologies become ubiquitous.One of the first victims of the GDPR implementation became the online mediasphere.

2 Materials and methods

This article relies on analysis of international documentary sources, all of which are public. These sources include general and specialized books, public documents, government reports, periodicals and scholarly research papers, academic and business literature. The authors used the method of comparative analysis to evaluateresults of GDPR implementation in differentstates. Methods of statistical and logical analysis also used to analyze the accumulated data.

3 Results

The study made it possible to identify a direct pattern between the GDPR implementation and the fragmentation of the global mediasphere into separate national segments.The introduction of the GDPR has led to the fact that the residents of the European Union have partially lost access to media resources of other states.As a result of the study, the authors conclude that General Data Protection Regulation has finally slowed down the globalization of the mediasphere, playing a decisive role in its regional fragmentation.

4 Discussions

Many researchers agree that globalization and digitalization have a positive impact on all spheres of human activity [5]. It seemsthat the mediasphere is no exception. Globalization and digitalization offer greatest opportunities for global information exchange [6-7]. Data becomes the metaphorical lifeblood of the global business. This is especially important in the aspect of development of new information technologies: Artificial Intelligence [8], Big Data, Cloud Computing and Internet of Things.

All of these technologies involve the use of automatic processing of huge volumes of data. Therefore, any additional data checks may lead to a decrease of effectiveness of these technologies.By complicating data processing processes, we slow down the development of all these technologies.

Digitalization opens up new horizons for doing business. However, it is very important to understand that the uncontrolled development of information technologies can threaten people [9-13]. Understanding that access to personal data creates a large number of potential threats has led to a tendency to tighten legislation on personal data.

All the reasons that different states justify restrictions on the dissemination of data can be roughly divided into three main groups:

- ensuring privacy and security;
- countering foreign surveillance;
- promoting economic development.

As we can see from the dates in this review the main wave of changes in the legislation on personal data in different countries swept after the publication of the story of Edward Snowden. This story is about the unprincipled violation the rights of citizens to private life

by state bodies. Therefore, the idea of dataensuring privacy and security looks quite justified.

Considering the task of attracting investment, it is not so clear.By introducing restrictions on the dissemination of personal data outside the state, we restrict our own citizens in access to global resources and increase the costs of small businesses. This can lead to a slowdown in technical progress and economic development of the state. It should also be remembered that data warehouses consume a huge amount of energy. Therefore, in the case of construction of new storage facilities, one can expect an increase in the cost of electricity and dissatisfaction with local energy consumers.

Butdozens of different countries have long adopted laws aimed at protecting the data of their citizens. They are putting up barriers to the free flow of personal data across regional borders. Data transfer becomes expensive or illegal.

Back in 2006, China applied e-banking law that requires e-banking data to be stored in China. Since then, Chinese data legislation has tightened several more times. The largest number of changes in Chinese personal data law occurred in 2016. In 2016, service customer data and cloud computing data were added to the list of data to be stored in China. In 2017, they added a ban on cross-border transactions with data that could pose a threat to national security.

The government of Kazakhstan has decided that since 2005, the entire infrastructure of the national segment of the domain name system should be stored on servers located inside the country. In 2015, an additional requirement was approved for the storage of data of citizens of Kazakhstan within the country.

In Russia, the law on the localization of personal data on the territory of the state was introduced in 2015 [14]. At the same time, the Russian government decided that the content of all messages transmitted between users must be injured within 6 months. The legislation on the storage of personal data of South Korean citizens is in many ways similar to the Russian one. The only difference is that in 2013 some companies received the right to store data outside the country.

Back in 2012, the medical legislation of Australia was supplemented by the requirement to store the medical data of citizens on the territory of the country. In the same year, a law was passed in Bulgaria instructing the gambling business to store customer data on the territory of the country.

Indian legislation allows for the transfer of citizens personal data on the territory of other states, but only in strictly defined by law. Taiwan's legislation in this regard is more democratic, but also provides for the possibility of restricting data transfer in order to ensure national security.Thai citizens transfer their data to the territory of another state by providing written consent.

Back in 2010, Malaysia passed a law stating that the data of its citizens should be stored only within the country. But there are a number of exceptions that allow Malaysian citizens to transfer data outside the country.

In 2013, the Government of Nigeria decided that all data of citizens should be stored on the territory of the country. It can be assumed that the main purpose of this restriction was to attract investment in the information industry in Nigeria, and not at all to care for the interests of citizens.

Vietnam also updated its personal data legislation in 2013. However, most of the changes were aimed not at attracting foreign investment or protecting user data, but at strengthening government control over the dissemination of information.

Venezuela requires that all information about electronic payments of citizens be stored internally.An interesting law has been in force in Turkey since 2013 obliging all payment systems to store transactions of Turkish citizens in Turkey for 10 years from the date of their creation. Storing other types of data is described in intricate rules.

