PalArch's Journal of Archaeology of Egypt / Egyptology

COMMUNICATION PRIVACY RESTRICTIONS DURING THE COVID-19 PANDEMIC

Anzhelika N. Izotova[1]

[1]Department of Information Law of the National Research University Higher School of Economics, Leading legal advisor of PJSC Mobile TeleSystems

[1]anzheliki@rambler.ru

Anzhelika N. Izotova. Communication Privacy Restrictions During The Covid-19 Pandemic--- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(10), 1849-1861. ISSN 1567-214x

Key Words. Communication Privacy, Eprivacy, Confidentiality, Privacy, Electronic Communications, Restriction Of Rights, Covid.

ABSTRACT

The work is devoted to the issues of restricting the privacy of communication which is an integral part of privacy, a necessary condition for freedom of speech and for trust in communication services, and is crucial for the development of the information society. In the context of the pandemic, it became possible to restrict the confidentiality of communication in the context of geolocating people through their mobile devices based on data from mobile operators. Therefore, it is important to note the essential conditions for restricting the right to privacy of communication in order to avoid unjustified violation of universally recognized fundamental human rights.

The work discusses the issue of geolocating a person via their mobile phone, as well as legal regulation and judicial practice regarding the restriction of the right to privacy of communication in Europe and Russia. Anonymization as a necessary condition for processing personal data, including the privacy of communication, is also considered.

The methodological basis of the study comprised dialectical, formal-legal, comparative methods, induction and analysis method.

As a result, conclusions were drawn on the similarity of the legal regulation of the privacy of communication in Europe and Russia, on the possibility of restricting the right to privacy of communication at the legislative level, subject to the principles of proportionality, necessity and temporary nature of such restrictions caused by the pandemic, as well as on the legality

of processing communication data (data on the location of users of communication services) on condition of anonymity, provided that it is impossible to deanonymize the data.

INTRODUCTION

Issues of the legitimate use of information of limited access, including personal information of citizens, increasingly arise in the context of the development of digital law and digital society.

Government agencies, faced with the COVID-19 pandemic, were forced to urgently develop measures to prevent the spread of the virus. In the fight against a pandemic, it is important for state governments to understand the full picture of what is happening and to have possible scenarios for the development of threats, and for the population to follow the measures taken to prevent the spread of infection. In light of this, location data are particularly attractive and can be of significant benefit.

The right to privacy of communication is regarded as an integral part of the institution of privacy and is designed to ensure the autonomy of a person and their freedom from any encroachment and interference from outside. However, we all understand that it is impossible to live in society and remain completely free from it[1]. Such restriction of constitutional rights can be called a manifestation of solidarity which allows for the cohabitation of people in society. However, when restricting constitutional rights, it is necessary to proceed from the principles of proportionality and of the need for restrictions, which is difficult to implement and requires effective control[2].

Location of the user of communication services

Representatives of various states suggested geolocating their citizens based on data from mobile operators – the Minister of Health of Germany, the British government and others. These ideas did not find support, since tracking cell phones leads to an extensive violation of the fundamental rights of citizens.

The location data of the mobile device have a comprehensive legal regime. On the one hand, they can be qualified as personal data and also, when it comes to the provision of communication services, as traffic data (communication messages) and must be protected as part of the confidentiality of communication.

The Charter of Fundamental Rights of the European Union (Article 8), the Convention for the Protection of Human Rights and Fundamental Freedoms, and the Constitutions of the EU Member States have proclaimed and guarantee the confidentiality of electronic communications. Directive 2002/58/EU of the European Parliament and of the Council of the European Union "Concerning the processing of personal data and the protection of privacy in the electronic communication sector (Directive on privacy and

---

[1] Avdeev M.Yu. Legislation of the Russian Federation on privacy: on the issue of borrowing foreign experience // Eurasian Bar. 2013. No2 (3).

