

LEGITIMATE EXPECTATIONS OF PRIVACY IN THE ERA OF DIGITALIZATION

ELENA OSTANINA,

Chelyabinsk State University (Chelyabinsk, Russia)

ELENA TITOVA,

South Ural State University (National Research University) (Chelyabinsk, Russia)

<https://doi.org/10.21684/2412-2343-2023-10-1-109-125>

This article contends that in the present era of digitalization people's right to privacy should be protected no less than it was before the widespread use of digital technologies. When taking into account the fact that digitalization has led to a greater exchange of information, it is important that the ways and forms of protecting privacy undergo certain changes. Firstly, more emphasis should be placed on the use of methods for the self-protection of privacy rights, including restricting access to information and configuring website settings so that reviews and comments can be posted only by registered users, and not anonymously. Secondly, the legal means of protection should be improved to prevent violations of privacy rights from occurring as well as to ensure that rights which have been violated are properly restored. In the event of a violation of the secrecy of personal data, the authors recommend the use of class actions. When a violation of the secrecy of correspondence, medical information or telephone conversations by a business entity or the owner of a website occurs, a claim for compensation for moral damage should be available. However, the authors of the article propose modifying such a claim for compensation for moral damage to more closely model a claim for the recovery of punitive damages. Furthermore, the authors establish a connection between the protection of the right to privacy and the variety of relevant information on the topic that is freely available.

Keywords: personal data; right to privacy; compensation for moral damage; punitive damages; medical secrecy; correspondence secrecy; banking secrecy.

Recommended citation: Elena Ostanina & Elena Titova, *Legitimate Expectations of Privacy in the Era of Digitalization*, 10(1) BRICS Law Journal 109–125 (2023).

Table of Contents

Introduction

1. Privacy as a Protected Intangible Personal Good

2. The Concept of Reasonable Expectations in Relation to the Protection of Privacy

3. Protection of Personal Data

4. Features of the Protection of Medical Secrets and Other Types of Secrets in the Era of Digitalization

5. Forms and Methods of Protecting Privacy

5.1. Self-defense of Personal Non-Property Rights

5.2. Compensation for Moral Damage as a Way to Protect the Right to Privacy

5.3. Possibility of Changing the Protection Method for More Complete Protection

Conclusion

Introduction

Privacy is one of the most important intangible personal benefits protected by constitutional and civil law. In the present era of digitalization, people voluntarily share their personal information as well as post their photographs on social media networks and other websites where they pay for goods, labor and services. As a result the question arises: How much should privacy protection change in the face of digitalization? Related to this question are other questions. In particular, can a person expect not to be filmed in public places without warning? And to what extent can a person object if a segment of this filming is used, for instance, on the network to illustrate news (such as, for example, the news about the fall of the meteorite that occurred in Chelyabinsk)? A person who participates in communication on a particular website or conducts transactions through an online platform typically expects that the information provided by him or her will be used only temporarily and only for the purposes for which it is provided.

Meanwhile, published jurisprudence shows that the use of information provided by a person is not always limited to the immediate purpose for which the information is provided. Two examples of unexpected (from the person's perspective) uses of the information provided by a person can be given.

The first is the case concerning the Prodoctorov.ru website (Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 12 November 2019 No. 14-KG19-15). A person granted permission to an employer to post information about the person's education, experience and expertise, as well as

a photograph on the company's website. All this information was published on the website of the medical organization, that is, it was freely accessible. Furthermore, the information was posted on the website "Prodoctorov.ru" such that users of the site could leave feedback on the professional activities of the doctor. Citing the fact that it was private information, the person demanded that it be removed from the Prodoctorov.ru website. The Supreme Court of the Russian Federation sent the case for a new trial, stating that during the new trial it should be determined whether or not the discussion of the doctor's professional activities is of public interest, and it should also be determined whether or not the plaintiff has effective means of protection against the anonymous reviews left on this website.

The second example is the well-known dispute that occurred between the Vkontakte society and the Data society (case no. A40-18827/2017, which was resolved by an amicable agreement reached between the two parties). The essence of the dispute was that the defendant had developed a program for processing the information posted by users on the Vkontakte social network. This information was made available in a machine-readable form and used for commercial purposes. According to the plaintiff, the defendant did not have the right to extract and use the information that was posted on the social network "VKontakte." It is noteworthy that the focus of the discussion was on the potential commercial opportunities presented by the use and processing of data. To what extent did users who posted information about themselves on a social network understand that they were adding their "brick" to a commercially valuable data array? This question remained open.

