MASS SURVEILLANCE AND DATA PROTECTION IN THE DIGITAL AGE

Safronova Elena
Doctor of law, Professor of the Department of constitutional and international law (Belgorod National Research University, Belgorod, Russia), elena_safronova_2010@mail.ru
Oganesian Tigran
PhD in law, Lecturer in international law of the North Caucasian branch of the Russian State University of justice (Krasnodar, Russia), t.oganesian@mail.ru
Nikonovich Sergei
Doctor of law, Associate Professor, Professor of Higher school of business, management and law (Russian state University of tourism and service, Moscow, Russia),trahezunt@yandex.ru
Koroleva Ekaterina
PhD in law. Associate Professor of criminal and civil law. (Lipetsk state technical University, Lipetsk, Russia). katysha-lip@mail.ru
Bocharov Alexander
PhD in law, Associate Professor of Higher school of business, management and law (Russian state University of tourism and service, Moscow, Russia, bocharov.lip@yandex.ru

Abstract .the article considers the legitimacy of mass surveillance in the context of international human rights law and the existing mechanisms of protection of the right to respect for private life. The author notes that the problems concerning the protection of personal data of millions of people from mass surveillance should be solved both at the national and international levels. 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. Special attention is paid to data protection in global social networks, which are vulnerable and store personal data of billions of people. The article provides examples of case-law of the court of justice of the EU and the ECtHR on the protection of personal data. Further, based on the examples of some countries, the prospects for the creation of a new international instrument for the regulation of surveillance are outlined and an attempt is made to identify the role of European countries and Russia in this process..

Keywords: data protection; mass surveillance; human rights; Internet.

From the author. One of the challenges facing European countries today is the development of mandatory international rules for the protection of personal data and their subsequent implementation in domestic legislation. Of course, Russia is not the last in this process. The Russian authorities have proved that despite the crisis of relations between Moscow and Strasbourg, our country remains an active participant in the adoption of the most important norms and standards for the whole of Europe. A striking example of such participation was the opening for signing in Moscow in October 2011. Convention of the Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (Convention 'Medicrime') is an innovative legal tool, in fact global in nature, developed at the initiative of Russia. Cooperation between Russia and Europe in the adoption of common standards in the field of personal data protection could mark the twenty-year period of Russia's recognition of the norms of the European Convention on human rights and perhaps would make a contribution to overcoming the crisis in relations with the PACE.

.When printing was invented, it became easier to control public opinion; radio and cinema allowed us to take a step further in this direction. And with the development of television technology, when it became possible to conduct reception and transmission of one device, private life came to an end.

George Orwell «1984»[1]

1. Introduction

The digital age or the age of information technology is characterized by the widespread use of computers, the Internet and digital technologies, involving the 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 is also an indispensable tool of state bodies in the fight against crime and terrorism. However, despite its many advantages, the digital age also poses challenges for privacy and data protection, as vast amounts of personal information are collected and processed in increasingly complex and opaque ways. Mass surveillance and technology 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 European Convention on Human Rights (ECHR, Convention).

Today, social media services are an integral part of the daily lives of millions of people. To join or create a profile on social networks, individuals are asked to provide personal: from photos, videos to contacts, political views and personal messages. The development of technology has also made it possible for law enforcement agencies to monitor devices that are in the hands of ordinary citizens (e.g. smartphones, GPS devices, tablets, smart watches, etc.).

[1] *Orwell George.* 1984. M: Progress. 1989.

Today as the personal data can be photos, email address, Bank details, GPS data (geolocation), messages on social networking sites, medical data, IP address, computer etc Analysis data can be used for commercial purposes, for example, based on the analysis of needs and interests to provide appropriate services and goods to consumers. On the basis of "likes" in social networks, listening to music or watching movies of the user, it is possible to get a clear picture of the person's personality, thereby imposing certain advertising or information on him, taking into account already identified interests.

It is clear that the challenges of protecting the privacy of millions of people from mass surveillance need to be addressed at both the national and international levels.