[2] Nesmeyanova S.E., Kolobaeva N.E. Constitutional restriction of fundamental human rights and freedoms // Russian Law: Education. Practice. Science. 2018. 3: 9-16.

electronic communication, hereinafter – the ePrivacy Directive)[3] respects and protects the rights of electronic communication privacy. According to the ePrivacy Directive, national legal acts of the member states, as well as the practice of the European courts, traffic data, including data on the location of the telephone, are classified as electronic communication privacy.

The ePrivacy Directive defines traffic data as data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. 'Location data' means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

The European Union laws, for the most part adopted before the advent of the ePrivacy Directive, follow a similar approach. As follows from Point 1, Paragraph 88 of the Law on Telecommunications (Telekommunikationsgesetz, TKG)[4] dated 06.22.2004, the information constituting a privacy of communication includes the content of correspondence, telephone conversations and other messages, as well as data on the fact of a person's participation in telephone conversations, as well as data obtained in the process of correspondence or sending messages[5]. The same is indicated in Articles 102, 105 of the Electronic Communication Act of Estonia [6]. The inclusion of data in the concept of communication privacy is also disclosed in a number of countries at the level of judicial practice. In Spain, the courts apply the principle of confidentiality to all aspects of communication that are not obvious to third parties[7].

In Russia, the concept of communication privacy is formed by judicial practice. As in the European Union, in Russia everyone is guaranteed the constitutional right to privacy of correspondence, telephone calls, telegraphic and other communication – the right to privacy of communication (Part 2, Article 23 of the Constitution of the Russian Federation). The Constitutional

---

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (Directive on privacy and electronic communications). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219 (Accessed 20 May 2020).

[4] Telekommunikationsgesetz vom 22. Juni 2004 (BGBI. I S.1190). Available at: https://www.gesetze-im-internet.de/tkg_2004 (Accessed 25 May 2020).

[5] Schaller, C. (2018). Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden. German Law Journal, 19(4), 941-980. Available at: https://www.cambridge.org/core/journals/german-law-journal/article/strategic-surveillance-and-extraterritorial-basic-rights-protection-german-intelligence-law-after-snowden/494F82EE78DCF2709B07A2B57D95454C (Accessed 07.06.2020).

[6] Electronic communication Act. Available at: https://www.riigiteataja.ee/en/eli/501042015003/consolide (Accessed 10.06.2020).

[7] Urgell A.M. Analisis juriprudenceial del derecho al secreto de las comunicaciones (art. 18.3 C.E.) [Electronic resource] // Diposit de la Recerca de Catalunya [Site]. – Available at: https://www.recercat.cat/bitstream/handle/2072/9115/treballrecerca.pdf;jsessionid=C6A2AE06E8DA7C4B7A127B7D6F2BE9A6.recercat1?sequence=1. – P. 56 (Accessed 31.05.2020).

Court of Russia[8] and then the Supreme Court of Russia[9] indicated that communications privacy includes any information transmitted, stored and established using telephone equipment, including data on incoming and outgoing connection signals from telephone sets of specific communication users (including data on the location of the subscriber).
In sum, the location data is protected within the confidentiality of communication in Europe and in Russia.

From the point of view of scientists, the feasibility of such approach was repeatedly studied, and various points of view were expressed.

Opinions are expressed when the feasibility of referring traffic data to communication privacy is being questioned, based on lower significance of such information for the subscriber in comparison with the content of transmitted messages. However, one can agree with this point of view only partially, for example, regarding technical identifiers of subscriber equipment.

The predominant is the opposite point of view. As the Advocate General of the European Court of Justice notes, traffic data are «in a sense more than personal». Traffic data are «special personal data, the use of which may make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity». Mobile devices basically function as location tracking devices, and communications metadata over longer periods can allow for a detailed mapping of an individual's social, professional, and private life, revealing many sensitive details[10]. Moreover, given the value of the location data of a person, regardless of the situation in which they were obtained (when providing communication services or when using a website or mobile application), and also taking into account the identity of publicly available communication services and other communication services (instant messengers, social networks, etc.) it is proposed to extend the protective measures of legal regulation of the confidentiality of communication to all data on the person's location[11].
In addition to the threat to human interests in terms of confidentiality, there is also a threat to freedom of expression. The behavior, as well as the statements of a person, can be different depending on whether someone is watching them or not. That is, the threat of observation itself limits freedom of communication. The same can be said about freedom of movement in the context of tracking a person's location. Knowing they are being watched, a person may limit their freedom of movement, fearing negative consequences

