THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 3 Article 9

11-2017

Private Life Safety Provision in Digital Age

Olga Anatolyevna Kuznetsova
Perm State University, kuznetsova_psu@mail.ru

Natalia Bondarenko
Perm State University

Recommended Citation

Kuznetsova, Olga Anatolyevna and Bondarenko, Natalia (2017) "Private Life Safety Provision in Digital Age," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 3 , Article 9.
DOI: https://doi.org/10.15394/jdfsl.2017.1460
Available at: https://commons.erau.edu/jdfsl/vol12/iss3/9

Private Life Safety Provision in Digital Age

Cover Page Footnote

PRIVATE LIFE SAFETY PROVISION IN DIGITAL AGE

Olga Anatolyevna Kuznetsova
Perm State National Research University
Perm, Russia

Natalia Bondarenko
Perm State National Research University
Perm, Russia

ABSTRACT

Digital technology nowadays covers all the spheres of life of an individual and society's activities. With this, it is not a secret that it can be used both for the benefit and to the detriment of the person. In the digital age, private life is becoming most vulnerable to arbitrary interference. This article considers various violations of the rights to privacy, communication safety and inviolability of privacy security brought in by the digital revolution. The article concludes that the most important task in the sphere of private life safety is to find a balance of interests of the state, the society and individuals. Private life restrictions caused by the new global threats should not lead to complete disappearance of privacy.

1. INTRODUCTION

The appearance of new digital technologies, including rather cheap ones, has created fertile ground for the increase in the number of cyber delicts that pose a real threat to private life safety infringing on its inviolability. New kinds of infringement on private life arise in the information space, and a new privacy concept is formed in juridical science.

Indeed, "the explosive growth of digital data in the twenty-first century has been both a boon and a curse for law enforcement" (Harvard Law Review, 2016)[1].

However, it has been "a boon and a curse" not only for the state and its bodies, but also for individual persons and their privacy.

The rapid development of information technology and the transition to information society entails new threats to privacy as "the right to be let alone". The founders of the privacy concept (the right to be let alone) are American lawyers Louis Brandeis and Samuel Warren, who not only determined the importance of privacy for every individual, but also foresaw the dangers of violation thereof on the part of print (non-digital) media that only existed at that time (Brandeis and Warren, 1890)[2].

Respect to private life of a person is an essential element of individual freedom and a

[1] Digital duplications and the fourth amendment (2016). Harvard Law Review, vol. 129, № 4, pp. 1046.

[2] Brandeis L. & Warren S. (1890) The right to privacy. Harvard Law Review, vol. IV, № 5.

priority responsibility of the state. A person's right to private life presupposes not only creation and control of information about himself, but also unhindered transfer and disclosure thereof by the person himself to other entities without fear for its inviolability.

With that, the problems of privacy protection in the new digital context are officially recognized in Russia. The Information Security Doctrine of the Russian Federation points out directly: "The citizens' rights to inviolability of private life, to personal and family secrets and to privacy of correspondence enshrined in the Constitution of the Russian Federation have insufficient legal, organizational and technical support. Protection of data on individuals (personal data) collected by federal bodies of state power, bodies of state power of constituents of the Russian Federation and local authorities is poorly organized (Russian newspaper, 2000)[3].

Private life is an expression of a person's sovereignty, which is nowadays endangered by unprecedented possibilities of control that have emerged in the digital era.

Safety protection is one of the main focus areas of a state's domestic and international activity. States, which are aimed to protect and defend the citizens' private life, increasingly take initiatives aimed at weakening of inviolability of private life, for instance, the initiatives to establish databanks (national data bases of the citizens' DNA, fingerprints and financial status); to scan iris; to introduce total video surveillance in public places. Not only the borders of this natural human right are being displaced, but also its content is being narrowed beyond recognition. Under such conditions, the right to privacy is on the verge of becoming declarative and dissolving completely in the state's endeavors to ensure national security.