2. Personal data protection: public opinion and international law

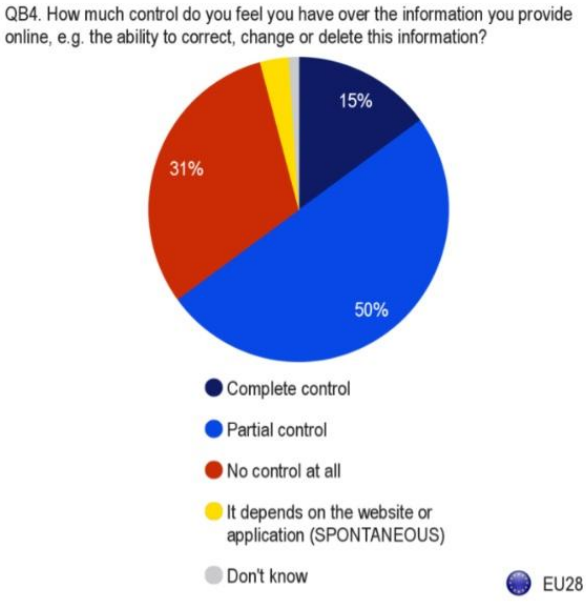
The information given to journalists by Snowden, still causes debate not only about the mass surveillance of intelligence services of the United States and other countries, but primarily about the lack of adequate legal regulation and legal protection at the national and international levels. "Snowdengate" indicates the existence of far-reaching, technologically advanced systems, created by the intelligence services of some States for collecting, storing and analyzing personal data on a global scale.

During the spring session of PACE, the Committee on legal Affairs and human rights at its meeting on April 8, 2014 organized a video conference with E. Snowden on mass surveillance. "Snowdengate" inevitably raises the question of the impact of large-scale personal data collection on human rights and is an important step in informing the public about the existence of mass surveillance programmes in the security services.

According to the survey Eurobarometer, conducted in March 2015 among EU citizens, 8 out of 10 people believe that they do not have full control over their personal data [2]. 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 a 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 is poorly protected from illegal use and only 11% of all respondents indicated that personal data in our country as a whole is well protected[3].

In turn, 45% of EU citizens who are more concerned about the protection of their data believe that the protection of personal data should be carried out at the EU (international) level, while about four out of ten people (42%) believe that protection should be provided at the national level. According to 55% of Europeans, state authorities should be responsible for illegal collection and storage of personal data.



Base: Respondents who provide personal information online (n=19,430 in EU28)

At the same time, article 8 of the European Convention guarantees everyone the right to respect for personal and family life, housing and correspondence and does not allow " interference by public authorities in the exercise of

[2]Special Eurobarometer 431. Data protection. P.4. URL: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

[3] Results of the public opinion Fund (FOP) survey among Russian citizens aged 18 and older on April 7, 2013. URL: http://runet.fom.ru/posts/10922

this right, except where such interference is provided by law and necessary in a democratic society in the interests of national security or public order…»[4].

The Council of Europe Convention on the protection of individuals with regard to automatic processing of personal data (Convention 108) provides additional protection for any data processing carried out by the private and public sectors, including data processing by judicial and other law enforcement authorities[5]. The Convention defines "personal data" as " any information about a particular or identifiable natural person (data subject)", which includes communications intercepted by government surveillance programmes.[6]

This Convention is the first binding international instrument to protect individuals from abuse 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.

Convention 108 not only provides guarantees for the collection and processing of personal data, but also prohibits, if national law does not provide adequate guarantees, the processing of "sensitive" data on a person's race, political views, health, religion, sexual life, criminal history, etc.the Convention also gives the person the right to know that data about him / her are collected, and, if necessary, to be able to correct them.

In the framework of the Council of Europe in 2001 adopted the Convention on cybercrime (Budapest Convention)[7], which, along with Convention 108 regulates the activities of States in cyberspace.

The Convention is the first international Treaty on crimes committed through the Internet and other computer networks.