---

[8] Determination of the Constitutional Court of Russia No.345-O, 02.10.2003. Available at: https://legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-02102003-n-345-o-ob/(Accessed 27.05.2020).
[9] Resolution of the Plenum of the Supreme Court of the Russian Federation of June 01, 2017 No. 19 "On the practice of consideration by courts of applications for investigative actions related to the restriction of constitutional rights of citizens (Article 165 of the Code of Criminal Procedure of the Russian Federation)" https://rg.ru/2017/06/09 /hodataistva-dok.html, Resolution of the Plenum of the Supreme Court of the Russian Federation No. 46 dated 12/25/2018, "On Certain Issues of Judicial Practice in Cases of Crimes Against the Constitutional Rights and Freedoms of Man and Citizen (Articles 137, 138, 138.1, 139, 144, 1, 145, 145.1 of the Criminal Code) "https://www.vsrf.ru/documents/own/27537/.
[10] Joris van Hoboken and Frederik Zuiderveen Borgesius, Scoping Electronic Communication Privacy Rules: Data, Services and Values, 6 (2015) JIPITEC 198, para 1. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777156 (Accessed 07.06.2020).
[11] Ibid.

or public censure. Yet in the context of the COVID-19 pandemic, the goal of such monitoring is partly to control and prevent the spread of infection.

European Union

From the point of view of confidentiality of communication, European legislation has numerous tools that impede or restrict the use of data from mobile operators.

The ePrivacy Directive says it is possible to process data on the location of subscriber equipment with the consent of the user of publicly available communication services. This stems from the essence of the natural right to privacy and the human right to exercise control over their data[12].

At the same time, given the prevalence of the COVID-19 pandemic, it is not possible to rely on collecting such consents. In emergency situations, governments are required to take decisive and operational measures to prevent the spread of infection and reduce the negative effect of its consequences. As a rule, the Constitutions of the states and the International Conventions are developed taking into account such crises or emergency situations[13].

The Convention for the Protection of Fundamental Rights and Freedoms, together with the national legislation of the EU member states, establishes strict rules for restricting the right to privacy of electronic communications. According to Point 2, Article 8 of the Convention, interference with the right to respect for correspondence is allowed in order to protect national security and public order, the economic well-being of the country, prevent disorder and crime, protect health or morality, protect the rights and freedoms of others. The European Court jointly with the legislator proceeds from the fact that the rights and freedoms guaranteed by the Convention are subject only to the restrictions that are expressly provided for in it. Accepted restrictions on the right to confidentiality of correspondence should be strictly contextual in nature. In terms of human location data, these can be very useful for epidemiological analysis during the COVID-19 pandemic. At the same time, in the context of a political crisis, the same location data may threaten the rule of law, democracy and the enjoyment of human rights[14].

The European Commission on Human Rights developed the concept of "inherent limitations", which do not require justification for the purposes stipulated by the Convention but are inherent in the situation in which the law is implemented or limited. This is also the best fit for the pandemic situation,

[12] Post, R.C. (2018) Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. Duke Law Journal, February. Available at: http://dx.doi.org/10.2139/ssrn.2953468. (Accessed 02.06.2020).

[13] Zwitter, A., Gstrein, O.J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Journal of International Humanitarian Action 5, 4 (2020). Available at: https://www.researchgate.net/publication/341476623_Big_data_privacy_and_COVID-19_-_learning_from_humanitarian_expertise_in_data_protection (Accessed 05.06.2020).

[14] Zwitter, A., Gstrein, O.J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Journal of International Humanitarian Action 5, 4 (2020). Available at: https://www.researchgate.net/publication/341476623_Big_data_privacy_and_COVID-19_-_learning_from_humanitarian_expertise_in_data_protection (Accessed 05.06.2020).

when, on the one hand, respect for correspondence and personal privacy, and on the other hand, protecting the health of the population are at stake.

