Journal of Siberian Federal University. Humanities & Social Sciences
2020 13(10): 1576–1589

DOI: 10.17516/1997-1370-0664
УДК 341.64

The Right to Privacy and Data Protection in the Information Age

Tigran D. Oganesian*
Institute of Legislation and Comparative Law
under the Government of the Russian Federation
Moscow, Russian Federation

Received 09.06.2020, received in revised form 31.08.2020, accepted 25.09.2020

Abstract. The article considers the legality of mass surveillance and protection of personal data in the context of the international human rights law and the right to respect for private life. Special attention is paid to the protection of data on the Internet, where the personal data of billions of people are stored. The author emphasizes that mass surveillance and technology that allows the storage and processing of the data of millions of people pose a serious threat to the right to privacy guaranteed by Article 8 of the ECHR of 1950.

Few companies comply with the human rights principles in their operations by providing user data in response to requests from public services. In this regard, States must prove that any interference with the personal integrity of an individual is necessary and proportionate to address a particular security threat. Mandatory data storage, where telephone companies and Internet service providers are required to store metadata about their users' communications for subsequent access by the law enforcement and intelligence agencies, is neither necessary nor proportionate.

The author analyses the legislation of some countries in the field of personal data protection, as well as examples from practice. Practice in many States is evidence of the lack of adequate national legislation and enforcement, weak procedural safeguards and ineffective oversight, which contributes to widespread impunity for arbitrary or unlawful interference with the right to privacy.

In conclusion, we propose a number of measures aimed at improving the level of personal data protection in accordance with the international standards. In order to provide guarantees and a minimum level of adequate data protection in the face of new challenges to human rights in an ever-changing digital environment, the author proposes to solve a number of pressing issues. Firstly, States should not have the right to ask companies for and have absolute access to user data without a court order. Secondly, the process of sending a request and receiving data from a telecommunications company should be regulated in detail and transparent. The availability of specialized judges with technical expertise shall be valuable.

* Corresponding author E-mail address: t.oganesian@mail.ru
ORCID: 0000-0001-8239-694X

Keywords: European court of human rights, Council of Europe, data protection, personal data processing, mass surveillance, right to respect for private life.

Research area: law.

Citation: Oganesian, T.G. (2020). The right to privacy and data protection in the information age. J. Sib. Fed. Univ. Humanit. Soc. Sci., 13(10), 1576–1589. DOI: 10.17516/1997-1370-0664.

Introduction

The digital age, or the information age, is characterized by the widespread use of computers, the Internet and digital technologies, involving collection and processing of personal data of millions of people. Search engines, social networks, messengers make our lives easier, allowing us to communicate with the world and express opinions. The collection and storage of personal data are also indispensable tools of state bodies in the fight against crime and terrorism. However, despite its many advantages, the digital age also poses challenges to privacy and data protection, as vast amounts of personal information are collected and processed in increasingly complex and opaque ways. Mass surveillance and technologies to store and process the data of millions of people pose a serious threat to the right to privacy guaranteed by Article 8 of the Convention for the protection of human rights and fundamental freedoms drafted in 1950 (ECHR, Convention).

As Orla Lynskey notes, Data protection legislation has until recently been viewed by lawyers, politicians, and academics as "marginal and technical" (Lynskey, 2017: 253). However, this perception has changed as data protection has become the focus of attention for a number of reasons. Firstly, the dramatic increase in the processing of personal data has inevitably led to the need for uniform standards of data protection. Secondly, the right to data protection has been recognized internationally in the case-law of the European Court of Justice (ECJ) and the ECHR.

According to the Eurobarometer survey conducted in March 2015 among citizens of the European Union (hereinafter – the EU), 8 out of 10 people believe that they do not have full control over their personal data (Special Eurobarometer, 2015: 4). And only 15% of citizens believe that they have full control over their data, while half of the respondents (50%) believe that they have partial control, and almost one third (31%) believe that they have no control over personal information on the Internet. As for Russian citizens, 68% of respondents believe that in Russia personal data are poorly protected from illegal use and only 11% of all respondents indicated that personal data in our country as a whole are well protected (Results of the public opinion Fund survey, 2013).

As recalled by the General Assembly in its resolution 68/167, the international law of human rights provides a universal structure, according to which it is necessary to evaluate any interference in the rights of an individual to inviolability of private life (UN General Assembly Resolution 68/167). The International Covenant on civil and political rights of 1966 provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence. Other international human rights instruments contain similar provisions. While the right to privacy under the international human rights law is not an absolute right, any case of interference must be carefully and critically assessed as necessary, legitimate and proportionate.

The international human rights law provides a strong and universal framework for the promotion and protection of the right to privacy, including in the context of surveillance, interception of digital communications and the collection of personal data. However, experience in many States indicates a lack of adequate national legislation and enforcement, weak procedural safeguards and ineffective oversight, which contributes to widespread impunity for arbitrary or unlawful interference with the right to privacy.