2. THE NOTION AND ELEMENTS OF PRIVATE LIFE

The term "private life" has long been used in international, European and national normative and enabling legislation.

Article 12 of Universal Declaration of Human Rights of 1948 imposes a ban on arbitrary interference with an individual's personal and family life and on arbitrary encroachment on inviolability of the home, privacy of correspondence, honor and reputation of the individual.

Article 17 of International Covenant on Civil and Political Rights says: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

In accordance with article 8 of European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950, everyone has the right to respect for his private and family life, his home and his correspondence.

In Russian law, the term "private life" first appeared at the legislative level in article 9 of the Declaration of Rights and Freedoms of Man and Citizen dated 1991. Subsequently, in Article 23 of the Constitution of the Russian Federation of 1993 there was declared a right to inviolability of private life, personal and family secret, protection of one's honor and reputation, as well as the right to privacy of correspondence,

[3] The information security doctrine of the Russian Federation (approved by the President of the Russian Federation from September 9, 2000, № PR-1895). Russian newspaper, 2000, September 28.

telephone conversations, mail, telegraph and other messages.

Article 24 of the Constitution of the Russian Federation says: "Collection, storage, use and dissemination of information about private life of a person without the person's consent is not allowed. Governmental authorities, local authorities and their officials have a responsibility to provide everyone with a possibility to consult documents and materials directly related to their rights and freedoms, unless it is provided for otherwise by the law".

The natural right to inviolability of private life is not one of the absolute rights of a person. According to par. 2 of article 1 of the Civil Code of the Russian Federation, civil rights can be limited by virtue of the federal law and only to the extent it is necessary for protection of the foundations of the constitutional order, morality, health, rights and legitimate interests of other entities, national defense and security of the state.

However, the above-mentioned concerns are phrased in such broad terms that they enable almost any limitation to be associated therewith. What are the "interests of society, state and other entities"? For example, in England, the Court of Appeal held it possible to disclose information on romantic relationship of a famous football player, because there is "public interest in making this information public" (Perova, 2012)[4].

It is evident that private life is an evaluative notion that does not allow formulating a strict logical definition. This is the part of life that people have the right not to make public.

The scope of private life may include "marriage, child-bearing, adoption, divorce, partition of property, family budget, disposal of property and money on deposit" (Petrukhin, 1999)5. Private life is "a sphere where every person exists, composed of relationships and actions meeting the personal needs of an individual, common to their way of life, including the information associated with family and love life of a person, his material standing, health status and character, that are of no significance for the society, but are important for the individual as they enable him to identify himself, as well as any other information protected from unauthorized access, all the more from disclosure" (Tarle, 2007)6.

The European Court of Human Rights has repeatedly pointed out that personal life encompasses physical and moral sides of human life and includes the right to enter into and develop relationships with other people and the outside world.

The Constitutional Court of the Russian Federation in its ruling № 248-O dated 09.06.2005 formulated its stand, according to which "the right to inviolability of private life ...means a possibility granted to a person and guaranteed by the state to control information about himself and prevent disclosure of information regarded as personal or private".

The Constitutional Court of the Russian Federation has repeatedly pointed out that the notion of "private life" includes the area of human life that is associated with an individual, that concerns himself only and is not subject to control by the society and the state, unless it is contrary to law.

With a view to study security threats and measures to prevent and combat them, one may

[4] Perova, N. (2012). Restrictions of freedom of expression to prevent disclosure of personal and state secrets in the law of the US and UK. Law and management. Twenty-first century, № 1 (22), pp. 93–99. (In Russ.).

[5] Petrukhin, I.L. (1999). Private life (legal aspects). State and law, № 1, pp. 64–73. (In Russ.).

[6] Tarle, E.G. Right to private life in Russia. The Law, March, pp. 163–166. (In Russ.).

distinguish certain elements of private life that are most attackable in digital age:

- the right to privacy and anonymity;
- the right to communicative inviolability;
- the right to inviolability of confidential information.