It should be noted that Convention No. 108 and the Budapest Convention were adopted as regional European instruments, but eventually acquired the status of international, even if not universal, since they allow non-European countries to join. The Budapest Convention was ratified by 56 countries, including non – members of the Council of Europe (USA, Canada, Japan and South Africa)[8]. Likewise, expanded its scope of Convention 108, to which in addition to the 47 COE member States joined in Mauritius, Senegal, Tunisia, Uruguay.[9]

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 cyberspace.

The Protocol amending Convention No. 108 contains relevant innovations that reinforce the requirement that data processing be proportionate and that the principle of data minimization be applied[10].

In view of all the changes and additions, Convention No. 108 and the Budapest Convention will provide a unique instrument for guaranteeing and adequately protecting human rights and freedom in the face of new challenges to human rights in an ever-changing digital environment. In addition to these two basic acts on 5 may 2018 came into force the General regulations of the European Union on personal data protection (General Data Protection Regulation, the GDPR), which amends and improves the principles enshrined in the former EU Directive.

Debate of the PACE. 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 Omcigt, beginning with a quote by Alexander Solzhenitsyn: "our freedom is based on the fact that others are unaware of our existence", confirms that States do participate in mass surveillance, exerting a chilling effect on the exercise of fundamental freedoms.

In the report, PACE expressed concern 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 has not contributed to the prevention of terrorist acts[11].

---

[4] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14. Rome, 4 November 1950. ETS No. 5. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765

[5] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28 January 1981. ETS No. 108. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[6] Pedraja-Rejas, Liliana, Roberto Vega Massó, and Jaime Riquelme Castañeda. "La importancia de los estilos de liderazgo en la calidad de las unidades académicas universitarias." Opción 34.86 (2018): 130-151.

[7] Convention on Cybercrime. Budapest, 23 November 2001. ETS No. 185. URL: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/185

[8] Countries that have ratified without signature: Australia, Chile, Dominican Republic, Costa Rica, Israel, Mauritius, Panama, Sri Lanka, Tonga.

[9] Varalakshmi, K., & Babji, Y. (2016). Production of Dried Chicken Meat products Extended with Different levels of soyaflour concentration. International Journal of Engineering, Science and Mathematics, 5(1), 210-218.

[10] Protocol amending the Convention for the protection of individuals with regard to the automatic processing of personal data (CED No. 108). Will be open for signature from 25 June 2018. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

[11] PACE Resolution 2045 (2015), § 11. URL: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692

PACE has proposed the adoption of an international "intelligence Code", which establishes General rules for the monitoring of citizens and the exchange of intelligence.

In order to restore confidence between the member States of the Council of Europe 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 intelligence surveillance activities within and outside 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, " unsubstantiated mass storage of communication data is fundamentally contrary to the rule of law, incompatible with the basic principles of data protection and ineffective"[12].

3. Data protection on the Internet

At the beginning of the digital era, American poet and essayist John Perry Barlow said that the Internet will open "a world in which anyone anywhere can Express their beliefs without fear of being forced to silence"[13].

When Internet privacy is threatened, the credibility of the Internet disappears, depriving everyone, including journalists, bloggers and human rights defenders, of privacy and freedom of communication, this has a deterrent effect on other rights, including freedom of expression.

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

At one time, the founder of Facebook declared a desire to "develop social infrastructure to give people the opportunity to build a global community that will work for all of us"[14]. Twitter has promised a policy that "will improve and not limit free and global communication"[15]. Russian company Vkontakte "unites people all over the world", while the Chinese technology company Tencent seeks to "help build a harmonious society and become a good corporate citizen"[16].

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 the removal of links, websites and other material that is alleged to be in violation of national law. Public authorities are increasingly seeking the removal of content through non-judicial means. Some States have established specialized government units to communicate with companies in order to remove certain content. Group of the European Union on the transfer of information in Internet, for example, "noted terrorist and violent extremist content on the Internet and works with suppliers of online services with the aim of eliminating this content"[17]. 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[18].

Each company undertakes to comply in principle with the national legislation in which it operates. As Facebook notes, "if, after a thorough legal review, we determine that the content is illegal under local law, we will make it unavailable in the relevant country or territory"[19]. One of the tools to minimize 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 government requests.