The German Constitution (Article 10)[15] speaks of the inviolability of the privacy of communication and the admissibility of restrictions only on the basis of law. Moreover, certain laws establish a mandatory requirement for a court decision [16]. The Declaration of Human Rights and the Citizen of France [17], Paragraph 4, also speaks of the restriction of natural human rights only on the basis of law. The Constitution of Spain[18] (Article 18) provides for the limitation of privacy of communication on the basis of a court decision, as well as in certain cases established by law (for law enforcement and anti-terrorism purposes). A very similar legal situation exists in other EU countries.

In other words, the legislation of the EU countries to limit the right to confidentiality of communication requires a special law to limit such right for the purposes expressly specified in the legislation.

As demonstrated by the Tele2 Sverige AB v Post-och telestyrelsen case or by Secretary of State for the Home Department v Watson and others (C-203/15 and C-698/15)[19], in accordance with Art. 15 (1) of the ePrivacy Directive, Member States of the European Union are entitled to take legislative measures to limit the rights and obligations provided for in certain articles of the Directive, if such restriction is a necessary, appropriate and proportionate measure within a democratic society to protect national (state) security, defense and public safety, and to prevent, investigate, detect and prosecute criminal acts or the unauthorized use of electronic communications systems. The European Court of Human Rights considers such principles necessary in a democratic society, and public authorities must provide appropriate and sufficient justification for establishing restrictions[20].

In connection with the issue of restricting the right to communication confidentiality, one can recall the previously valid Data Storage Directive 2006/24/EU [21], which obliged telecom operators to keep a significant list of data relating to privacy of communication. However, in 2014, the European Court ruled that the Directive was invalid, since the implementation of its provisions led to serious interference with the rights to privacy and the confidentiality of communication. The Court of Justice of the European Union

---

[15] **Grundgesetz für die Bundesrepublik Deutschland. Available at: https://www.gesetze-im-internet.de/gg/ (Accessed 27 May 2020).**

[16] **См.: §23a Zollfahndungsdienstgesetz от 16.08.2002, §305a Versicherungsaufsichtsgesetz от 01.04.2015 и др. Available at: https://www.gesetze-im-internet.de (Accessed 22 May 2020).**

[17] **Déclaration des Droits de l'Homme et du Citoyen de 1789. Available at: https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789 (Accessed 25 May 2020).**

[18] **Constitución Española. Available at: https://app.congreso.es/consti/constitucion/indice/index.htm (Accessed 25 May 2020).**

[19] **Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others [Electronic resource] : Judgment of the European court of justice (Grand Chamber) dated December 21, 2016 (Joined Cases C-203/15 and C-698/15) // The Court Of Justice Of The European Union [Site]. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=26020 (Accessed 22 May 2020).**

[20] **Brunner, L. (2018) Digital Communications and the Evolving Right to Privacy. Cambridge University Press. New technologies for Human Rights Law and Practice. In Land, M., Aronson, J. (Eds.). Available at: https://doi.org/10.1017/9781316838952.010 (Accessed 27 May 2020).**

[21] **Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024 (Accessed 02.04.2020).**

also found that interfering with communication privacy is disproportionate to the objectives of the Directive. However, the scientific community believes that the storage of data on electronic messages can take place, but legal regulation should (in addition to the main goal of ensuring the security of the state) guarantee privacy, including by monitoring interference with communication privacy[22]. In fact, in Russia in 2018, legal regulations [23] on the storage of communication data by telecom operators and organizers of messaging services (instant messengers, email services, etc.) entered into force. Such data shall be provided in cases established by laws in response to requests from law enforcement agencies based on a court decision. Thus, the Russian legislator tried to maintain a balance of interests between guaranteeing confidentiality of specific users and ensuring security in the country.

Returning to the topic of geolocating people according to the data of mobile operators, it should be noted that in practice the states of the European Union did not take the path of limiting the right to privacy of electronic messages even in the context of the COVID-19 pandemic. Moreover, Europe is actively discussing the application of restrictive measures in the context of the inadmissibility of authoritarian governments abusing power[24].