All the components of the right to private life form a single legal institution that includes provisions of different branches of law, as well as rules of both international and national instruments.

The above-mentioned elements of private life are potential objects of various cyber threats. For instance, in circumstances where a person's movements can be easily traced via his credit card or his cell phone, one can hardly speak of any right to privacy.

3. THREATS TO THE RIGHT TO PRIVACY AND ANONIMITY

The right to privacy presupposes inviolability of personal self-fulfillment (identification), physical and psychological privacy and anonymity.

The primary basis for psychological health of a person is the possibility to be alone, to define his whereabouts at any time period, to plan independently his movement from point A to point B on condition of anonymity. Autonomy of an individual is a condition of apartness from the state, the society and other people (even closest ones).

However, the widely used systems of satellite monitoring (GPS, GLONASS) make it possible to track the movement of almost everyone, often without the consent and knowledge thereof.

Some employers have recently started asking their employees to install applications on their smartphones that enable keeping track of them 24 hours a day, even during off-work hours. There have been cases where people were dismissed for having switched off such applications out of hours. Thus, Mirna Arias, who had been dismissed on that basis, brought an action against her employer for invasion of privacy and compensation of damage in excess of $500,000 (Mirna Arias vs Intermex)[7] (The suit, which claims invasion of privacy, retaliation, unfair business practices, and other allegations, seeks damages in excess of $500,000 and asserts she was monitored on the weekends when she was not working).

The modern world has introduced another way of "tracking" the object – radio-frequency identification, which is commonly used in marking of goods by RFID-marks. The threat to privacy is the possibility of remote information readout without the customer's knowledge.

If the marked item is paid for by a credit card (which is, in the digital world, getting more frequent), it becomes possible to link the mark to a certain person.

The problem of RFID-marks was pinpointed by senator Debra Bowen back in 2003: "How would you like it if, for instance, one day you realized your underwear was reporting on your whereabouts?"[8].

In the monitoring boom, the right to privacy can be lost completely.

[7] Kravets, D. Worker fired for disabling GPS app that tracked her 24 hours a day. Retrieved on July 23, 2016 from http://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day.

[8] Gilbert, A. (2015). Privacy advocates call for RFID regulation. Retrieved on July 30, 2016 from http://www.cnet.com/news/privacy-advocates-call-for-rfid-regulation.

Another major challenge in the modern world is the use of drones – pilotless aircrafts that, inter alia, can be used for secret surveillance of an individual, his private life and private property (Baude & Stern, 2016)[9].

Extensive installation of video cameras, including hidden ones, is also a threat to the right of privacy. Thus, in the European Court of Human Rights with regard to case "Martin against the United Kingdom", it was ascertained that local authorities had installed a hidden video camera on the wall of the house located near Martin's house, against the entrance to her house, in order to record her anti-social behavior. Ms. Martin applied to court with a complaint where she noted that video monitoring had been a burdensome factor of her everyday life and it had ruined her normal family and personal life. Her complaint was held acceptable in the procedure of article 8 of the Convention[10].

Installation of video cameras becomes a matter in dispute between neighbors in apartment houses. Thus, with regard to case of K.D. against K.L., the court ascertained that the parties of the dispute were living in different rooms of the same apartment, where K.D., with prior notice to K.L., had installed a video camera in the common corridor. The plaintiff thought that installation of the camera was an invasion of privacy, because the defendant had a possibility to record his private life. However, the court rejected the suit, because the plaintiff had failed to prove the fact of video recording and use of the video by the defendant[11]. In our opinion, such a judgment of the court can hardly be considered substantiated, because the neighbors' agreement is needed for installation of video cameras rather than just a notice thereof, while the use of the recorded video should be presumed.

4. THREATS TO THE RIGHT TO COMMUNICATIVE INVIOLABILITY

The right to communicative inviolability presupposes protection of privacy of negotiations and privacy of correspondence, which, in the digital world, is starting to seem a standard beyond attainment.