United States of America prescribes in-country storage of Department of Defense data and Internal Revenue Service data. Canada and the Netherlands requires to keep the country data of state bodies. Germany and France have made efforts to force companies operating in their countries to store all data also on their territory. At the same time, they provided separate clouds for storing government data.

But the biggest damage to the global mediasphere was caused by the implementation of the EU's General Data Protection Regulation. GDPR applies to all information systems containing data of EU's citizens around the world. Misusing or carelessly handling personal data bring fines of up to 20 million euros or 4% of the annual turnover of the offending company.

After the upcoming GDPR, online media owners around the world had three ways to avoid penalties:

- adaptation of information systems in full compliance with the all requirements of the GDPR;
- exclusion of the collection, storage and processing of personal data of citizens of the EU's citizens, while preserving the opportunity for them to receive information;
- blockaccess to the information system for EU-based users.

All these methods involve certain financial losses. The most expensive solution is one that implies a complete redesign of the information system to meet the requirements of information legislation. There are still many unresolved problems. For example, it is not clear whether it is necessary to spend resources on deleting personal data from old backups [15].

A slightly less costly method is the refusal to collect, store and process personal data of EU citizens. For example, a number of media companies offer EU citizens access to a text-only version of their electronic resources (Table 1). These lite versions do not include tools for collecting user data, thus avoiding accusations of violating the GDPR.

Table 1. Examples of actual text-only versions of online media resources.

Media company name	UniformResourceLocator
CNN (Cable News Network)	http://lite.cnn.io
National Public Radio	https://text.npr.org
The Christian Science Monitor	https://www.csmonitor.com/layout/set/text/textedition

These lightweight versions of online media were originally created to deliver news during natural disasters. As a rule, during natural disasters, communication networks are under serious stress, so online media decided to ease the speed of their Internet pages by getting rid of unnecessary decorations and ad units. Later, the owners of media companies came up with the idea that these lightweight versions can be provided to users from the European Union, since they do not contain tools for obtaining information about users. However, it should be born in mind that by providing users from the European Union with these lightweight versions, owners of electronic resources incur losses. They consume system resources, but do not compensate for them, since users of the lite version do not receive ads.

Therefore there is nothing surprising in the fact that most popular American media companies prefer isolation strategy.Popular sites within the Tronc (the Baltimore Sun, the Chicago Tribune, the Orlando Sentinel, the New York Daily News and the San Diego Union-Tribune) and Lee Enterprises (46 daily newspapers across 21 American states) media publishing groups started blocking EU-based users from reading their content. For

example, TroncInc sites redirected EU-based users to a page with the message: "Unfortunately, our website is currently unavailable in most European countries". Along with blocking access, users were removed from the site database.

We shouldn't think that online media are the only ones affected. The implementation of the GDPR has become a problem for all information systems that can contain data from citizens of different states. Researchers from different countries are still looking for ways to implement GDPR in various information systems [16-17].

Looking at the amount of fines (Table 2), we can understand the reluctance to process the personal data of EU citizens. The UK was the most demanding data protection authority in Europe, imposing fines totaling around €44 million, followed by Germany (€36.16 million), Italy (€12.38 million), Sweden (€ 7.25 million) and Spain (€5.59 million). In terms of the number of issued fines, the Spanish AEPD (Agencia Española de Protección de Datos) was in the lead, which issued 24 fines in the Q4 2020 and 131 fines for the entire 2020. This is almost half of all GDR fines issued in 2020.

Table 2. Amount of GDPR fines by countries.

Country	Q4 2020 (€)	total fines issued in 2020 (€)
Austria	750	850
Belgium	68.000	805.700
Bulgaria	none recorded	2.000
Cyprus	22.000	115.200
Denmark	none recorded	195.600
Estonia	none recorded	100.548
Finland	none recorded	207.500
France	3.066.300	3.316.300
Germany	36.158.708	37.398.708
Greece	1.000	35.000
Hungary	113.525	415.910
Isle of Man	none recorded	12.250
Ireland	450.000	565.000
Italy	12.357.601	69.657.547
Latvia	21.250	21.250
Lithuania	15.000	15.000
Netherlands	none recorded	1.355.000
Norway	19.100	978.590
Poland	716.080	757.206
Romania	125.000	184.650
Spain	5.585.600	8.116.10
Sweden	7.248.260	14.280.060
UK	43901.000	43.901.000

The total amount of fines for violations of the GDPR in 2020 was 182 million euros. The GDPR fines for Q4 2020 break down as follows (Table 3). Most of the fines were issued for violations of GDPR Articles 5, 6 and 32, which contain the basic principles of personal data processing.

Table 3. Amount of GDPR fines for Q4 2020.

