10.53477/2668-2028-21-20

LEGAL FRAMEWORK FOR DATA RETENTION IN THE RUSSIAN FEDERATION

Savov ILIN, PhD
Professor, Ministry of Interior Academy, Sofia, Bulgaria
ilin_savov@abv.bg

Abstract: *The report examines and assesses the existing procedures for data retention to be used to combat crime and terrorism in the Russian Federation. The procedures regarding the control over data retention are presented and systematized. The existing differences between the Russian Federation and the member states of the European Union regarding the adopted legislation are described.*

Keywords: *information; data retention; crimes; terrorism; Russia; European Union.*

Introduction

With the development of technologies to facilitate the monitoring of means of communication by law enforcement agencies, states cannot always ensure that laws and regulations related to the control of communication networks adhere to international human rights and adequately protect the right to privacy and freedom of speech. Privacy is a fundamental human right and plays a key role in maintaining a democratic society. It is an integral part of human dignity and reinforces other rights, such as the right to freedom of expression, the right to free access to information and freedom of association, and is recognized by international human rights law. Actions restricting the right to privacy, including the control of telecommunications networks, may be lawful only if they are provided for by law, are necessary to achieve legitimate aims and are proportionate to the aim pursued.

Before the Internet became so widespread, the legal principles and logistical difficulties inherent in monitoring communication networks created restrictions on the control of communications by public authorities. In recent decades, logistical barriers to interception of communications have been reduced, and the application of legal principles in the new technological context raises many questions.

The rapid development of the industry, in which practically everything is transmitted in digital form, and the information about the transmitted data or traffic data from the communication (remember, this is the information about human communications or the electronic devices used by him), the rapidly decreasing price for storage and retrieval of huge amounts of data, as well as the provision of personal data by users to external service providers, has allowed the state to carry out surveillance on an unprecedented scale. Now the formation of the understanding in the modern legislation in the field of human rights fails to keep pace with the existing and constantly changing possibilities of the state to monitor communications, the ability of the state to collect and analyze information obtained with the help of various technologies monitoring, or the increasing sensitivity in society to the state's ability to access information.

The frequency with which the state turns to access the content of information exchange and its traffic data is growing rapidly without the presence of any competent verification. For example, in the UK every year, 500,000 inquiries are made annually about the provision of data retention; in the country, there is virtually self-government for police authorities to decide on their own requests for access to information held by communication service providers. In South Korea in 2011 and 2012, 6 million requests for information on subscribers or authors and about 30 million requests for other types of data retention were submitted annually.

Receiving and analyzing data retention from communications allows to create a profile of human life, including information about the state of his health, political and religious views, connections, interactions and interests, revealing as much or even more information than can

be obtained having access to the content of the information exchange[1]. In order for States to be able to effectively fulfill their obligations under international human rights relating to the interception of transmitted information, they must comply with international principles. These principles must be applicable both to the monitoring applied by the state structures and extraterritorially. The principles are applicable regardless of the purpose of the data interception: support the activities of law enforcement agencies, combating serious organized crime and terrorism, protection of national security or any other state goals[2].

"Communication control" in modern conditions includes monitoring, interception, collection, analysis, use, preservation and storage, interference or access to information that contains, reflects, originates from or is part of human communication in the past, now or in future[3].

Given the speed with which technological progress is evolving, laws restricting the right to privacy must be subject to periodic review through participatory[4] legislative and regulatory processes.

Laws allowing the monitoring of communication networks by certain state agencies should limit this action only in cases where this need is absolute and obvious in order to achieve a legitimate aim. The interception of data from communication networks should only take place when it is the only means of achieving the legitimate aim or, in the presence of multiple means, that means is least likely to lead to human rights violations.

The responsibility for establishing this exculpatory circumstance in judicial as well as in legislative proceedings lies with the state. Decisions on the control of communication networks must be taken by a competent judicial body that is impartial and independent.

Appropriate legal procedure requires the state to respect and guarantee human rights by ensuring that the procedure provided for in the law, which restricts the violation of his rights, is sufficiently described in the law, appropriate for practice and accessible to the general public.

The state must ensure transparency regarding the use, scale and potential of surveillance technologies. It must provide, as a minimum, summary information on the number of intercepted and rejected wiretapping requests, the distribution of requests by communication service providers, the type of investigations and their objectives. The state must provide the public with sufficient information so that people can fully understand the scale, nature and application of the laws allowing the control of communication networks.

Europe can be given as an example of compliance with these international principles. The EU enjoys one of the most protected systems in this area, based on Council of Europe Convention № 108 and European Union (EU) acts, as well as the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

Legal possibilities for control of communications and retention of data by the authorities in the Russian Federation

The actions of law enforcement agencies to obtain such information are related to the requirement of Ch. 2 art. 23 of the Constitution of Russian Federation, establishing that the right of citizens to secrecy of correspondence, telephone conversations, postal, telegraphic and other communications may be limited only on the basis of court decisions.