States often face 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, the scandal occurred when it became clear that Cambridge Analytica illegally used the data of users 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. Facebook in his letter of 08 Jun 2018. The us Congress had to tell about the information that the social network collects about its users and about the sources

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

[13] John Perry Barlow, A Declaration of the Independence of Cyberspace, 8 February 1996.

[14] Mark Zuckerberg, Building global community, Facebook, 16 February 2017.

[15] Twitter, S-1 Registration Statement, 13 October 2013, pp. 91–92.

[16] Tencent, About Tencent.

[17] European Union, Internet Referral Unit, Year One Report, sect. 4.11; submissions by European Digital Rights (EDRi), p. 1 and Access Now, pp. 2−3.

[18] European Commission, Code of Conduct on countering illegal hate speech online: First results on implementation (December 2016).

[19] Facebook, Government requests: FAQs. See also Google legal removal requests; Twitter rules and policies; Reddit content policy.

where it receives it. Facebook, in particular, collects and stores information about the time and duration of the network, information about online purchases of users; contacts from the user's address book, etc.[20]

A distinction needs to be made between failures and government requests for companies to delete data. It companies such as Facebook, Google and Twitter are receiving more and more requests from intelligence agencies to provide user data and delete content every year. The common purpose of this kind of interference (failures) are not only social networks, but messengers (for example, WhatsApp, Telegram). This is especially common when rising public dissent and protests are considered fuelled by digital communication networks.

In this regard, the report by Jan Rydzak, PhD in public and public policy at 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 study on the impact of network violations on human rights. The author argues that mass copyright infringement on the Internet by limiting access to social networks and monitor user data, represent a radical form of digital repression which restricts many rights enshrined in international treaties[21].

4.1. Legal positions of the European court of human rights in the field of data protection

Mass surveillance is a prima facie interference with article 8 of the ECHR. The European court of human rights (ECtHR) once ruled on a number of cases concerning data protection and surveillance, including interception of communications[22], various forms of surveillance[23], storage of personal data by public services .[24].

According to the ECtHR, "private life is a broad term that cannot be fully defined"[25]. Since the protection of personal data is fundamental to the right to privacy, the Court has repeatedly held that "the systematic collection and storage of data by the security services of citizens constitutes an interference with the privacy of these persons, even if the data is collected in a public place or relates exclusively to the professional or social activities of that person"[26].

In a recent decision in the case of v Benedik. Slovenia from April 24, 2018, the Court found a violation of article 8 of the Convention due to the fact that Slovenian police has not received a court order to access information of the subscriber associated with a dynamic IP-address.[27]. The Slovenian police, without a court order, received information about a subscriber associated with an IP address that was calculated by Swiss law enforcement after the applicant shared files containing child pornography on the network. In August 2006, the Slovenian police asked the local Internet service provider to provide information about the user to whom this dynamic IP address was assigned by the company. In August of the same year, the Slovenian police requested information from the Internet service provider about the IP address, but a court order allowing such information to be requested was issued only in December 2006.

The ECtHR concluded that the provision of the Criminal procedure law used by the police to gain access to subscriber information did not raise questions about its accessibility, but that there were sufficient safeguards against abuse. This provision concerns the request for information about the owner or user of an electronic communication device, but it does not contain rules relating to the connection between a dynamic IP address and subscriber information.

The ECtHR has recognized that dynamic IP addresses registered by online carriers are the providers of the services constitute personal data[28]. According to the Court, the police had to obtain the permission of the national court in advance.

In a dissenting opinion on the case, ECHR judges A. Yudkovskaya and M. Boshnyak note that the case in question provided a unique opportunity to clarify the scope of reasonable expectations of privacy in a digital age where a striking amount of information about our privacy is easily shared outside our control. In turn, the bosnian judge F. Vehabovic does not agree with the majority opinion, indicates that the data about the IP address cannot be considered personal data.