Theoretical framework

The study is based on consideration of some issues of mass surveillance and data protection in the context of the right to privacy. Particular theoretical attention is paid to authors who study the evolutionary interpretation of the provisions of Article 8 of the Convention in the light of "modern conditions," which allows the ECHR to include the right to personal data protection (Nardell, 2010: 46). At the same time, long before the development of digital technologies, a number of researchers warned that the processing of information by computers in combination with the availability of data can lead to serious risks, in particular, have a negative impact on privacy (Westin, 1970: 299; Raymont, 1986: 119). In the context of the analysis of national data protection norms, some experts note that as a result of the use of the term "confidentiality" in the US, this definition was subsequently integrated into international and European legal instruments in the field of personal data protection (González Fuster, 2016: 6). In this regard, some authors argue why the data protection legislation has until recently been viewed by lawyers, politicians and academics as "marginal and technical" (Lynskey, 2017: 253).

Experts' research on the impact of digital technologies not only on human privacy, but also on a wide range of other human rights, from freedom of expression and freedom of Assembly to protection against discrimination, is of great interest (Bernal, 2016: 245; Raymont, 1986: 119; Chesterman, 2012: 414).

Statement of the problem

The development of digital technologies has made it easier to monitor, collect and process personal data. Personal data obtained illegally against millions of users of social networks and messengers represent important information for their intended use. In this regard, the international legal regulation of personal data protection plays a key role. The problem of mass surveillance is still not adequately addressed, either at the national or international levels. Although the right to respect for private life under Article 8 of the ECHR applies extraterritorially, it is clear that the rules governing state surveillance require additional legal standards. As the United Nations High Commissioner for Human Rights rightly pointed out, government surveillance "has gone from an exceptional measure to a dangerous habit" (Report of the Office…, 2014). It is clear that the protection of the privacy of millions of people from mass surveillance needs to be addressed at both national and international levels.

Methods

The methodological basis of the research included general scientific methods of cognition: dialectical, logical, system, statistical, etc. In addition, the methods inherent in the science of international law were used: the system-legal method, the comparative-legal method and the method of interpretation of law. The latter was particularly relevant when considering the legal nature and specificity of the decisions of the European court of Human Rights. The method of legal analysis, which allows to identify patterns and trends in the development of national legislation, legal positions of international courts in the field of data protection, is of particular importance.

The chronological method determines the sequence of international legal acts, court practice of the ECHR, regulating the protection of personal data. The technical and legal method makes it possible to analyse the content of Convention No. 108, as well as other documents in the field of automated data processing. The involvement of statistical data allows us to assess the attitude of European society to the protection of their data and to conclude that data protection has become one of the issues of concern to people. With the help of the comparative legal method the specificity of the judgments of the European Court of Human Rights, as well as the legislation of individual countries on the protection of personal data is considered.

In general, the systematic methodology is associated with the fact that the research is closely linked with practice, which allows us to examine the real processes and phenomena.

Discussion

The conventional framework of the Council of Europe on data protection

Article 8 of the Convention for the protection of human rights and fundamental freedoms of 1950 guarantees everyone the right to respect for personal and family life, housing and correspondence and prevents interference by public authorities with the exercise of this right, except where such interference is provided for by law and is necessary in a democratic society in the interests of national security or public order. As noted by G. Nardell, ECtHR interprets Paragraph 1 of Article 8 of the ECHR quite "generously and widely" (Nardell, 2010: 46). This evolutionary interpretation of the provisions of Art. 8 of the Convention, in the light of "modern conditions," allows the Strasbourg court to include the right to protection of personal data.

Mass surveillance is prima facie interference with Article 8 of the ECHR. The European Court of Human Rights at the time issued decisions in several cases concerning data protection and surveillance, including the interception of communications (Malone v. the United Kingdom), multiple forms of surveillance (Klass and Others v. Germany), storing of personal data by public services (Leander v. Sweden, S. and Marper v. the United Kingdom). Article 8, Paragraph 1, of the Convention affirms the right to privacy. Communications intercepted and stored under the mass surveillance programmes without the consent of an individual are subject to Article 8 of the Convention.

The Council of Europe Convention on the protection of individuals with respect to the automatic processing of personal data (hereinafter – Convention 108) provides additional protection for any data processing carried out by the private and public sectors, including the processing of data by judicial and other law enforcement authorities (Convention No. 108). The Convention defines "personal data" as "any information about a particular or identifiable natural person (data subject)," which includes communications intercepted by the government surveillance programmes.

This Convention is the first binding international instrument to protect individuals from abuses that may occur in the collection and processing of data, and at the same time aims to regulate the cross-border flow of personal data.

The Convention 108 not only provides safeguards for the collection and processing of personal data, but also prohibits, if national law does not provide adequate safeguards, the processing of "sensitive" data regarding a person's race, political opinion, health, religion, sexual life, criminal history, etc. The Convention also gives a person the right to know that data is collected and, if necessary, to be able to correct them.

The Council of Europe adopted the Convention against cybercrime (Budapest Convention) in 2001, which, along with the Convention 108, regulates the activities of states in the cyberspace.

