Confidentiality of Communications: What it Covers according to the Russian Judicial Practice

Nikita Danilov

Senior Lecturer, Law Faculty, National Research University Higher School of Economics, Candidate of Juridical Sciences. Address: 20 Myasnitsky Str., Moscow 101000, Russian Federation. E-mail: ndanilov@hse.ru

Abstract

Analysis of confidentiality of communications in Russian judicial practice.

Keywords

citizens, correspondence, service, rights and freedoms, offence, liability, the Constitutional Court, the Supreme Court.

For citation: Danilov N.A. (2020) Confidentiality of Communications: What it Covers according to the Russian Judicial Practice // *Legal Issues in the Digital Era,* no 2, pp. 163–172.

DOI: 10.17323/2713-2749.2020.2.163.172

At the legislative level, the concept of confidentiality of communications and what it covers are defined in the Constitution of the Russian Federation and the Federal Law "On communications".

According to Article 23 of the Constitution of the Russian Federation, everyone has the right to the inviolability of private life, personal and family confidentiality and to protection of their honor and good name. Everyone has the right to confidentiality of correspondence, telephone conversations, postal, telegraph and other communications. Restriction of this right is permissible only on the basis of a court order.

Paragraph 1 of Article 63 of the Federal Law "On communications" also provides that the confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication and postal networks is guaranteed within the territory of the Russian Federation.

A literal interpretation of these provisions would conclude that the lawmakers initially regarded the content of communications as confidential. This is certainly very sensitive information, as people obviously do not want the content of their telephone conversations, short text messages or emails to be made public, or the content of communications to be accessed by third parties. Violation of the confidentiality of correspondence is a significant infringement of the rights and freedoms of citizens.

However, Russian judicial practice has applied a broader interpretation of the concept and coverage of confidentiality of communications.

According to the ruling of the Constitutional Court of the Russian Federation dated 2 October 2003 No. 345-O "Concerning declining to consider the inquiry of the Soviet district court of Lipetsk concerning confirmation of the constitutionality of paragraph four of Article 32 of the Federal Law dated 16 February 1995 'On communications'", the right of each person to confidentiality of phone calls in its constitutional sense implies a set of actions for the protection of information received via a communication channel, regardless of the time of receipt, or the extent and content of the information recorded at separate stages of its implementation. For this reason, any information transmitted, stored and established by telephone equipment, including data on incoming and outgoing signals of connection between telephone devices of specific users of communications is considered information that is subject to the confidentiality of telephone conversations protected by the Constitution of the Russian Federation and laws in force within the Russian Federation. In order to access this information, bodies engaged in operational search activities must obtain a court order. Otherwise, this would fail to comply with the requirement in Article 23(2) of the Constitution of the Russian Federation concerning the permissibility of restricting the right to confidentiality of telephone conversations only on the basis of a court order.

This decision of the Constitutional Court of the Russian Federation was largely dispositive in the development of subsequent judicial practice. It was consequential not so much in that it attributed confidentiality of communications to data about the incoming and outgoing signals of telephone connections, which are in fact details about calls (information on the date and time of calls made, data identifying call recipients and callers, and the duration of connections), but rather because the decision applied confidentiality of communications to any information transmitted, stored and provided using telephone equipment. This interpretation subsequently led courts of

general jurisdiction and arbitration courts to apply confidentiality of communications to any information, even of a technical kind, that is used in a communication network when making telephone calls or when subscribers use telecommunication services and data transmission services. This includes, for example, the IMSI number, IMEI, and other information.

That interpretation hinders the development of modern telecommunication services. For example, information about changes in an IMSI number (the unique identification code of a SIM card) can be used as part of information exchange between telecom operators and banks in order to counter fraud. There are instances in which hackers have used fraudulent powers of attorney to create duplicate SIM cards that are "linked" to bank accounts. Then the attackers used the duplicates to illegally debit money from the bank account of a bona fide person. Furthermore, telecom operators track information about the IMSI numbers used by the subscribers on their network. If this number changes, it is a signal potentially flagging an illegal modification of a SIM card, and this information can be transmitted by the operator to a bank for additional authorization when performing a banking operation. However, due to the classification of IMSI numbers as confidential communication which can only be disclosed on the basis of a court order, these verification practices fall into a "gray" legal zone.