The case of former officer of the US National Security Agency Edward Snowden has had a broad resonance. He asserted that NSA officers were illegally wiretapping telephone conversations and intercepting e-mail correspondence. Governed by presumption of innocence, we are making no judgment on the case itself, evidence in the case and culpability of the subject. However, the potential possibility of a governmental agency performing such acts is a convincing threat to inviolability of correspondence and negotiations.

In 2016 the issue of communicative inviolability in Russia has become topical owing to the adoption of the so called "amendments by deputies Yarovaya and Ozerov" that modified a number of federal laws aiming at protection against terrorism and extremism. Among these amendments is the one to the Communication Law that makes the communication service providers responsible for storage on the territory of the Russian Federation of the following:

[9] Baude W. & Stern J.Y. (2016). The positive law model of the fourth amendment. Harvard Law Review, vol. 129, № 7, pp. 1883–1884.

[10] Martin v United Kingdom. Bulletin of the European Court of Human Rights, 2003, № 8. (In Russ.).

[11] The appellate decision of the Perm regional court from 2014, Mach, 12 in case № 33-1914. Retrieved on July 30, 2016 from http://www.consultant.ru/cons/cgi/online.cgi?base=SOJ&n=849180&req=doc.

1. information on receiving, transmitting, delivery and/or processing of the subscribers' voice data, text messages, pictures, sounds, video and other messages – for a period of three years upon completion of such processes;
2. the subscribers' text messages, voice data, pictures, sounds, video and other messages – up to six months upon completion of receiving, transmitting, delivering and/or processing them.

Communication service providers are obliged to submit to the authorized governmental bodies of the Russian Federation that carry on operational search activities or provide safety the specified information, information on subscribers to communication services, as well as information on the services rendered thereto and other information that is necessary for the performance of tasks assigned to such governmental bodies in the instances established by federal laws.

The above-mentioned amendments are strongly criticized by the society for reason of vulnerability of such information storages and possible violations of the communicators' private life secrets (NEWSru.com, 2016; postsovet.ru, 2016)[12].

In 2016 Russia lost in the European Court of Human Rights the case of Roman Zakharov[13], who appealed against infringement of the right to respect for private life and correspondence by the organization of a mobile phone communication secret wiretapping system and absence of efficient means of legal defense. Having heard the case, the European Court of Human Rights found violations of requirements formulated in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms that guarantees protection of the right to respect for private life.

5. INVIOLABILITY OF CONFIDENTIAL INFORMATION AND THREATS TO ITS SECURITY

In 2011 UNESCO examined and took note of the Code of Ethics for the Information Society, which asserts that respect for private life and personal data will be vitally important in the information society. In this regard: a) private individuals should take action for the protection of their private life and enhancement of safety of their data; b) organizations that have access to personal data should be compliant with the standards of bona fide activities in the field of information[14].

Russia ratified the Convention for the Protection of Individuals with regard to Automatic Processing of personal Data (concluded in Strasburg on January 28, 1981), according to article 7 of which, in order to protect personal data that are stored in automated data files, due security arrangements are made for prevention of accidental or unauthorized destruction or accidental loss thereof, as well as for prevention of unauthorized access to, alteration or dissemination of such data.

[12] NEWSru.com, (2016). Internet experts: "The Laws of Yarovaya-Ozerov" threaten national security. Retrieved on July 23, 2016 from http://www.newsru.com/russia/21jun2016/nationaldanger.htm; postsovet.ru, (2016). Retrieved on July 23, 2016 from https://www.postsovet.ru/blog/russia/770006.html.

[13] Roman Zakharov v Russia (complaint No. 47143/06). Bulletin of the European Court of Human Rights, 2016, № 6. (In Russ.).

[14] Code of Ethics for the Information Society. Retrieved on July 23, 2016 from http://www.ifap.ru/ofdocs/unesco/etcodex.pdf.