Instead, special mobile applications were developed that the user installs on their mobile phone and agrees to the processing of their whereabouts and other personal data, if necessary. Formally, data obtained this way does not fall under the definition of traffic data. Such data is not the data of the communication network in the provision of publicly available communication services and is received not from the mobile operator but from the owner of the mobile application. Although, as noted earlier, in science there is an opinion about the identity of the legal nature of such data and the need to harmonize their legal regulation, regardless of who collected these data and which technologies were used. At the same time, in the existing legal realities, cell phone geolocation data in this case is the personal data of the user of the mobile application, which is already regulated by the General Data Protection Regulation (GDPR)[25] and the consent of the personal data subject is sufficient to process such data. At the same time, in particular, the British government made a statement that installing the application is purely voluntary.

Data on the location of subscriber equipment in the context of the confidentiality of electronic messages is also used for humanitarian purposes. Thus, the German communications operator Deutsche Telecom organized an interaction with the Robert Koch Institute (which deals with infectious diseases and is one of the main institutions where information about the

---

[22] Drewry, L. (2016) Crime without culprits: why the European Union needs Data protection, and How it can be balanced with the right to privacy. Wisconsin International Law Journal, Spring. Available at: https://wilj.law.wisc.edu/issues/ (Accessed 02.03.2020).

[23] Federal Law of 06.07.2016 No. 374-FL "On Amending the Federal Law" On Countering Terrorism "and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public safety". Available at: http://www.kremlin.ru/acts/bank/41108 (Accessed 15.05.2020).

[24] Deutscher Bundestag Stenografischer Bericht 161. Sitzung Berlin, Freitag, den 15. Mai 2020. Available at: http://dipbt.bundestag.de/dip21/btp/19/19161.pdf#P.20001 (Accessed 17 June 2020).

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Accessed 17 June 2020).

coronavirus is gathered) to provide data on the movement of the country's population in the form of 'heat maps'[26]. A similar interaction is established between the French telecom operator Orange and the French national institute of health Inserm[27]. The location data of mobile devices were anonymized and aggregated, which seems to be a sufficient condition for processing such data without violating the right to privacy of communication.

Communication confidentiality as one of the basic human rights and an integral part of privacy is directly related to the personality of a particular citizen. It is logical to assume that excluding the possibility of identifying a person will allow processing communication data by analogy with the processing of anonymized personal data according to the GDPR. At the same time, data anonymization is an ambiguous data processing tool; this is largely due to the degree of possibility of deanonymization, which can negate all actions to anonymize data and to prevent violations of the right to privacy of communication. It is possible to say that data anonymization is discredited, because usually there is some external information that, after combining with anonymous data, allows identifying a person. Recent studies reveal that the combination of a huge amount of data (including personal data) and the improvement of their processing methods make data anonymization meaningless. On the other hand, anonymized and aggregated data, as in the example with heat maps, without the possibility of deanonymizing them and reconnecting with a specific person (on the condition this is still possible) are very valuable, especially from a humanitarian point of view. Certainly, the more anonymous the data, the less valuable they are[28], but interference in privacy, including the privacy of communication, should not be limited to a greater extent than is necessary to solve a specific data processing problem.

Russia

The Russian government was no exception and instructed the Ministry of Digital Development, Telecommunications and Mass Media of Russia to organize the creation of a tracking system for citizens in contact with patients with the new coronavirus infection, based on information from mobile operators about the location of a specific person's cell phone[29].

Moreover, the Prime Minister of the Russian Federation noted that with the help of telecom operators, it is planned to monitor whether the arrived citizen are in quarantine. In case of non-compliance with the conditions of self-isolation, operators must transmit information to law enforcement agencies[30].

---

[26] Deutsche Telekom überlässt Robert Koch-Institut Bewegungsprofile von Nutzern. Available at: https://deutsch.rt.com/inland/99427-deutsche-telekom-ueberlasst-robert-koch/ (Accessed 11 June 2020).