This position of the Constitutional Court of the Russian Federation was reflected in some of its subsequent decisions, for example, in the ruling dated 21 October 2008 No. 528-O-O "On declining to accept the plea of Alexander Mullin concerning violation of his constitutional rights under the provisions of Article 9 of the Federal Law 'On information, information technologies and information protection' and Article 53 of the Federal Law 'On communications'".

The position of the Supreme Court of the Russian Federation also merits study. As noted in the review of judicial practice by the Supreme Court of the Russian Federation entitled "Review of judicial practice in criminal cases of crimes related to illicit trafficking in narcotic drugs, psychotropic, potent and toxic substances" (approved by the Presidium of the Supreme Court of the Russian Federation on 27 June 2012), information that is protected by the Constitution of the Russian Federation and laws in force within the Russian Federation is considered to be any information transmitted, stored and provided using telephone equipment, including data on incoming and outgoing connection signals of the telephone apparatuses of specific users of communications. In order to access this information, the authorities en-

gaged in search operations must obtain a court order. Otherwise, a search would fail to comply with the requirement of Article 23(2) of the Constitution of the Russian Federation that restricting the right to confidentiality of telephone conversations is permissible only on the basis of a court order. Hence, it is necessary to obtain a court decision to locate a telephone apparatus relative to a base station, as well as to identify subscriber devices of persons of interest in a search because obtaining that information is an invasion of privacy and entails restriction of the constitutional rights of citizens to the confidentiality of telephone conversations.

Therefore, this decision of the Supreme Court of the Russian Federation applies not only to the confidentiality of communications but also of information about the location of a subscriber's device.

Certainly, information about the location of a subscriber's device is quite important and sensitive information from the point of view of citizens' rights. It is unlikely that we want third parties to know about our location at a certain time and place. However, geolocation data can be processed anonymously in a data array. For example, at 13:00 in the vicinity of 7 Tverskaya Street there were 700 young people aged 18 to 35 years. This information is of commercial value because it could perhaps be used to make decisions about opening retail stores. That kind of information is completely depersonalized in that it does not directly or indirectly identify persons and does not indicate the location of a particular person. But there is a risk that regarding access to such information as restricted will interfere with providing services through Big Data analytics.

These decisions of the Constitutional Court and the Supreme Court of the Russian Federation have also influenced the practice of arbitration courts and courts of general jurisdiction.

For example, the decision of the Moscow Arbitration Court (decision dated 8 June 2015 in case No. A40-76979/2015) found the MTS (Mobile TeleSystems) service guilty of committing an administrative offense, liability for which is provided by paragraph 3 of Article 14.1 of the Administrative Code and punishable by an administrative fine in the amount of 30,000 rubles.

The materials in the case indicate that on 9 December 2010 a contract for the provision of communication services was concluded between a person identified by the initial 'S' and the telecom operator MTS OJSC (open joint stock company). In accordance with this agreement, MTS was assigned a subscriber number for the purpose of providing mobile radiotelephone services to subscriber S.

A credit card agreement and a debit card agreement were signed between subscriber S. and Tinkoff Credit Systems Bank CJSC (closed joint stock company). Subscriber S. provided the subscriber number (with first four digits 7915) as the main contact number for informational and financial interactions with the bank in the course of providing remote services under the specified agreements.

On the basis of clause 4.2 of the terms applicable to comprehensive banking services at Tinkoff Credit Systems Bank, the court established that the bank under the Universal Agreement for remote services provides information to its client by sending that information via the client's contact details as stated on the application form.

Subscriber S. received a message from Tinkoff Credit Systems Bank to the effect that sending passwords to the subscriber number beginning with 7915 was blocked due to replacement of the SIM card. In response to a request that subscriber S. sent by e-mail to Tinkoff Credit Systems Bank, the bank's customer service department explained that the block was imposed for security reasons and also indicated that the bank had tried to verify the link of the IMSI to the mobile phone number. When the bank sends messages to a subscriber, the IMSI is linked to the mobile phone number contact. If the SIM card is replaced (without changing the phone number), the IMSI changes. As a result, the bank's system will not automatically reestablish the link, and the subscriber must reset the IMSI binding in order to have the services to work as expected.

As the court noted in its decision, in accordance with the international standardization recommended by ITU-T E. 212, an international mobile subscriber identification number (IMSI or International Mobile Subscriber Identity) is a sequence of decimal digits, not to exceed 15 digits, that identifies a single subscriber. The IMSI is contained in the operator's database, stored on the subscriber's SIM card and, for the purpose of identifying the subscriber, is transmitted over the telecommunication network from the subscriber station to the receiving equipment of the operator when the subscriber is initialized in the network.