It should be noted that the Convention 108 and the Budapest Convention were adopted as regional European instruments, but eventually acquired the international, albeit not universal, status, since they allow non-European countries to join. The Budapest Convention was ratified by 56 countries, including non-CoE member states that signed it (USA, Canada, Japan and South Africa). Similarly, the Convention 108 has expanded its scope, to which, in addition to 47 CoE member states, Mauritius, Senegal, Tunisia and Uruguay have acceded.

Today, it is obvious that both conventions require appropriate modifications in connection with the changed realities of the development of mass surveillance technologies. The evolution of information and communication technologies, which offers unprecedented opportunities for humanity, poses new challenges, including in the area of criminal justice and the rule of law in the cyberspace.

The Protocol amending the Convention No. 108 contains relevant innovations that reinforce the requirement that data processing be proportionate and that the principle of data minimization be applied. The modernized Convention also strengthens the accountability of data controllers and the transparency of data processing; introduces additional safeguards

for relevant persons in the context of algorithmic decision-making, such as the right to know the logic behind data processing.

All the changes and additions to the Convention 108 and the Budapest Convention will provide a unique tool to promote safety and adequate protection of the rights and freedoms of an individual in the face of new challenges to human rights in a constantly changing digital environment. In addition to these two fundamental acts, the General Data Protection Regulation (GDPR) of the European Union entered into force on 5 May 2018, amending and improving the principles enshrined in the previous EU Directive.

PACE Reaction

The practice of mass surveillance is a fundamental threat to human rights and violates the right to privacy enshrined in Article 8 of the ECHR. A report prepared by Dutch Deputy Peter Omzigt, beginning with a quote by Alexander Solzhenitsyn: "Our freedom is based on the fact that others do not know about our existence," confirms that states do participate in mass surveillance, having a chilling effect on the exercise of fundamental freedoms.

In the report, PACE expressed concerns about "far-reaching, technologically advanced systems" used by states for the collection, storage and analysis of personal data of citizens. The Assembly recognized the need for "effective targeted surveillance of suspected terrorists and organized criminals," while noting that mass surveillance did not contribute to the prevention of terrorist acts (PACE Resolution 2045, 2015).

PACE proposed the adoption of the international "intelligence Code," which establishes general rules for the monitoring of citizens and the exchange of intelligence. In order to restore confidence between Council of Europe member states and between citizens and their own governments, it is necessary to establish a legal framework at the national and international levels that protects human rights, especially the right to privacy.

All of this points to the urgent need to establish a clearer legal framework for the activities of intelligence agencies to monitor within and beyond national borders. The Council of Europe has an important role to play in this regard, as stated by the Council of Europe Commissioner for Human Rights N. Muižnieks, "groundless mass storage of communication data is fundamentally contrary to the rule of law, incompatible with the basic principles of data protection and ineffective" (The rule of law…, 2014: 22).

Protection of personal data on the Internet

At the beginning of the digital era, American poet and essayist John Perry Barlow said that the Internet would open "a world in which anyone anywhere could express their beliefs without fear of being forced into silence" (Barlow, 1996). The digital revolution and technological advances have not only changed people's attitudes to personal data, but in turn have challenged existing concepts of privacy and remedies. It's hard to disagree with C. Chesterman who said that "efforts to protect privacy have always been forced to respond to new threats and technologies" (Chesterman, 2012: 414). At the same time, Alan F. Westin warned that the information processing by a computer in combination with the availability of data can lead to serious risks, in particular, have a negative impact on privacy (Westin, 1970: 299).

Internet companies have become central platforms for discussion, access to information, trade and human development. They collect and store personal data of billions of people, including information about their habits, locations and activities.

Few companies comply with human rights principles in their operations by providing user data in response to threats and demands from governments. Some states require to remove links, websites and other materials that are alleged to be in violation of national law. Public authorities are increasingly seeking to remove content out of court. Some states have established specialized government units to communicate with companies to remove content. The group of the European Union on the transfer of information on the Internet, for example, "seeks terrorist and violent extremist content

on the Internet and works with suppliers of online services with the aim of eliminating this content" (EDRi, 2016: 3). The European Union code of conduct on combating illegal hatred on the Internet provides for an agreement between the European Union and four major companies, including on the removal of unwanted content.

Each company undertakes to comply in principle with the national legislation in which it operates. As Facebook notes, "if, after careful legal review, we determine that content is illegal under the local law, we will make it unavailable in the relevant country or territory" (Facebook, Government requests). One of the instruments of minimization is transparency: many companies report annually on the number of government requests they receive from each state. However, companies do not always disclose sufficient information on how they respond to government requests and do not regularly report on government requests.