[27] Les statistiques issues du réseau de téléphonies mobiles au service de la lutte contre la pandémie de Covid-19. Available at: https://presse.inserm.fr/les-donnees-des-telephones-mobiles-au-service-de-la-lutte-contre-la-pandemie-de-covid-19/38831/ (Accessed 11 June 2020).

[28] Paul Ohm. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review, Vol. 57, p. 1701, 2010. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (Accessed 02.05.2020).

[29] On decisions following a meeting of the Presidium of the Coordination Council under the Government of the Russian Federation to combat the spread of new coronavirus infection. Available at: http://government.ru/orders/selection/401/39243/ (Accessed 30.04.2020).

[30] The meeting of the Presidium of the Coordinating Council under the Government to combat the spread of new coronavirus infection in the territory of the Russian Federation. Available at: http://government.ru/news/39327/ (Accessed 30.04.2020).

Under ordinary conditions, the rights and freedoms of man and citizen are a “limiter of state power”[31]. Yet, given the global scale of the COVID-19 threat and the danger of its consequences for humans, the restriction of the right to privacy of communication arising from the said order of the Government of the Russian Federation could be considered justified.

The above-mentioned order of the Government of the Russian Federation once again demonstrates (in the context of the spread of COVID-19) the issue of competition between the constitutional rights of citizens to privacy and communication privacy, enshrined in Art. 23 of the Constitution of the Russian Federation, and to health which is also a natural right and is enshrined in Article 41 of the Constitution.

At the same time, one cannot but take into account the procedure laid down in the Constitution of Russia for restricting the right to privacy of communication, similar to European standards. Thus, Part 2 of Article 23 speaks about the restriction of this right only based on a court decision. Additionally, Art. 55 of the Constitution of Russia indicates the possibility of restricting fundamental rights and freedoms, firstly, on the basis of federal law, and second, to protect the health, rights and legitimate interests of others.

Naturally, it is impossible to obtain a court decision in respect of each patient with COVID-19 or those who have contacted this patient. If it is still possible to take measures to obtain judicial acts in respect of people infected, it is not possible in respect of those who contacted them. In addition, a special law to fulfil the order of the Government of the Russian Federation on geolocating a person based on data from telecom operators was not adopted and is not planned in Russia.

The data of the telecom operator are of great value since almost everyone has a mobile phone and it is quite possible to track the location of the owner. It is enough to know the mobile phone number of the coronavirus patient in order to monitor the trajectory of this person’s movement. The telecom operator has the technical ability to receive information through the communication network about subscribers in the immediate vicinity of the infected. Yet, existing legal norms do not allow implementing the measures proposed by the Government of the Russian Federation.

Information and technological progress today opens up ambitious opportunities for transforming processes, including those at the state level [32]. The importance of data (including those that constitute privacy of communication, in particular, information about connections/messages, traffic data) is growing in the context of digitalization of society. To exercise their powers more effectively, government bodies show interest in the privacy of communication. Russian judicial practice on disputes regarding various state bodies limiting the privacy of communication shows that courts stand up for

[31] Lisina O.V. Constitutional restriction of the rights and freedoms of man and citizen: concept and limits . Bulletin of PIM. 2019. 3: 10-18.
[32] Mamitova N. V. Problems of public administration in the era of digitalization of the state and society based on ‘Soft models’ // Science and Education Today. 2019 No. 9 (44). Available at: https://cyberleninka.ru/article/n/problemy-gosudarstvennogo-upravleniya-v-epohu-tsifrovizatsii-gosudarstva-i-obschestva-na-osnove-myagkih-modeley (Accessed 14.05.2020).

the right to privacy of communication, citing the need to directly specify the law on restricting it in relation to legal sides involved in a dispute, as well as to have a court decision.

However, one cannot but pay attention to the negative experience of Russia. As noted above, Europe, when processing data on the location of a mobile phone, took the path of anonymizing and aggregating data without the possibility of deanonymizing it.