The age of digitalization has thus posed new challenges to constitutional and civil law. People, as participants in property and non-property relations, on the one hand, are clearly reluctant to part with privacy, medical, banking and other confidential information; on the other hand, generalized and machine-readable information about the activities of people on the network, their inclinations, preferences, habits, as well as their usual locations and places of residence have commercial value, including for targeted advertising. The commercial demand for information data creates supply. On the one hand, site owners are expected to make increased technical efforts to protect the information provided by users. On the other hand, it takes effort on the part of lawyers to distinguish the legitimate use of user information from the improper use of information. If the development of technical methods of protection is a task for an engineer rather than for a lawyer, then the definition of acceptable forms and methods of protection is a legal task in and of itself.

1. Privacy as a Protected Intangible Personal Good

Privacy is one of the most traditional and essential components of intangible personal benefits. The right to privacy is one of the indispensable foundations of personal well-being, and respect for privacy is a *sine qua non* of a democratic society.

The right to privacy is an absolute subjective civil right. This right covers the physical and psychological integrity of the individual, including the right to live in solitude without attracting unwanted attention.

At the same time, activities of a professional or business nature cannot be completely excluded from the content of private life.

Like any other moral right, the right to privacy may be limited in the name of public interest or to protect a more significant private interest, such as the protection of the right to life or health, and its boundaries in any given dispute are determined by taking into account the nature and value of those interests for the sake of which it is supposed to limit the personal non-property right.

In particular, the free use of a photograph of a person is not allowed as a general rule; the consent of the person depicted is required. However, in certain cases provided for by law, the consent of the person depicted is not required. One of the exceptions is the case when the use of the image is carried out in the interests of the state or public or other public interests (Art. 152.1 of the Civil Code of the Russian Federation). A similar provision is contained in the case law of other countries. For example, the Austrian Supreme Court heard a dispute regarding the use during a newscast of a photograph of a girl who had been abducted and then managed to escape from her abductor. The defendant, in an effort to prove the legitimacy of the use of the photograph, referred to the fact that during the search for the girl, her photograph was widely distributed and published by almost all local media. The court, however, disagreed with these arguments, stating that while the search for the missing girl was ongoing, the use of the photograph was justified by a purpose that was of public significance. Once the girl was found, however, there was no public interest in showing her photograph, and the privacy of the person depicted should certainly not have been compromised. Therefore, the court considered the use of a photograph in a news release without the consent of the person depicted a violation of the personal non-property right of the depicted person.¹

In the era of digitalization, when information is being shared at an increasing rate, personal non-property rights need to be protected in a more effective manner. The fact that information about private life and personal data can be accessed from open sources does not, in and of itself, deprive people of the right to protect their privacy and personal data.

¹ See the details of this argument in Elena A. Ostanina, *Is It Allowed to Quote Photos in Austria? Translation of the Decision of the Supreme Court of Austria Dated 26 Sept. 2017 No. 4 Ob 81/17S and Commentary to It*, 10 Bull. Econ. Just. RF 49 (2018).

2. The Concept of Reasonable Expectations in Relation to the Protection of Privacy

In the legal literature, legitimate expectations are defined as one of the means of legal certainty, as a reaction of the rule of law to the need to protect the rights and legitimate interests of people from potential arbitrariness and abuse that arise in a situation of constant change, including those that are objectively predetermined. Legitimate expectations are an important means of ensuring people's confidence in the law and the courts.² If the legitimate expectations of people are taken into account, it is more likely that a norm that corresponds to legal expectations will operate effectively, not only because it is provided with sanctions but also because it is perceived as fair or even as the only possible option.

What legitimate expectations do people have in the era of digitalization? In sociology, the uneven processes of the digitalization of society are noted.³ The majority of people who have been immersed into the process of digitalization are residents of large cities, and they, as a rule, are accustomed to remaining "unrecognized in the crowd" and disclosing as little information as possible about their private lives. On the other hand, people, who later became involved in the digitalization process, gained access to the already established Internet culture, which allowed them to maintain their anonymity, the ability to use pseudonyms and pictures instead of their own images and other means to distinguish between their own "I" and the character acting online. In other words, the Internet community has developed to a point where there is sufficient respect for privacy. There are, of course, exceptions, such as websites that debate news from the sports or entertainment industries, but even in these cases, the reduction in privacy protection applies only to those whom the European Court of Human Rights once referred to as "faces of modern history." These faces of modern history are actors, writers, politicians, members of the ruling royal families and anyone who has a significant influence on the formation of public opinion. According to the precedent that has been set by the European Court of Human Rights, the activities of influential people in modern history that may have an impact on the life of society may be discussed freely. However, private life events that are not considered significant to society remain the subject of protection and are included in the concept of "privacy."⁴