A distinction must be made between failures and government requests to companies to delete data. Such companies as Facebook, Google, and Twitter are receiving increasing requests from intelligence agencies each year to provide user data and delete content. A common purpose of this kind of interference (failures) are not only social networks, but messengers (for example, WhatsApp, Telegram). This is particularly common when rising public dissent and protests are considered to be fuelled by the digital communication networks. Communication shutdown, in such circumstances, disorientate protesters and disrupts the coordination between the leaders of the protest or movement. Blackouts can also be used as a security measure in a period of uncertainty following terrorist attacks. A striking example of the pre-smartphone era is the suicide bombings in London in July 2005, followed by the disconnection of the cell phone signal in the area around the affected metro station. This measure was strongly condemned in the United Kingdom and reflects an approach more widely adopted in the non-democratic countries.

In this regard, the report of Jan Rydzak, PhD in Government and Public Policy of the University of Arizona and former Google policy officer of the global network initiative is of interest. The report presents the results of the author's research on the impact of network violations on human rights. The author argues that massive violations of rights on the Internet by restricting access to social networks and exercising control over user data constitute a radical form of digital repression that restricts numerous rights enshrined in the international treaties (Rydzak, 2018: 9).

In his report, the American scientist considers new technological means of suppressing protests, noting that since 2011, network failures and massive network outages have become a widespread tool for information control. As the author of the report rightly points out, "requests for personal data and content removal are part of the information monitoring and control mechanism in many states" (Rydzak, 2018: 7). Based on world development indicators and own observations (2017), Rydzak lists the countries with the fastest growing trends in state control over the Internet for 2005-2015: Bahrain (72.4%), Kazakhstan (69.9%), Azerbaijan (69%), Qatar (68.2%), Russia (58.2%), Albania (57.2%), Saudi Arabia (56.9%). It is noteworthy that this list includes three member states of the Council of Europe: Azerbaijan, Albania and Russia.

To overcome this problem, we should emphasize the role of partnerships between the Council of Europe and leading companies with access to billions of personal data around the world, such as: Facebook, Google, Kaspersky Lab, Digital Europe, GSMA Europe, Deutsche Telekom. As Executive Director of the Global Network Initiative Judith Lichtenberg rightly pointed out, "by underpinning this partnership, the Council of Europe is investing in a dialogue between states, companies and the civil society to address the critical global digital rights challenges facing all countries."

The first ever report on the regulation of online content, in which a special rapporteur examines the role of states and companies in social networks in creating an enabling environment for freedom of expression and access to information on the Internet, can make a significant contribution. In the face of contemporary threats such as "fake news," "virtual"

extremism, the special rapporteur urges states to refrain from adopting laws that require "active" monitoring or filtering of content that is incompatible with the right to respect for private life (Report of the special…, 2018). States should refrain from imposing disproportionate sanctions, whether fines or incarceration, on companies that do not wish to meet states' requests for data.

Recognizing that surveillance of electronic communications data may be necessary for the national security interests, government mass surveillance programmes raise issues of compliance with the international legal standards. States must demonstrate that any interference with the personal integrity of an individual is necessary and proportionate to address a specific security threat. Mandatory data retention, where telephone companies and Internet service providers are required to store metadata about their users' communications for subsequent access by the law enforcement and intelligence agencies, is neither necessary nor proportionate (Report of the Office…, 2018).

In assessing the need for action, the Human Rights Committee, in its general comment No. 27 on Article 12 of the International Covenant on Civil and Political Rights, stressed that "restrictions must not violate the very essence of the right [...]; the relation between the right and restriction, between the norm and exception must not be reversed" (CCPR/C/21/Rev.1/Add. 9, p. 3. 11). In addition, such measures should be proportionate: if there is a legitimate aim and appropriate safeguards, the state may be allowed to monitor; however, the burden of proving that intervention is necessary and proportionate rests with the government. Thus, the mass surveillance programmes can be considered arbitrary, even if they serve a legitimate purpose and have been adopted on the basis of an accessible legal regime. In this regard, the Human Rights Committee stressed the importance of "measures to ensure that any interference with the right to privacy is consistent with the principles of legality, proportionality and necessity, regardless of the nationality or location of persons whose communications are under direct supervision" (CCPR /C/USA/CO/4, para. 22).

Legal positions of the European Court of Human Rights

Technological advances have changed the nature of data that can be obtained through surveillance – for example, the increased use of smartphones and related devices provide a new dimension of data, such as geolocation data and biometric data, including face and fingerprint recognition. This combination of factors means that the new digital surveillance is qualitatively and quantitatively different from the traditional surveillance or interception of communications. Where traditional data have been considered as an element of the right to privacy, as reflected in Article 8 of the ECHR, the new form of communication (data) has a broader meaning, a broader scope, affecting a wider range of human rights. Mass surveillance affects not only privacy, but also a wide range of other human rights, from freedom of expression and assembly to protection against discrimination. As p. Bernal rightly points out, "confidentiality acts as the guardian of these rights" (Bernal, 2016: 245).