At the same time, a recent dispute between Russian mobile operators (MTS, Beeline, Megafon) and the Federal Tax Service of Russia over the refusal of telecom operators to provide tax authorities with connection details regarding specific subscriber numbers (without specifying a name of communications services user) in order to conduct a tax audit in respect of PJSC Rostelecom is noteworthy. According to Russian law, telecom operators can provide information constituting privacy of communication only to bodies engaged in operational-search activities, and the tax service does not apply to such bodies. Regarding telecom operators, the Moscow Arbitration Court ruled on disputes [33] that provoked a stormy reaction in the media. The court determined that only information (available from the telecom operator) on a particular subscriber that allows identifying them is related to the privacy of communication. Therefore, in the opinion of the court, the details of connections without indicating the name of the subscriber does not allow them to be identified and therefore is not privacy communication. The indicated position of the court is upheld in the court of appeal[34].

The author of the present work believes that such justification is controversial for the following reasons. In Russia, the judicial practice was formed earlier regarding information about subscribers who made a call, an Internet connection, etc. Thus, the Supreme Court of the Russian Federation supported the state body (antimonopoly service) which requested information from the telecom operator about the subscriber who made Internet access to a specific site at a specific time from a specific IP address, since the state body did not request information about Internet connections, but only information about the subscriber who committed them, which relates to personal data but not to communication privacy[35].

In such jurisprudence, the following situation is unacceptable from the point of view of protecting communications privacy: a state body can first send a request to a telecom operator to provide details of connections (without specifying a name), and then request information about the subscriber who made a specific call, thereby receiving fully-fledged call details of a particular subscriber, which is undoubtedly privacy communication and is recognized as such by the courts.

---

[33] **Decisions of the Moscow Arbitration Court of 01.22.2020 in case No. A40-272873 / 19-75-4881, of 01.27.2020 in case No. A40-272737 / 19-107-6590, of 06.02.2020 in case No. A40 -272978 / 19-140-6979. Available at: https://kad.arbitr.ru/ (Accessed 10.06.2020).**

[34] **Decisions of the Ninth Arbitration Court of Appeal in case No. 09AP-14822/2020 of 06/01/2020, in case No. 09AP-17966/2020 of 06/01/2020, in case No. 09AP-13430/2020 of 06/04/2020. Available at: https://kad.arbitr.ru/ (Accessed 10.06.2020).**

[35] **Decision of the Supreme Court of the Russian Federation of March 30, 2016 No. 82-AD16-1. Available at: http://www.vsrf.ru/stor_pdf.php?id=1430686 (Accessed 08.06.2020). Decision of the Supreme Court of the Russian Federation of October 11, 2016 No. 82-AD16-5. Available at: https://www.vsrf.ru/stor_pdf.php?id=1517020 (Accessed 08.06.2020).**

This example indicates negative data anonymization which does not allow speaking about guaranteed confidentiality of communication. This also confirms once again, as previously pointed out, that anonymization as a condition for processing confidential communication data is compromised and should be used very carefully.

In relation to the situation with the coronavirus infection, Russia, like Europe and other countries, introduced a mobile application to track the location of the infected person, where the data is processed with their consent, as provided for by personal data legislation.

Thus, the prerequisites for a possible restriction of the confidentiality of communication, including tracking the location of users of communication services, are laid down in the constitutional legislation of Russia. Yet for a real restriction of the right to communication privacy in Russia for the sake of health protection, one Government instruction is not enough, and it is necessary to adopt a special law regulating the procedure for such restriction of the law, and guaranteeing its proportionality. Therefore, in the current legal realities in Russia, tracking the locations of citizens in order to prevent a pandemic is impossible.

CONCLUSION

European and Russian legislation, judicial and law enforcement practice attribute traffic data for the provision of communication services (including location data of a mobile device) to communication privacy, which imposes special requirements on the processing of such data. The ePrivacy Directive, the Constitutions of the Member States of the European Union, as well as the Constitution of Russia contain a mechanism to limit the right to privacy of communication, namely by adopting a special law, including with a view to protecting the health of the country's population.