---

[1] P. Marinov, *Terrorism – Abstractions and Realities*, East-West, Sofia, 2016, ISBN 619152866-3.

[2] P. Marinov, *Contemporary Challenges for the Management of the security and counter-terrorism system*, East-West, Sofia, 2016.

[3] L. Milushev, *Preparation of the governing bodies and the crisis response forces - a significant resource for crisis protection*, First National Scientific Practical Conference on Emergency Management and Protection of the Population, Sofia, BAS, 2005.

[4] *Participatory processes – all participants in these processes are provided with a real opportunity for expression. This evokes a sense of empathy, which dramatically increases motivation and creativity.*

The procedures for obtaining information on data retention in the investigation of crimes and terrorism are legally regulated in the Criminal Procedure Code of the Russian Federation[5] and the Communications Act[6].

Article 186.1 "Receiving information about the connections between the subscribers and (or) the subscriber devices" was introduced by Federal law on 1.07.2010. Point 1 of that article states:

"1. If there is sufficient grounds to assume that the information about the connections between subscribers and (or) subscriber devices is relevant for the criminal case, the receipt by the investigator of the said information is allowed on the basis of a court decision adopted in accordance with Art. 165 of this Code".

Pursuant to Article 165, the investigator, with the consent of the head of the investigative body, and the investigator, with the consent of the prosecutor, shall submit to the court a request for an investigative action, on which a decision shall be taken. The investigator's request for an investigative action concerning the receipt of information on the connections between the subscribers and / or the subscriber devices shall indicate:

- The criminal case, in the proceedings of which it is necessary to carry out the specified investigative action;
- The grounds for which it is necessary to carry out the said investigative action;
- The period for which the relevant information must be obtained and / or the time limit for the production of the said investigative action;
- The name of the organization from which the information is to be obtained.

The request shall be submitted for consideration by a single judge in a district court or a military court of the respective level in the place of the preliminary investigation or the investigative action, who must announce his decision no later than 24 hours from the moment of the request.

The prosecutor, the investigator and the police officer have the right to participate in the court hearing. The judge must announce in his decree for authorization of proceedings of the investigative action or for refusal of its proceedings, indicating the reasons for the refusal.

In case the court adopts a decision for receiving information about the connections between the subscribers and/or the subscriber devices, the investigator shall send a copy of this decision to the respective organization providing telecommunication services. The head of this organization is obliged to provide the specified information on some material carrier. The information shall be provided in a sealed form with a cover letter stating the period to which it relates and the number of the subscriber and/or the subscriber unit.

The receipt of information from the investigator on the connections between the subscribers and / or the subscriber devices can be established for a period of six months. The relevant telecommunications organization shall be obliged to provide the investigator with the specified information during the entire period of production of this investigative action in the cases of its receipt, but not less than once a week.

The investigator examines the provided documents containing information about the connections between the subscribers and / or the subscriber devices with the participation of a specialist (if necessary), for which he draws up a protocol (by analogy with other procedural actions in Russia) in which this part of the information, which in the opinion of the investigator is relevant to the criminal case (date, time, duration of connections between subscribers and / or subscriber devices and other data). The persons who are present at the drawing up of the minutes shall have the right to state their remarks in the same protocol or separately from it.

The provided documents, containing the information about the connections between the subscribers, shall be attached to the materials of the criminal case in full on the basis of a decree

[5] "Criminal Procedure Code of the Russian Federation" dated 18.12.2001 N 174-FZ.
[6] Federal Law of 07.07.2003 N 126-FZ.

of the investigator as material evidence and shall be kept in a sealed form, excluding the possibility of acquaintance with them and ensuring their storage.

If the need for the said investigative action disappears, its proceedings shall be terminated by a decree of the investigator, but not later than the completion of the preliminary investigation in the criminal case.

In exceptional cases, due to circumstances that cannot be postponed, the said investigative actions may be carried out on the basis of a decree of the investigator or the investigator without obtaining a court decision. In this case the investigator or the police officer shall notify the judge and the prosecutor no later than three days from the beginning of the investigative action. A copy of the decree and the protocol for the investigative action for verification of the legality of its proceedings shall be attached to the notification.

Upon receipt of the notification, the judge shall check the legality of the actions within the already indicated term and issue a decree on its legality or illegality. In the cases when the judge recognizes the actions as illegal, then all the evidence obtained in the course of this investigative action shall be recognized as inadmissible in accordance with Art. 75 of the Criminal Procedure Code of the Russian Federation.

The obligations of the telecommunication operators are regulated in art. 64 of the Communications Act[7]. According to item 1 of this article, the operators are obliged to store on the territory of the Russian Federation:

1. Information on the facts of reception, transmission, delivery and/or processing of voice information, text messages, images, sounds, video and other messages of the users of communication services - within three years from the moment of completion of such actions.

2. Text messages of the users of communication services, voice information, images, sounds, video, other messages of the users of communication services – up to six months from the moment of their reception, transmission, delivery and/or processing[8].