The ECHR has consistently held the view that the collection and storage of personal data by the police or national security authorities constitutes an interference with Article 8 (1) of the ECHR (Malone v. the United Kingdom, Klass and Others v. Germany, Leander v. Sweden). Many other decisions of the ECHR are related to the interference in the right to privacy by conducting surveillance and observation. For example, the ECHR came to the conclusion that there has been a violation of Article 8 of the ECHR in the case of Allan v. the United Kingdom, when the authorities secretly recorded a private conversation between a prisoner in a prison cell. The court held that the use of audio and video recording devices in the applicant's cell, in the prison visit area and in relation to another prisoner constituted a violation of the applicant's right to privacy. Since there was no regulatory system in place at the time to regulate the use of secret recording devices by the police, this interference was not in accordance with the law.

Transactions involving the processing of personal data may not be subject to Article 8 of the ECHR unless the private interest or

personal life of an individual has been jeopardized. In its case law, the ECHR considers the concept of "private life" as a broad concept, covering even aspects of professional life and social behaviour. The court also notes that the protection of personal data is an important part of the right to respect for privacy (Handbook on European Data Protection Law, 2018). However, despite the broad interpretation of privacy, not all types of personal data processing in themselves jeopardize the rights protected by Article 8 of the Convention. Where the ECtHR considers that the processing operation in question affects the right of individuals to respect for private life, it examines whether such interference is justified. The right to respect for private life is not an absolute right, but must be balanced and consistent with other legitimate interests and rights.

For example, in Rotaru v. Romania the applicant alleged a violation of the right to respect for private life in connection with the possession and use by the Romanian intelligence service of a file containing his personal information. The ECHR pointed out that, while domestic legislation allows for the collection, recording and archiving in secret files of information affecting national security, it does not impose any restrictions on the exercise of these powers, which remain at the discretion of the authorities. For example, domestic legislation does not specify the types of information that can be processed with respect to individuals, as well as the circumstances in which such measures can be taken and other procedural aspects. The Court therefore concluded that domestic legislation did not meet the requirements of Article 8 of the ECHR (§ 57).

Another aspect of the protection of personal data is not only the collection of data, but also their storage. So, in Brunet v. France the complainant appealed against the storage of information in the police database containing information on convicted persons, accused persons and victims. Despite the fact that the criminal proceedings against the applicant were discontinued, the data stored in the database. The ECtHR, having found out that there had been a violation of Article 8 of the Convention, considered that in practice the applicant had not been able to delete his personal data from the database. The ECtHR also examined the nature of the information included in the database and indicated that it was intrusive into the applicant's private life because it contained personal data about the applicant. In addition, the Court found that the period of retention of personal records in a database of 20 years is excessive, especially considering the fact that no court has issued a guilty verdict to the applicant.

The collection and compilation of several types of protected information from various sources creates new human rights risks that this court cannot turn a blind eye to, given that almost everything we do leaves a digital trail. Similarly, the protection of health data is fundamental to the realization of the right to respect for private and family life, in particular when it comes to information on HIV infection.

As for the compliance of Russian legislation with the Council of Europe's Convention standards, in addition to the key ruling in the case of Roman Zakharov v. Russia, in which the ECHR found that the system of secret interception of telephone communications in the Russian Federation does not meet the requirements of Article 8 of the Convention (§ 244), other decisions will be made in the future that are important for the development of domestic practice and legislation in the field of personal data protection.

Currently, due to the adoption of a package of anti-terrorist laws in Russia, the ECHR has adopted two complaints from Telegram on the decision of the Russian authorities to block the messenger in the country. In the complaints, Telegram points out that "the Russian authorities did not even try to establish a balance between the need to counter terrorism and ensure public security and the protection of citizens' rights to respect for private life."

Protection of personal data in selected countries

Gloria González Fuster notes that, as a result of the use of the term "privacy" in the United States, this definition was subsequently integrated into the international and European legal instruments in the field of personal data

protection (Gonzalez Fuster, 2016: 9). The USA most often faces the problem of protecting users' personal data, since most of the global IT companies are registered there. In this regard, global companies are the most vulnerable and are able to transfer millions of personal data to third parties. For example, a scandal occurred when it became clear that Cambridge Analytica illegally used the data of 87 million Facebook users in the interests of the election headquarters of Donald Trump and the organizers of the campaign for the UK's withdrawal from the EU. In a letter dated June 08, 2018, Facebook had to tell the US Congress about the information that the social network collects information about its users and about the sources where it receives it. Facebook, in particular, collects and stores information about the time and duration of work in the network, information about online purchases of users; contacts from the user's address book, etc.

Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes the intelligence services of the United States to obtain "information from foreign intelligence" targeting surveillance of persons who are not U.S. citizens abroad. The law promotes important intelligence gathering, and poses serious challenges to the privacy and data protection of non-US residents.

A certain concern is the so-called CLOUD Act (Clarifying Lawful Overseas Use of Data Act) adopted in March 2018 by the US Congress, which allows the US government agencies to enter into bilateral agreements with the authorities of other countries and obtain from it companies access to personal data of citizens stored on foreign servers, without notifying users or local authorities about the request for personal data.