The pandemic clearly showed that guarantees of respect for human rights are very vulnerable, especially in emergency situations. Although such crises require decisive and effective measures on the part of government bodies, the measures taken should be contextual, targeted and temporary in nature due to the situation that required applying such restrictions. The exercise of powers by state bodies, including with a view to protecting the rights of others, should not occur to the detriment of fundamental human rights and freedoms and should not level the guarantees given to people. Given the mechanism (in the supreme legal acts of countries) to limit the confidentiality of communication, it is difficult to talk about the possibility of softening the data protection regimes used. Yes, monitoring the movement of citizens during a pandemic requires adopting special laws, which will be time-consuming and costly, yet at the same time, minimum guarantees for basic human rights will be respected.

In the meantime, no special laws were adopted that determine the conditions and procedure for limiting the confidentiality of communication during a pandemic'; therefore, an anonymization and aggregation tool for data from mobile operators can be used, yet with guarantees that it is impossible to deanonymize them.

As President of the European Parliament D. Sassoli noted[36], “The virus cannot stop democracy!”

REFERENCES

Brunner, L. (2018) Digital Communications and the Evolving Right to Privacy. Cambridge University Press. New technologies for Human Rights Law and Practice. In Land, M., Aronson, J. (Eds.). Available at: https://doi.org/10.1017/9781316838952.010 (Accessed 27 May 2020).

Drewry, L. (2016) Crime without culprits: why the European Union needs Data protection, and How it can be balanced with the right to privacy. Wisconsin International Law Journal, Spring. Available at: https://wilj.law.wisc.edu/issues/ (Accessed 02.03.2020).

Avdeev M.Yu. (2013). Legislation of the Russian Federation on privacy: on the issue of borrowing foreign experience // Eurasian Bar. No2 (3).

Ohm P. 2010. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review, Vol. 57, p. 1701. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (Accessed 02.05.2020).

Lisina O.V. 2019. Constitutional restriction of the rights and freedoms of man and citizen: concept and limits . Bulletin of PIM 3: 10-18.

Mamitova N. V. 2019. Problems of public administration in the era of digitalization of the state and society based on ‘Soft models’ // Science and Education Today. No. 9 (44). Available at: https://cyberleninka.ru/article/n/problemy-gosudarstvennogo-upravleniya-v-epohu-tsifrovizatsii-gosudarstva-i-obschestva-na-osnove-myagkih-modeley (Accessed 14.05.2020).

Nesmeyanova S.E., Kolobaeva N.E. 2018. Constitutional restriction of fundamental human rights and freedoms // Russian Law: Education. Practice. Science. 3: 9-16.

Post, R.C. (2018) Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. Duke Law Journal, February. Available at: http://dx.doi.org/10.2139/ssrn.2953468. (Accessed 02.06.2020).

C. Schaller. Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden, 19 German Law Journal 941. Available at: Electronic resource Nexis Uni. (Accessed 02.05.2020).

Urgell A.M. Analisis juriprudenceial del derecho al secreto de las comunicaciones (art. 18.3 C.E.) // Diposit de la Recerca de Catalunya [Site]. – Available at: https://www.recercat.cat/bitstream/handle/2072/9115/treballrecerca.pdf;jsessionid=C6A2AE06E8DA7C4B7A127B7D6F2BE9A6.recercat1?sequence=1. – P. 56 (Accessed 31.05.2020).

[36] **European Parliament to hold extraordinary plenary on 26 March. Available at: https://www.europarl.europa.eu/pdfs/news/expert/2020/3/press_release/20200319IPR75308/20200319IPR75308_en.pdf (Accessed 23.05.2020).**

Rego A.V., Matskevich A.Yu. 2019. The problem of access of antitrust authorities to the privacy of communications // Russian Competition Law and Economics. No 3.P. 18.

Joris van Hoboken and Frederik Zuiderveen Borgesius, Scoping Electronic Communication Privacy Rules: Data, Services and Values, 6 (2015) JIPITEC 198, para 1. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777156 (Accessed 07.06.2020).

Zwitter, A., Gstrein, O.J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Journal of International Humanitarian Action 5, 4 (2020). Available at: https://www.researchgate.net/publication/341476623_Big_data_privacy_and_COVID-19_-_learning_from_humanitarian_expertise_in_data_protection (Accessed 05.06.2020).