Furthermore, when many services became available online, consumers typically believed that the personal data they transmitted was protected at least as well as

² Mikhail V. Presnyakov, *The Problem of Substantive Certainty and Constitutional Protection of Social Rights*, 6 Const. & Mun. L. 16 (2020).

³ Olga M. Slepova, *Formation of Adaptive Behavior in Conditions of Deepening Information and Digital Inequality*, Author's review to the thesis of Candidate of Sociology, Penza 8 (2019).

⁴ ECHR Ruling of 24 June 2004 in the case *Von Hannover (Princess of Hannover) (Von Hannover) v. Germany* (complaint No. 59320/00).

if the information were transmitted on paper. When people enter into contractual or public law relationships and exchange information about themselves, they have a legitimate expectation to receive the maximum care from the person who receives, processes and stores the information in digitized form.

Thus, the legitimate expectation of people in relation to the inviolability of their private lives is that both their personal data and their private lives will be protected with the utmost diligence.

The extent to which these legitimate expectations are realized or not realized can be inferred from news reports concerning the “leakage” of certain information about a person.

“In the first half of 2019, the Central Bank found 1.5 thousand ads on the Web for the sale and purchase of databases of personal data of clients of financial institutions,” according to an excerpt from a report by the Royal Bank of Canada (RBC).⁵

According to a 2022 Report on the Study of Leaks of Restricted Access Information:

Almost weekly in the first half of the year, information was published about major leaks from Russian companies and government agencies, including: Russian Railways, the Pobeda airline, the telecommunications companies Rostelecom and VimpelCom, the Ykt.ru information portal, the services of Mir Tesen services, Fotostrana.ru and Text.ru, entertainment resource Pikabu, delivery services Yandex.Food, Delivery Club and 2 Berega, Skolkovo School of Management, educational portal GeekBrains.⁶

Even based on these examples, it is reasonable to conclude that the legitimate expectations of people who entrust information about themselves to the owners of large sites in the process of obtaining entertainment content or Internet services are either not realized or are not sufficiently realized. However, the fact that the protections in place are not as effective as they could be does not indicate that we need new legislation: existing civil law norms (and, in part, some public law norms) make it possible to provide more effective protection of the privacy of people in the digital environment. In the next section, we will consider possible options for interpreting the norms of civil law in order to provide a more serious and thorough protection of the rights of Internet users.

⁵ Число баз данных банковских клиентов на продажу в даркнете упало вдвое // РБК. 21 декабря 2021 г. [*The number of bank customer databases for sale on the dark web has halved*, RBC, 21 December 2021] (Jan. 15, 2023), available at <https://www.rbc.ru/finances/21/12/2021/61c04ef59a79476d4782d2b9>.

⁶ Report on the Study of Leaks of Restricted Access Information in the First Half of 2022, Expert and Analytical Center InfoWatch (2022); see Expert and Analytical Center InfoWatch 2022.

3. Protection of Personal Data

In both public and private law, the instruments for protecting privacy are (a) the institution that receives and holds personal data and (b) the rules on the protection of medical, legal and banking secrecy.

The Russian legislation on the protection of personal data proceeds from the fact that, as a general rule, any action for the processing and storage of personal data requires the consent of the person to whom the personal data relates (Art. 6 of the Law on Personal Data⁷). In this regard, the Russian legislator stands in solidarity with the legislators of the other BRICS countries.

China has specifically adopted laws to protect the personal data of its people, including the Personal Information Protection Law (PIPL), which came into force on 1 November 2021 and the Data Security Law (Data Security Law), which came into force on 1 September 2021. With 1.01 billion Internet users in China, the largest Internet community in the world, the PIPL has the potential to have a significant impact on the protection of personal data. Article 3 of the PIPL provides for the operation of the rules on the processing of personal data not only in the territory of the state, but also in the case when the consumer is located outside of China and the provision of goods or services to individuals is supposed to take place within the borders of China.