This law will have a negative impact on the inter-state exchange of information during investigations conducted by the law enforcement agencies. The effect of this law will also affect the case law, in particular, currently the Supreme Court of the United States (SCOTUS) is considering a case that raises the question of whether the US Department of Justice had the right to force a company to provide e-mail clients, which is stored on the company's servers in Ireland, without the permission of the Irish government (Jeong, 2018).

Technology development also means that surveillance, which would be prohibitively expensive as well as difficult to implement at the practical level, has now become relatively simple and inexpensive and, therefore, more accessible to the state. In France, in 2015, the law No. 2015-912 was adopted, or as it was called by the French themselves "big brother Le Francais", which expanded the powers of public services to collect and store metadata "for national security purposes." Similar laws have recently been adopted in Australia (in 2015 amended the Law "On telecommunications"), Sweden (2010), Belgium (2013).

A clear example of the observation is the incident that occurred in **Ukraine** in January 2014. During the protest in Kiev, a group of people whose mobile phones indicated that they were in close proximity to the venue of the rally received text messages that they were "registered as participants in the riots" (The New York Times, 2014). Surveillance via mobile phones was used to try to intimidate people into not participating in further protests. The consequences of this observation go far beyond the right to privacy, but also affect the right to freedom of Assembly and Association.

Another serious problem is the security of connected devices. In particular, in **Germany**, government authorities banned a toy named Kayla, who was answering questions of a child playing with it; through the built-in application it was looking for answers on the Internet. After serious concerns about the impact of toys on respect for the privacy of children the German authorities found that the doll was actually a hidden spy device. This doll could record and transmit the messages through the app. If doll makers had not taken adequate security measures, the doll could have been used by anyone to eavesdrop and record conversations (Walsh, 2018).

A little later, in November 2017, the German authorities called on parents to destroy the smartwatch for children with a SIM card and a limited telephony feature that is configured and controlled by the app. In October 2017, similar-

ly, the Norwegian consumer Council (NCC) reported that "some children's watches, including Gator and GPS for children, had flaws such as transmitting and storing data without encryption." This meant that strangers, using hacking techniques, could track children as they moved or force the child to be in a completely different place.

This example is a clear example of the fact that technologies that are ahead of the law do not always meet the data protection standards. What is the violation in this case? Firstly, the companies behind these toys reserve the right to share the personal data of children with third parties. Secondly, children's data can be used for analytical and research purposes not related to the toys themselves. Thirdly, the data of children is collected and used for the purposes for which you have not obtained explicit consent. Fourth, there are no clear data storage procedures.

A striking example of arbitrariness on the part of the authorities in the implementation of illegal mass surveillance are the facts set out in the report of Human Rights Watch in relation to **Ethiopia** (Human Rights Watch, 2014). The report proves how websites of opposition parties, independent media, blogs and a number of international media are regularly blocked by government censors. Radio and television stations are constantly subject to failures. Bloggers and Facebook users face harassment and threats of arrest because of their posts.

However, targeted advances in efforts to protect personal data can be seen in some developing countries. For example, in February 2018, the Moroccan data protection authority (CNDP) organized an international conference, the purpose of which was to inform numerous participants and discuss the right to privacy and data protection, its role in African economies, supporting measures that are necessary for technological advances without risk, as well as the impact of the new international and European standards on the African continent.

An interesting proposal to support the Council of Europe was the opportunity given to the Republic of Belarus to visit the French National Commission on Informatics and Liberty (CNIL) at the stages of the draft law on data protection to discuss technical aspects of data protection and draw on experience.

Data protection in Russia

Despite the undeniable, albeit not very high-profile successes, it can be said that the period of bringing the Russian legal system into line with the Convention has not yet been completed and requires action at all levels of the national legal system. One of the challenges facing many countries today is the development of mandatory international rules for the protection of personal data and their subsequent implementation in domestic legislation.

Russian law enforcement practice and national legislation in the field of personal data protection indicate that the authorities not only do not create effective legal remedies against illegal data collection, but also pursue a policy of expanding the powers of special services for the arbitrary collection and storage of personal data.

What can be done in this situation? According to the author, the main step is the introduction to the standards of the Council of Europe, as well as the manifestation of activity in the discussion of the draft additional Protocol to the Convention 108. Despite the crisis in relations between the Russian Federation and PACE, which we hope will be resolved in the near future, the national authorities need to make proposals and comments on the modernized version of the Convention 108. In the future, it is very important to sign and ratify the Protocol to Convention 108 in a timely manner, which is intended to become an upgraded version of Convention 108 that meets modern information and communication realities and standards for the protection of personal data. At the same time, the Russian Federation needs to revise national legislation in order to adapt the protection of private life to the problems associated with the technological advances that allow mass surveillance. At the national level, appropriate technical and organizational measures should be taken to ensure the protection of personal data, ensuring compliance with the principles enshrined in the practice of the ECtHR, as well as to prevent accidental or illegal data collection. The Russian authorities

should abandon the policy of requiring the organizers of the dissemination of information to keep data on millions of citizens for 6 months, without creating appropriate legal remedies against arbitrary mass surveillance, as well as mechanisms to control the activities of the security services.