The new case-law of the ECHR shows the Court's desire to call upon States to establish safeguards against abuse of power in monitoring. So in the case of Ben Faiza v. France the Complainant claimed that the installation of a geolocation device on his vehicle had further enabled his movements to be tracked, which constituted an interference with his right to respect for private life.

---

[20] Facebook report to the us Senate. June 8, 2018. URL: https://www.commerce.senate.gov/public/_cache/files/ed0185fb-615a-4fd5-818b-5ce050825a9b/62027BC70720678CBC934C93214B0871.senate-judiciary-combined-7-.pdf

[21] Jan Rydzak. Disconnected: A Human Rights-Based Approach to Network Disruptions // Global Network Initiative (GNI). 2018. P. 9. URL: https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/05/Disconnected-Report-Network-Disruptions.pdf

[22] ECtHR, *Malone v. the United Kingdom*, no. 8691/79, 2 August 1984. URL: http://hudoc.echr.coe.int/.

[23] ECtHR, *Klass and Others v. Germany*, no. 5029/71, 6 September 1978.

[24] ECtHR, *Leander v. Sweden*, no. 9248/81, 26 March 1987; *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, 4 December 2008.

[25] ECtHR, *Shimovolos v. Russia*, no. 3194/09, 21 June 2011, § 64.

[26] Ibid.

[27] An IP address is a unique number assigned to each device on the network that allows devices to communicate with each other. Unlike static IP addresses, dynamic IP addresses change each time you connect to the Internet.

[28] Breyer v. Germany. 19.10.16. URL: http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

The European Court, while recognizing that the real-time installation of a GPS geolocation device was a violation of article 8 of the Convention, concluded that the French law in the field of real-time geolocation activities at that time (until the Adoption of the law of 28 March 2014) did not provide sufficiently clearly, to what extent and how the authorities had the right to use their powers.

As for the compliance of Russian legislation with the Council of Europe Convention standards, in addition to the key decision in the case "Roman Zakharov V. Russia", in which the ECtHR 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[29], in the future will be made and other decisions relevant to 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[30] the ECtHR has received 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 strike a balance between the need to counter terrorism and ensure public safety and protection of citizens rights to respect for private life"[31].

Thus, in the case-law of the ECtHR, the conditions for the collection and storage of personal data by public services are formulated.

First, intervention must be in accordance with the law.

Second, interference with the right to respect for private life must be necessary in a democratic society in the interests of one of the legitimate objectives of article 8, paragraph 2: national security, public safety, economic welfare, etc.

4.2. Legal positions of the court of Justice of the European Union (CJEU)

French scientist P. Bernal rightly asks and answers in the affirmative: is there "balance" between the right to privacy and national security considerations – or is it a delusion to create such a balance?[32]

The fact that such a balance change is necessary was highlighted in the judgment of the court of justice of the European Union in the Digital Rights Ireland case in April 2014, in which the data retention Directive (Directive 2006/24/EC) was declared illegal. The Directive required public electronic communication providers to retain citizens ' telecommunications data for a period of two years to ensure that the data were available for the prevention, investigation and prosecution of serious crimes. This measure applied only to metadata, location data and data needed to identify the subscriber or user and did not apply to the content of electronic communications.

The CJEU concluded that Directive 2006/24/EC was an interference with the fundamental right to protection of personal data "because it provides for the processing of personal data"[33]. The CJEU also noted that Directive 2006/24 entailed "widespread and particularly serious interference with fundamental rights"[34]. However, the decision stated that the interference with these rights was disproportionate: data collection is even carried out for persons in respect of whom there is no evidence of their involvement in serious crimes [35].

Another aspect of privacy and protection of personal data is the right to be forgotten or, as it is also called, the right to be forgotten, an example of which may be the case of Google Spain, which addressed the issue of Google's responsibility for providing search results links to outdated information about the financial difficulties of the applicant. Google claimed that it simply provided a hyperlink to a web page that posted information about the applicant's insolvency[36]. Google argued that the request to remove outdated information from a web page should be addressed to the owner of the web page, not Google, which simply provides a link to the original page. The CJEU concluded that Google, when it provides links to web pages and indexes content to provide search results, becomes the data controller to which the duties and obligations under EU data protection legislation apply. The CJEU ruled that, under certain

[29] ECtHR, *Roman Zakharov v. Russia* [GC], no. 47143/06, 4 December 2015, § 244.