In Russia, the federal law "On Personal Data" has been in force since 2006, according to which personal data include any information associated, directly or indirectly, with a certain or defined individual (the subject of personal data). Besides, a List of Data of Confidential Character has been confirmed, where personal data are defined as "information about the facts, events and circumstances of private life of a citizen that makes it possible to establish his identify, apart from information subject to disclosure in mass media in circumstances prescribed by federal law"[15].

The entities that organize and perform processing of personal data, as well as define the objectives of personal data processing, the content of personal data to be processed and the actions (operations) to be applied to personal data are called personal data operators and they can be a governmental authority, a municipal authority, a corporate entity or a physical person[16].

In Russia, there are numerous official state-operated databases that store information on electorate (national automated system "Elections"), taxpayers (automated information system of the Federal Tax Administration), insured persons (automated information system of the Compulsory Medical Insurance Fund) and retired persons (automated information system of Pension Fund of the Russian Federation). In the short run, another database will be created – State Population Register of the Russian Federation, which is a part of the federal program "Electronic Russia" and which will contain information on every citizen of Russia under 19 counts: the person's surname, first name and patronymic name, gender, nationality, place of residence, kin relationship, information on birth and death, etc.

It is obvious that existence of such information systems is a mandatory attribute of information society, and renouncing them is irrational and already impossible. However, the problem of personal information leakage remains topical and becomes more complicated, because almost any entity can collect and process personal data.

In Russian practice, there are numerous cases of disclosure of the clients' personal data by the banks to third parties, including collection organizations. For example, Ms. Nikonova, I.G. and public joint stock company "Ural Bank for Reconstruction and Development" concluded a loan agreement where Ms. Nikonova gave her consent to processing of her personal data by the bank, including disclosure thereof to third parties for the purpose of execution of contractual obligations. Subsequently the borrower sent an application to the bank to recall her consent to processing (disclosure) of her personal data: personal mobile and home phone numbers; any contact phones and data of the third parties mentioned in the loan documentation; relatives' residential addresses, employers' names and addresses. However, the bank communicated her personal data to the collector for the purpose of debt recovery. The public prosecutions department and the court ruled the bank's actions to be a violation of legislation on personal data[17].

In it important to emphasize that one's consent to processing of personal data should be particular, informed and conscious.

[15] The decree of the President of the Russian Federation of 1997, March, 6 № 188 "On approval of List of data of confidential character". Russian newspaper, 1997, March, 14.

[16] Federal law of 2006, July, 27 № 152-FZ "On personal data". Russian newspaper, 2006, July 29.

[17] The resolution of the Seventeenth arbitration court of appeal dated 2016, January, 15 № 17АП-17396/2015-АК in case № А60-33071/2015. Retrieved on July 23, 2016 from http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=RAPS017;n=148454.

6. EXTERNAL AND INTERNAL THREATS AND PROTECTION OF SAFETY OF PRIVATE LIFE

The sources of threats to the safety of private life are most often ones of external nature. The delinquents that pose such a threat can be both governmental authorities and other entities. Thus, journalists, employers, spouses and relatives can unfoundedly interfere in private life using security cameras.

Yet, the development of digital technology has considerably increased the role of internal threats to safety of private life that emanate from the person himself. The notion of victimhood, as an inclination to become a victim of a delict, has stepped over the framework of criminal law. In the sphere of civil jurisdictional protection of private life, we can speak of the rise of such a phenomenon as self-delictolization – the person himself, using digital technologies imprudently and thoughtlessly, creates opportunities for violation of his private life safety. Posting his photos, personal data, telephone numbers, addresses, stories and videos about his life on various internet sites, the person considerably reduces the safety of his private space and, actually, contributes to acquisition of "victim of a delict" legal status.

For that matter, the category of inviolability of personal life, being an element of private life, is getting great significance. Personal life is the inner world of a person, his thoughts, feelings, world view and psychological security (Zhuravlev, 2014)[18]. The mobile, information-intensive and saturated life itself becomes a threat to an individual's personal and psychological safety.