Conclusion

The protection of personal data is of primary importance for the exercise of the right to privacy and family life. In this regard, covert surveillance is even more important in the context of the development of the Internet, as it is based on the creation of programmes and methods for monitoring the transmission of information online. Telecommunication companies provide a large amount of data to government services each year in response to government demands (Brown, 2010: 95). Monitoring of the use of the Internet and telephone data by national authorities may well be at the centre of further proceedings in the ECHR.

In this regard, as a hopeful signal, it is possible to consider the recent decision of the court of Appeal of the United Kingdom (Case No C1/2015/2612, 2015), which recognized the current legislation regulating surveillance as violating the right to privacy and noted the need to bring it in line with the international human rights law.

As the Council of Europe Commissioner for human rights, Dunja Mijatovic, rightly points out, "it is extremely important to find the right balance between technological development and the protection of human rights, because the future of the society in which we want to live will depend on it". It is important to recognize that this balance requires closer cooperation between public authorities (governments, parliaments, judicial and law enforcement agencies) and private enterprises, academia, NGOs, international organizations and society at large.

Because of the need to protect millions of citizens' data, IT companies must be able to engage in dialogue with governments. It is necessary to solve three urgent questions. Firstly, the states should not have the right to request and obtain absolute access to users' data from companies without a court decision, serious grounds for a suspect's involvement in a crime that, in turn, is in the interests of national security. Secondly, the process of sending a request and receiving data from telecommunication companies should be regulated in detail and transparent. Thirdly, with regard to the question of whether special courts should be established to deal with surveillance measures, the states need to find judicial means of protecting personal data. A good option is to have special procedures to deal with confidential information before the courts. The availability of specialized judges with technical expertise would be valuable.

Taking into account the constantly developing technology implementation in the national legislation the provisions of the Convention 108 and Convention on Cybercrime (Convention on Cybercrime, 2001), will provide a unique tool to promote safety and a minimum level of adequate protection of the rights and freedoms of an individual in the face of new challenges to human rights in a constantly changing digital environment. In addition to these two fundamental acts for the protection of personal data of citizens, General Data Protection Regulation (GDPR) is of particular value, which amends and improves the principles enshrined in the previous EU Directive.

References

Barlow, J.P. (1996). *A Declaration of the Independence of Cyberspace*. Available at: https://www.eff.org/cyberspace-independence (accessed 1 October 2020).

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. In *Journal of Cyber Policy*, 1: 2, p. 245.

Brown, I. (2010). Communications Data Retention in an Evolving Internet. In *International Journal of Law and Information Technology.* 19(2), 95–109.

Chesterman, S. (2012). After Privacy: The Rise of Facebook, the Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012, In *Sing. J. Legal Stud.* P. 414.

Clarifying Lawful Overseas Use of Data Act. In *CLOUD Act*. Available at: https://www.congress.gov/bill/115th-congress/house-bill/4943 (accessed 28 May 2019).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28 January 1981. ETS No. 108.

Convention on Cybercrime (2001). Budapest, 23 November 2001. ETS No. 185.

Gonzalez Fuster, G. (2016). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer International Publishing. P. 6.

ECtHR (2002). In *Allan v. the United Kingdom*, No. 48539/99, 5 November 2002.

ECtHR (2014). In *Brunet v. France, No. 21010/10*, 18 September 2014.

ECtHR (1984). In *Malone v. the United Kingdom*, no. 8691/79, 2 August 1984.

ECtHR (1978). In *Klass and Others v. Germany*, no. 5029/71, 6 September 1978.

ECtHR (1987). In *Leander v. Sweden*, no. 9248/81, 26 March 1987.

ECtHR (2008). In *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, 4 December 2008.

ECtHR (2000). In *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000.

ECtHR (1997). In *Z v. Finland,* No. 22009/93, 25 February 1997.

ECtHR (2015). In *Roman Zakharov v. Russia* [GC], no. 47143/06, 4 December 2015.

European Union, Internet Referral Unit, Year One Report (2016), sect. 4.11; submissions by European Digital Rights (EDRi), 2–3.

Facebook report to the us Senate (2018). June 8. Available at: https://www.commerce.senate.gov/public/_cache/files/ed0185fb-615a-4fd5-818b-5ce050825a9b/62027BC70720678CBC934C93214B0871.senate-judiciary-combined-7-.pdf (accessed 1 October 2020).

Foreign Intelligence Surveillance Act. Available at: https://fas.org/irp/agency/doj/fisa/ (accessed 1 October 2020).

Handbook on European data protection law (2018). Available at: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed 1 October 2020).

Human Rights Watch. They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia. Available at: https://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf (accessed 1 October 2020).

Jeong, S. (2018). *What's at stake in the Microsoft Supreme Court case.* Available at: https://www.theverge.com/2018/2/26/17052946/microsoft-email-supreme-court-case-law-enforcement (accessed 1 October 2020).