[30] The package of antiterrorist laws signed by the President of the Russian Federation in July 2016 (the so-called" Yarovaya package") obliges mobile operators and Internet companies to store information about the content of conversations and correspondence of users, including photo, video and audio files, to provide them on request of special services. The approved rules require companies to provide FSB decoding keys in case if Internet services use message encryption.

[31] Telegram filed a second complaint to the ECHR against the blocking in Russia. URL: https://www.kommersant.ru/doc/3661707

[32] Paul Bernal (2016) Data gathering, surveillance and human rights: recasting the debate, Journal of Cyber Policy, 1:2, P. 244.

[33] Para. 36. Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union (8 April 2014).

[34] Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union (8 April 2014).

[35] para 58. Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union (8 April 2014).

[36] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, paras. 55–58.

conditions, individuals have the right to request the deletion of personal data. This right may be invoked where information relating to a person is inaccurate, inadequate, inappropriate or excessive for data processing purposes.

5.1. Protection of personal data in certain countries

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, Law No. 2015-912 [37] 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 good example of 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 of the riots"[38]. Surveillance through mobile phones was used to try to intimidate people so that they would not participate in further protests. The consequences of this monitoring go far beyond the right to privacy, but also affect the right to freedom of Assembly and Association.

Another major problem is the security of connected devices. In particular, in **Germany,** government agencies banned a toy named Cayla, which is answering questions of a child playing with her, through the built-in application looking for answers on the Internet. After serious concerns about the impact of toys on children's privacy, the German authorities admitted that the doll is actually a hidden spy device. With this doll the messages of the child as well as those nearby can be recorded and transmitted through the app. If doll manufacturers had not taken adequate security measures, the doll could be used by anyone to eavesdrop and record conversations[39].

A little later in November 2017, the German authorities called on parents to destroy smart watches for children with SIM cards and limited telephony features that are set up and controlled by the app. In October 2017, similarly, the Norwegian consumer Council (NCC) reported that "some children's watches, including Gator and GPS for children, had shortcomings, such as transmission and storage of data without encryption. This meant that strangers, using hacking methods, could track children as they moved, or make the child appear in a completely different place[40].

This example is a clear example of the fact that advanced legislation technologies do not always meet the standards of data protection. What is the expression of the violation in this case? First, the companies behind these toys reserve the right to share the personal data of children with third parties. Second, children's data can be used for analytical and research purposes unrelated 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 procedures for storing data.

5.2. Russia's role

In General, despite Russia's initiatives to adopt international acts in the field of mass surveillance and protection of personal data, national legislation is still far from the Convention standards.

Russian law enforcement practice and national legislation in the field of personal data protection show that the authorities not only do not create effective legal remedies against illegal data collection, but also conduct 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 to introduce the CE standards, as well as the manifestation of activity in the discussion of the above-mentioned «iCodex». Despite the crisis in relations between Russia and PACE, which we hope will be resolved in the near future, the national authorities need to make proposals and comments on the concept of the «iCodex». It is necessary that as many countries as possible sign and ratify the Protocol to the Convention 108, which is intended to become a modernized version of the Convention 108, which meets modern information and communication realities and standards of personal data protection. 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 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.

6. Conclusion

Non-targeted mass surveillance in Europe is illegal under international human rights law. It is obvious that the rules of regulation of mass surveillance and data protection by European States are outdated and require additional legal standards.

The protection of personal data is of paramount 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

[37] Loi № 2015-912 du 24 juillet 2015 relative au renseignement publiée au Journal Officiel du 26 juillet 2015 URL: http://www.assemblee-nationale.fr/14/dossiers/renseignement.asp

[38] The New York Times. URL: https://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html

[39] The Internet of Things: Cayla doll is banned in Germany over privacy and security concerns. URL: https://www.lexology.com/library/detail.aspx?g=d3a5448e-ecbc-41fb-b0cb-3d28bdfe841e

[40] Germany bans children's smartwatches. URL: https://www.bbc.com/news/technology-42030109

based on the creation of programmes and methods for monitoring the transmission of information online. Telecommunications companies provide a large amount of data to government services every year in response to government demands. 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.