Telecommunication operators are obliged to provide to the authorized state bodies, carrying out operative-search activity or ensuring the security of the Russian Federation, the indicated information, the information about the users of communication services and about the provided communication services and other information necessary for the implementation of the assigned to these bodies tasks, in cases established by federal law. It is noteworthy that in such a general wording the obligations of the operators are fixed from July 6, 2016.

There is a legal norm in the legislation of the Russian Federation, unknown in the legislation of the European countries, when it is possible to suspend the provision of communication services. It is carried out on the basis of a motivated decision in writing to one of the heads of the body carrying out operative-search activity or ensuring the security of the Russian Federation, in the cases established by federal laws.

Communication operators are obliged to restore the provision of communication services on the basis of a court decision or a reasoned decision in writing to one of the heads of the body conducting operational search activities or ensuring the security of the Russian Federation, which has decided to suspend the provision of communication services.

Based on the above, the following conclusions can be made:

1. In the legislation of the Russian Federation, like our Law on Electronic Communications, there is no detailed indication of the crimes for which information may be requested about the connections between the subscribers and/or the subscriber devices. Moreover, there is no mention of the gravity of the crimes for which such information may be requested from the competent authorities.

[7] Federal Law "On Communications" of April 7, 2020 N 109-FZ.

[8] Sub-point 2 from vol. 1 to chapter 64 entry into force from July 1, 2018 (Subparagraph 2 of paragraph 1 of Article 64 shall enter into force on 1 July 2018).

2. As of July 2016, the information on the facts of the provided communication services must be stored for three years, ie. significantly longer than the period set out in data retention legislation in most EU Member States.
3. The content of the text messages of the users of the communication services, voice information, images, sounds, video and other messages of the users of the communication services must be kept for six months.
4. Telecommunications operators shall provide not only information on traffic data and subscribers, but also "…other information necessary for the performance of the tasks assigned to those authorities…", ie. there is no precise definition of the type and volume of information provided by operators.

Conclusions

The sustainability of the management and functioning of public relations in the context of crime is increasingly reflected in various scientific research sections[9]. The scope of consideration is constantly expanding and a look at the various expressions of crime inevitably shows that the need for constant in-depth scientific analysis in modern reality has not passed, but is still a hot topic for reflection.

If we look at the different scientific points of view, we could see a variety of scientific understandings of the basic, essential and secondary, non-essential aspects of the nature and content of crime.

The information received by the law enforcement agencies through the communication operators is limited by the current legislation in the Russian Federation, mainly due to different interpretations of legal norms by different court panels. In these conditions, constant improvement of the legal norms regulating the powers of the human rights bodies for access to the information of the communication operators is required.

As in other countries, so in the Russian Federation ensuring the protection of citizens from criminal encroachments, effective detection and investigation of serious crimes and terrorist attacks in modern conditions is impossible without the use of information circulating in electronic communications networks and without the involvement of the technical resources of the communication operators.

The new computer and information technologies and their introduction in the field of preparation and commission of criminal encroachments inevitably lead to the substantiation and application of innovative approaches, policies and practices for comprehensive counteraction to crime. In today's everyday life, it is more than necessary to combine all the various tools and resources in an integrated way to achieve a drastic reduction in the levels of individual types of crime.

[9] L. Milushev, *Social Aspects of Crime, MNC "Security in Southeast Europe, Crises, Challenges, Policies"*, Sofia, 2011, Proceedings, Demax.

BIBLIOGRAPHY

1. *Criminal Procedure Code of the Russian Federation* dated 18.12.2001 N 174-FZ.
2. *Federal Law* of 07.07.2003 N 126-FZ.
3. SAFRONOV I., Chernenko E., *He who has ears, let him hear again*, Kommersant (July 16, 2014).
4. PHILIP Molnar, *Restricted web access to The Guardian is Armywide*, officials say, Monterey Herald.
5. EVEN MacAskill, Julian Borger, Nick Hopkins, Nick Davies, James Ball, *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian (21 юни 2013).
6. KUPTSOVA Maria, *The NSA collects data on 5 billion phone calls every day*, Russian newspaper (05.12.2013).
7. MARINOV P., *Contemporary Challenges for the Management of the security and counter-terrorism system*, East-West, Sofia 2016, ISBN 978-619--01-0027-0.
8. MARINOV P., *Terrorism – Abstractions and Realities*, East-West, Sofia, 2016, ISBN 619152866-3.
9. MILUSHEV L., *Preparation of the governing bodies and the crisis response forces - a significant resource for crisis protection*, First National Scientific Practical Conference on Emergency Management and Protection of the Population, Sofia, BAS, 2005, ISBN 10: 954-91827-1-1, ISBN 13: 978-954-91827-1-2.
10. MILUSHEV L., *Social Aspects of Crime, MNC "Security in Southeast Europe*, *Crises, Challenges, Policies"*, Sofia, 2011, Proceedings, Demax, ISBN: 978-954-479- 038-7.