Month	Amountoffines (€)
October	78.204.258
November	23.412.061
December	8.352.855

The main amount of fines in Q4 2020 accounted by some major cases. For example, in October 2020, the clothing retailer H&M (Hennes&Mauritz) was fined €35.3 million for keeping "excessive" records about employees at its Nuremberg service centre. In November 2020, the Italian data protection authority fined Vodafone more than €12.25 million for unlawfully processing the personal data of millions of users for telemarketing purposes. Also, in November 2020, the ICO fined the ticket sales and distribution company Ticketmaster £1.25 million for failing to implement appropriate technical and organisational measures to secure its customers payment details.

These colossal amounts of fines make it possible to understand why the GDPRimplementation was the driving force that led to the regional fragmentation of online mediasphere. The desire to avoid such hefty fines really prompts us to refuse to receive data from EU-based users.

The main problem with the implementation of the GDPR is that many of the features of its practical application are still not clear.There are still many open questions. For example, it is not clear how to be in a situation when the site administration wants to block a user for violating the site rules. To block a user, you need to use his data so that he cannot create a new account. Obviously, in this case, the use of the data is contrary to the interests of the blocked user. Does this mean that the site administration has no right to block users for violating the rules?

In a cybercrime investigation article by IngeSebyan Black and Lawrence J. Fennelly mentioned that the implementation of the GDPR has made it difficult to find criminals [18]. This is really an interesting problem. In order to identify a criminal, it is often necessary to store data that allows him to be identified. This goes against the prohibition of storing data contrary to the interests of the user.

Summing up the general result of the discussion, it can be stated that despite the fact that various social spheres have suffered from the implementation of the GDPR, it was the media sphere that received the greatest damage. This is not only about financial damage, but also about the loss of the possibility of free dissemination of information, which has become the reason for the national fragmentation of the mediasphere.

In the end, the question arises: is the fragmentation of the global mediasphere really the only way to make people's lives more convenient and safer?

5 Conclusion

In the course of the analysis, it was concluded that if at first the development of the Internet created favorable conditions for the globalization process in the mediasphere, this process continued only until the laws of individual regions did not begin to contain provisions that tightened data storage and processing regulations.

Based on the results and discussion, we can make a general conclusion that the personal data protection measures of individual regions played a crucial role in stopping the globalization of the mediasphere. These changes in international law served as a serious organizational and economic obstacle for expanding the audience of media companies at the expense of citizens of other regions and initiated the process of national fragmentation of the mediasphere.

References

1. N. Kovalchuk, et al., Astra Salvensis, **6**, 255-264 (2018)
2. R. Taylor, Telecommunications Policy, **44 (8)** (2020), doi:10.1016/j.telpol.2020.102003
3. J. Lee, Procedia Computer Science, **91**, 542-546 (2016), doi:10.1016/j.procs.2016.07.138
4. J. Garber, Computer Fraud & Security, **6**, 14-15 (2018), doi:10.1016/S1361-3723(18)30055-1
5. I. Abakumova, et al., E3S Web of Conferences, **210**, 20015 (2020), doi:10.1051/e3sconf/202021020015
6. N. Morozova, et al., Lecture Notes in Networks and Systems, **57**, 236-240 (2019), doi:10.1007/978-3-030-00102-5_25
7. P. Taranov, Current Achievements, Challenges and Digital Chances of Knowledge Based Economy, 597-609 (2021), doi:10.1007/978-3-030-47458-4_69
8. J. Meszaros, Ch. Ho, Computer Law & Security Review, **41**, 105532 (2021), doi:10.1016/j.clsr.2021.105532
9. N. Alieva, et al., Lecture Notes in Networks and Systems, **57**, 1020-1026 (2019), doi:10.1007/978-3-030-00102-5_108
10. L. Barashyan, et al., Humanities and Social Sciences Reviews, **7 (5)**, 738-743 (2019), doi:10.18510/hssr.2019.7591
11. O. Grechenkova, Y. Kuzmenko, Lecture Notes in Networks and Systems, **57**, 612-621 (2019), doi:10.1007/978-3-030-00102-5_64
12. V. Zvereva, Russian Literature, **118**, 107-140 (2020), doi:10.1016/j.ruslit.2020.11.005
13. P. Anesa, Discourse, Context & Media, **35** (2020), doi:10.1016/j.dcm.2020.100398
14. A. Savelyev, Computer Law & Security Review, **32**, 128–145 (2016), doi:10.1016/j.clsr.2015.12.003
15. E. Politou, Computer Law & Security Review, **34 (6)**, 1247-1257 (2018), doi:10.1016/j.clsr.2018.08.006
16. F. Menges, et al., Computers & Security, **103**, 102165 (2021), doi:10.1016/j.cose.2020.102165
17. M. Shuaib, et al., Materials Today: Proceedings (2021), doi:10.1016/j.matpr.2021.03.059
18. I. Black, L. Fennelly, Investigations and the Art of the Interview (Fourth Edition), 173-177 (2021), doi:10.1016/B978-0-12-822192-1.00020-9