The problem of mass surveillance is still not adequately addressed, either at the national or international level.

In order for the national and international legal framework to be credible, they must be provided with credible verification mechanisms. The Council of Europe should take this opportunity to draw attention to the need for international standards in this area, while ensuring that intelligence agencies continue to protect our security by using an effective and proportionate means. One possible solution is to offer PACE to adopt an iCodex to protect an unlimited number of people from mass surveillance. If adopted, it has all the chances to become not only a regional Treaty, but also to provide an opportunity for non-European States to become parties to it, respectively, extending its action outside Europe.

References

1. Bernal Paul. Data gathering, surveillance and human rights: recasting the debate, Journal of Cyber Policy, 2016. 1:2, P. 244.
2. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14. Rome, 4 November 1950. ETS No. 5.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28 January 1981. ETS No. 108.
4. Convention on Cybercrime. Budapest, 23 November 2001. ETS No. 185.
5. CJEU. Breyer v. Germany. 19.10.16.
6. CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, paras. 55–58.
7. Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union (8 April 2014).
8. ECtHR, Malone v. the United Kingdom, no. 8691/79, 2 August 1984.
9. ECtHR, Klass and Others v. Germany, no. 5029/71, 6 September 1978.
10. ECtHR, Leander v. Sweden, no. 9248/81, 26 March 1987.
11. ECtHR, Roman Zakharov v. Russia [GC], no. 47143/06, 4 December 2015, § 244.
12. ECtHR, Shimovolos v. Russia, no. 3194/09, 21 June 2011.
13. European Commission, Code of Conduct on countering illegal hate speech online: First results on implementation (December 2016).
14. European Union, Internet Referral Unit, Year One Report, sect. 4.11; submissions by European Digital Rights (EDRi), p. 1 and Access Now, pp. 2−3.
15. Facebook report to the us Senate. June 8, 2018. URL: https://www.commerce.senate.gov/public/_cache/files/ed0185fb-615a-4fd5-818b-5ce050825a9b/62027BC70720678CBC934C93214B0871.senate-judiciary-combined-7-.pdf
16. John Perry Barlow, A Declaration of the Independence of Cyberspace, 8 February 1996.
17. Orwell George. 1984. M: Progress. 1989.
18. PACE Resolution 2045 (2015), § 11. URL: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692
19. Protocol amending the Convention for the protection of individuals with regard to the automatic processing of personal data (CED No. 108). Will be open for signature from 25 June 2018.
20. Pedraja-Rejas, Liliana, Roberto Vega Massó, and Jaime Riquelme Castañeda. "La importancia de los estilos de liderazgo en la calidad de las unidades académicas universitarias." Opción 34.86 (2018): 130-151.
21. Results of the public opinion Fund (FOP) survey among Russian citizens aged 18 and older on April 7, 2013. URL: http://runet.fom.ru/posts/10922
22. Rydzak Jan. Disconnected: A Human Rights-Based Approach to Network Disruptions // Global Network Initiative (GNI). 2018. P. 9.
23. Special Eurobarometer 431. Data protection. P.4. URL: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf
24. The rule of law on the Internet and in the wider digital world. Issue paper published by the Council of Europe Commissioner for Human Rights. December 2014. P.22. URL: https://rm.coe.int/ref/CommDH/IssuePaper(2014)1.
25. The Internet of Things: Cayla doll is banned in Germany over privacy and security concerns. URL: https://www.lexology.com/library/detail.aspx?g=d3a5448e-ecbc-41fb-b0cb-3d28bdfe841e
26. Varalakshmi, K., & Babji, Y. (2016). Production of Dried Chicken Meat products Extended with Different levels of soyaflour concentration. International Journal of Engineering, Science and Mathematics, 5(1), 210-218.