Subscriber S. did not provide information about the IMSI value of his SIM card to the bank, and the contract for the provision of communication services between MTS and subscriber S. does not specify the value of this identifier.

In response to the request, a representative of Tinkoff Credit Systems Bank confirmed that in the course of providing services to customers, the

bank uses verification of the link between the IMSI number located in the SIM card memory and the customer's subscriber number in order to identify a customer. The bank further explained that the IMSI is provided to the bank by the mobile telecommunications operator after the ID is transmitted by the mobile communication device during registration in the network.

In the explanation provided to Roskomnadzor, MTS denied that it had provided information about the IMSI value of the SIM card of subscriber S. to Tinkoff Credit Systems Bank.

According to Roskomnadzor, these actions by MTS constituted an administrative offense, liability for which is established in paragraph 3 of Article 14.1 of the Administrative Code of the Russian Federation (which covers conduct of business activities in violation of the conditions applicable to a special permit or license).

In accordance with Article 23.1 of the Administrative Code of the Russian Federation, Roskomnadzor filed a statement in arbitration court to the effect that MTS should be held liable for an administrative offense under paragraph 3 of Article 14.1 of the Administrative Code. The company was in fact held liable.

MTS appealed the decision, but the court of appeals upheld the legality of the administrative liability.

The court noted in its decision that, on the basis of paragraph 1 of Article 63 of the Federal Law "On communications", the confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication networks and postal networks is guaranteed within the Russian Federation. Restriction of that right to confidentiality is permissible only as stipulated by federal laws.

In accordance with the national standard of the Russian Federation GOST R 53801-2010 "Federal communications: Terms and definitions", a telecommunication message is any information transmitted by means of telecommunications.

Hence, the court found that an IMSI belongs to the category of messages transmitted over telecommunication networks, and as such it is subject to the requirements of the legislation of the Russian Federation which ensure confidentiality of communications. Paragraph 2 of Article 63 of the Federal law "On communications" stipulates that the operator must ensure the confidentiality of communications when providing services.

As follows from the materials of another case (decision of the Ninth Arbitration Court of Appeals dated 28.03.2014 N 09AP-1573/2014 in case N

A40-145794/13), the unique IMEI number which identifies an apparatus also constitutes information that is subject to confidentiality of communications.

MTS sued in arbitration court to have a decision of the Bank of Russia's financial markets service declared illegal and to rescind liability of MTS for an administrative violation under paragraph 9 of Article 15.9 of the Administrative Code of the Russian Federation, which stipulates a fine of 500,000 rubles as penalty.

The case establishes that, in the course of conducting a desk audit to investigate possible misuse of insider information and market manipulation, the Federal Service for Financial Markets (FSFM) asked MTS to provide the following information:

All information listed in paragraph 1 of Article 53 of the Federal law "On communications" concerning all users of communication services who were allocated a subscriber number beginning with +7(985)386.... The information was to include the period of use of this number by each of the users of communication services and the IMEI of the terminal equipment used in each period. Copies of documents confirming the information provided, including contracts, agreements, and customer profiles as well as changes and additions to these documents were also to be provided;

Information about whether communication services were provided to the subscriber number +7(985)386... in the period from 1 January 2012 until the date of receipt of the order;

Information about other subscriber numbers used during that period by the service user who was assigned the subscriber number +7(985)386... under contracts concluded between the subscriber and MTS, specifying the subscriber numbers, dates on which contracts were concluded or terminated, and the IMEI of terminal equipment used by the subscriber;

Details of the subscriber's invoices for the period in electronic form using the MS Excel format on optical media.

MTS provided the information and documents requested by order of the Federal Service for Financial Markets with the exception of the identification numbers of subscriber devices (IMEI) and information about the details of subscriber accounts for the period in MS Excel on optical media.

The FSFM charged MTS with an administrative offence on grounds of refusal to provide information.

Subsequently, the Bank of Russia's financial markets service under the Central Bank of the Russian Federation issued a decision to the effect that,

under paragraph 9 of Article 19.5 of the Administrative Code of the Russian Federation, MTS was subject to administrative liability in the form of a fine of 500,000 rubles.