Another factor that enhances vulnerability of personal life is low respect to privacy, which was devaluated during the Soviet period by "a Soviet man has nothing to hide" principle and is still unable to gain a high position in the legal values hierarchy of Russians.

However, even in highly developed foreign countries with the reign of law and long traditions of respect to and every possible protection of privacy, people are ready to discard a number of private life's aspects by virtue of combating the terrorist threat. It should be remembered that behind the vast databases storing private information there are real people, who can use them for unauthorized purposes[19]. No one has estimated the threat posed by their misbehavior associated with the use and disclosure of private information. After all, the ongoing processes of digital globalization make it possible to release an individual's private information to the "global domain".

Protection of private life safety is ensured by law-making and law-enforcement efforts.

The state, as a rule-making entity, sets:

1. permissive rules that establish the borders of an individual's possible conduct in private life in accordance with the prima facie principle "whatever is not prohibited is permitted";
2. imperative rules that prescribe due conduct of third parties with regard to non-violation of an individual's privacy (for example, obtaining a person's consent to processing of personal data and installation of a video camera);

[18] Zhuravlev, M.S. (2014). Philosophy of information security. *Proceedings of the Tula State University. Humanities,* № 2, p. 42.

[19] Bird, S.J. (2013). Security and privacy: Why privacy matters. Science and engineering ethics, vol. 19, № 3, pp. 669–671.

3. prohibitive rules that envisage criminal, administrative and civil liability for violation of one's privacy.

But the above-mentioned arrangements can hardly be found efficient; thus, the Criminal Code of the Russian Federation provides for penalties for violation of inviolability of private life (unlawful collection or dissemination of information on a person's private life that constitutes his personal or family secret without the person's consent or dissemination of such information in public speaking, publicly demonstrated work or mass media) (article 137); for violation of privacy of correspondence, telephone conversations, mail, telegraph or other messages (article 138); for unlawful circulation of special equipment designed for secret information acquisition (article 138.1). Still, there are few cases of prosecution for such crimes in Russia.

The law-enforcement arrangements are implemented by the authorized governmental bodies and non-governmental organizations. In this regard the most important role in prevention of violations of inviolability of private life should be allocated to the individual himself.

It is also important to emphasize the role of judicial authorities in protection of inviolability of private life. Privacy, unlike, for instance, the right to life and the prohibition of torture, is not absolute and can be limited "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (The Rt Hon the Lord Phillips of Worth Matravers, 2014)[20]. In this connection, it is important for the courts to look for and find proportionality and balance of private and public interests.

The legal views of the Constitutional Court of the Russian Federation have also a great lawmaking potential "for initiating changes in the country's normative sphere" (Kokotov, 2015)[21], which contributes to positive change of legislation associated with protection of private life with a glance to new digital reality.

7. CONCLUSION

Modern technology forces frequent and prompt revisions of social contract between the state and the individual with a view to the borders of interference in private life. As M. Losavio fairly remarked, "The future regulation of the informational lives of everyone will shape how the relationships between citizen and government evolve" (Losavio, 2014)[22]. Global threats, first of all terrorist ones, cannot but affect possibilities of restriction and interference in the private space of the individual. And still, the phenomenon of inviolability and secrecy of private life should not vanish in this process.

The most important objective in this sphere nowadays is to find a proper balance between the interests of the security of the state and the society and the private life of an individual.

[20] The Rt Hon the Lord Phillips of Worth Matravers, (2014). European Human Rights – a force for good or a threat to democracy? Russian Law: theory and practice, № 2, p. 10.

[21] Kokotov, A.N. (2015). On the Lawmaking matters of the Acts of the Constitutional Court of the Russian Federation. Russian Law: theory and practice, № 1, p. 13.

[22] Losavio, M. (2014). Evidentiary power and property of digital identifiers and the impact on privacy rights in the United States. Journal of Digital Forensics, Security and Law (JDFSL), vol. 9, № 2, p. 202.