Lynskey, O. (2017). The «Europeanisation» of Data Protection Law. In *Cambridge Yearbook of European Legal Studies*. Vol. 19. Pp. 252-286.

Nardell, Gordon Q.C. (2010). Levelling up: Data privacy and the European Court of Human Rights. In *Data protection in a profiled world, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert. Dordrecht: Springer.* 43-52.

PACE Resolution 2045 (2015). § 11. Available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692 (accessed 1 October 2020).

Raymont P. (1986). New Technology and Data Protection. In *Y.B.L. Computers & Tech*. Vol. 2. Pp. 110-139.

Results of the public opinion Fund survey among Russian citizens aged 18 and older (2013). Available at: http://runet.fom.ru/posts/10922 (accessed 1 October 2020).

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2018). 18 June–6 July. Available at: https://freedex.org/a-human-rights-approach-to-platform-content-regulation/ (accessed 1 October 2020).

Report of the Office of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age (2014). 30 June. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (accessed 1 October 2020).

Rydzak, J. (2018). Disconnected: A Human Rights-Based Approach to Network Disruptions. In *Global Network Initiative (GNI*). P. 9.

Special Eurobarometer 431 (2015). Data protection. P.4. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf (accessed 1 October 2020).

Telegram complaint to the ECHR. Available at: https://agora.legal/fs/a_delo2doc/65_file_Telegram_ESPCH_Dop.pdf (accessed 1 October 2020).

The law of France No. 2015-912 from 24 Jul 2015. Available at: http://www.assemblee-nationale.fr/14/dossiers/renseignement.asp (accessed 1 October 2020).

The New York Times (2014). Available at: https://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html (accessed 1 October 2020).

The rule of law on the Internet and in the wider digital world (2014). Issue paper published by the Council of Europe Commissioner for Human Rights. December. P. 22. Available at: https://rm.coe.int/ref/CommDH/IssuePaper(2014)1 (accessed 1 October 2020).

UK Case No C1/2015/2612 (2015). Available at: https://www.judiciary.uk/judgments/secretary-of-state-for-the-home-department-v-david-davis-mp-and-others/ (accessed 1 October 2020).

UN General Assembly Resolution 68/167 (2013). UN Doc A/RES/68/167. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 1 October 2020).

Walsh, C. (2018). *The Internet of Things: Cayla doll is banned in Germany over privacy and security concerns.* Available at: https://www.lexology.com/library/detail.aspx?g=d3a5448e-ecbc-41fb-b0cb-3d28bd-fe841e (accessed 1 October 2020).

Westin, Alan F. (1970). *Privacy and Freedom*, (originally published in 1967). New York: Atheneum. 299 p.

Право на неприкосновенность частной жизни и защита данных в эпоху информационных технологий

Т.Д. Оганесян
Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации
Российская Федерация, Москва

Аннотация. Рассмотрена правомерность массового наблюдения и защиты персональных данных в контексте международного права прав человека, в том числе права на уважение частной жизни. Особое внимание уделяется защите данных в интернете, где хранятся личные данные миллиардов людей. Автор подчеркивает, что массовое наблюдение и технологии, позволяющие хранить и обрабатывать данные миллионов людей, представляют серьезную угрозу для права на неприкосновенность частной жизни, гарантированного статьей 8 Конвенции о защите прав человека и основных свобод 1950 г.

Немногие компании соблюдают принципы прав человека в своей деятельности, предоставляя данные о пользователях в ответ на запросы государственных служб. В этой связи государства должны доказать, что любое вмешательство в личную жизнь является необходимым и соразмерным для решения конкретной определенной угрозы безопасности. Хранение данных, когда телефонные компании и поставщики интернет-услуг обязаны хранить метаданные о сообщениях своих пользователей для последующего доступа правоохранительных и разведыватель-

ных агентств, не представляется ни необходимым, ни пропорциональным.
Авторы анализируют законодательство некоторых стран в области защиты персональных данных, а также примеры из практики. Практика во многих государствах свидетельствует об отсутствии надлежащего национального законодательства и правоприменения, о слабых процессуальных гарантиях и неэффективном надзоре, что способствует повсеместной безнаказанности за произвольное или незаконное вмешательство в право на частную жизнь.
В заключение предлагаются меры, направленные на повышение уровня защиты персональных данных в соответствии с международными стандартами. Для обеспечения гарантий и минимального уровня надлежащей защиты данных перед лицом новых вызовов к правам человека в постоянно меняющейся цифровой среде автор предлагает решить ряд насущных вопросов. Во-первых, государства не должны иметь право запрашивать у компаний и получать абсолютный доступ к данным пользователей без судебного решения. Во-вторых, процесс отправления запроса и получения данных у телекоммуникационных компаний должен быть детально регламентирован и прозрачен. Наличие специализированных судей, обладающих техническими знаниями, будет иметь определенную ценность.

Ключевые слова: Европейский суд по правам человека, Совет Европы, защита персональных данных, обработка персональных данных, массовое наблюдение, право на уважение частной жизни.

Научная специальность: 12.00.00 – юридические науки.