In finding MTS liable under paragraph 9 of Article 19.5 of the Administrative Code of the Russian Federation, the Bank of Russia reasoned that MTS had violated Article 16(1) of the insider trading law and article 11(1) of the law concerning protection of investors' rights.

According to legislation on countering insider information (in the version that was in effect at that time), legal entities are required to submit documents, explanations, and information in written and oral form, including commercial, official, and banking information subject to confidentiality.

MTS alluded to these circumstances as the basis for its appeal to the court concerning the above requirements.

The court sided with MTS.

As the court noted in its decision, the details of the subscriber's account contain information about the mobile communication services provided, indicating the date and time of all connections, their duration and subscriber numbers.

Hence, the subscriber account details represent data on incoming and outgoing connection signals of the telephone sets of specific communication users.

Information contained in the subscriber's account details, including data on incoming and outgoing connection signals of telephone apparatuses of specific communication users, is stored and set by the communication operator using only telephone equipment.

In addition, the identification number of the subscriber's IMEI device is not required by the terms of the mobile service agreement, and therefore it cannot be established based on the provisions of contracts concluded with subscribers.

When concluding mobile communication service contracts with subscribers, the operator provides them with subscriber identification modules (SIM cards) where the subscriber number is recorded, but the operator does not provide the telephone apparatus. Subscriber devices are purchased by the subscriber independently in a retail network, which sells them without requiring an identity document, and therefore the IMEI code of the subscriber device is not directly linked to either the telecom operator or to the subscriber himself.

At the same time, the subscriber has the right to use any subscriber devices, and the telecom operator is not obliged to maintain a database containing information about these devices.

Information about the identification numbers of subscriber IMEI devices is "registered" (set) by the communication equipment only during telephone connections; that is, it is contained only in the connection protocols (details) of specific subscribers whose SIM cards were used in a particular telephone device.

Given the above, as noted in the court decision, it was justifiable to find with the court of first instance that information about the IMEI identification numbers of subscriber devices also represents information transmitted, stored and installed using telephone equipment, and it therefore falls under the confidentiality of telephone conversations.

In accordance with Article 63 of the Federal Law "On communications", the confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication and postal networks is guaranteed within the Russian Federation.

Restriction of the right to confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication and postal networks is permitted only as stipulated by federal laws. Telecom operators are required to ensure the confidentiality of communications.

This right is guaranteed by the aforementioned Article 23 of the Constitution of the Russian Federation.

In light of the above and the previously mentioned legal position of the Constitutional Court of the Russian Federation, set out in the definitions dated 2 October 2003 N 345-O and 21 October 2008 N 528-O-O, information subject to the confidentiality of telephone conversations includes any information transmitted, stored and installed using telephone equipment, including data on incoming and outgoing connection signals of telephone devices of specific communication users; and to access this information it is necessary to obtain a court order.

The court of appeals, in accordance with the rules pertaining to the nature of the information (data) requested by the administrative authority, held that the billing details of a specific subscriber and information about the identification numbers of subscriber devices (IMEI) are subject to confidentiality of communications, inasmuch as those details consist not only of the information contained in the telephone connection (conversations), but also data on the connections between individual subscribers (date, time, duration), and any other information transmitted, stored, and installed with communications equipment.

The information withheld by MTS was subject to the confidentiality of communications and therefore should not have been provided upon request to the administrative body.

In this case, the court of first instance rightly alluded to the response of the Ministry of Communications and the letter of Roskomnadzor, which explained that the account details specific to a caller and data about the identification numbers of their subscriber devices (IMEI, IMSI) are protected by the Constitution of the Russian Federation as confidential interactions by telephone.

In view of the above circumstances, the court rightly upheld the conclusion of the court of first instance that the refusal of MTS to provide such information to the FSFM does not constitute sufficient proof of an offense as specified by paragraph 9 of Article 19,5 of the Administrative Code. That conclusion was the basis for a declaring that the decision to subject MTS to administrative liability is unlawful and void.

The judicial practices outlined above show that the concept of confidentiality of communications is interpreted very broadly by the courts. In addition to the content of interactions, confidentiality of communications extends to geolocation, call details, and technical information transmitted over communication networks (IMSI, IMEI). The classification of technical information as a confidential communication is questionable because processing that information does not affect the rights and freedoms of citizens, and it does not violate the right to privacy in any way.