In India, a personal data protection bill was submitted by the government to parliament, but the bill was withdrawn for revision in 2022.

In Brazil, the General Data Protection Law was passed in 2019. The body of academic literature has already noted a feature of China's approach to the protection of personal data, which consists in the fact that the theory of identification is used, and personal information is understood as everything that can directly or indirectly identify a person.⁸ The processing of personal data requires the consent of the owner of the personal data (Art. 4 PIPL).

Let us turn our attention to some very successful rules of the new Chinese law (PIPL). Firstly, the legislator emphasizes that the forms of consent and standard contracts providing for the processing of personal data must be understandable to people (Art. 17 PIPL). This requirement deserves support, given that many sites frequently publish standard contracts that are so long that the average user is unlikely to finish reading them.

In addition, it is possible to take note of a beneficial rule regarding the need for an agreement between the persons responsible for processing personal data. According

⁷ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954 [Federal Law No. 152-FZ of 27 July 2006. On Personal Data, Legislation Bulletin of the Russian Federation, 2006, No. 31 (part 1), Art. 3451].

⁸ Ts. Shaoxue, *Administrative and Legal Protection of Personal Data in China: Problems and Solutions*, 12 Admin. L. & Proc. 64 (2020).

to Article 20 of the PIPL, if two or more subjects of professional activity jointly decide on the methods of processing or storing personal data, these persons must determine by mutual agreement the rights and obligations of each, after which they are then jointly and severally liable to the person whose personal data is processed or stored. A person may address the prohibition of further use of personal data to all these subjects, as well as to one of them. This norm seems reasonable due to the fact that multiple subjects can be allowed access to the personal data of a person when carrying out a wide range of activities. With regard to Russian law, the joint and several liability of persons who caused damage during the joint processing or storage of personal data can be justified by applying Article 1080 of the Civil Code.

The Russian legislator supplemented the Civil Code with a norm designed to regulate the relationships among the parties when exchanging information. An agreement by virtue of which the contractor agrees to take certain actions in order to provide certain information to the customer (a contract for the provision of information services) may provide for the obligation of one or both parties not to take certain actions for a predetermined period of time, as a result of which information may be disclosed to a third person (Art. 783.1 of the Civil Code). According to research that has been conducted, relations related to data analytics can be formalized by certain kinds of agreements under which one party transfers a specific set of information to the other party, and the other party, on a reimbursable basis, processes and analyzes such information using various algorithms and then provides a specialized report containing the results of such analytics. In particular, such a model can analyze the data contained in social networks in order to determine consumer sentiment regarding a recently released product. It is important that the person or persons collecting information do not violate the prohibitions established by the law on the protection of personal data.

4. Features of the Protection of Medical Secrets and Other Types of Secrets in the Era of Digitalization

In order to emphasize the particular value of some information related to a person or activity, as well as to emphasize the obligation of those admitted to this information to keep it confidential, the legislation uses the concept of “secret.” Examples of such information include, for example, banking secrecy and medical secrecy.

The secrecy of medical information originates in a special relationship between the patient and the doctor that is based on trust.⁹ The doctor and medical organizations are obliged to maintain medical secrecy since, on the one hand, a patient’s concealment

⁹ Erwin Deutsch & Andreas Spickhoff, *Medizinrecht: Arztrecht, Arzneimittelrecht, Medizinprodukterecht, und Transfusionsrecht* 602 (2014).

of certain information may be detrimental to the patient's health and life and possibly the health of others, and on the other hand, a patient may choose to keep silent about potentially compromising information if he or she is not sure that the doctor will uphold confidentiality. The same trusting relationship between a person and a service provider underlies other forms of secrets, including banking secrecy and notarial secrecy. Since today almost all patient-related information is held in a digitized form, the question arises as to whether a medical institution is responsible if a third party illegally obtains information regarding material constituting a medical secret and stored in a digitized form by a medical organization. A similar question arises in relation to other types of secrets. Is a notary responsible if a third party, using technical knowledge, illegally gains access to digitized information constituting a notarial secret? Is a bank responsible in the case of illegal access to information constituting bank secrecy? In relationships between an organization and a person, the person represents the weaker party, whereas the commercial organization (and occasionally a non-profit organization) is the economically and organizationally stronger party. As a result, it is reasonable for there to be some degree of paternalism in the relationship that exists between the person and the owner of the site.

In addition, a person who entrusts personal information to a commercial or non-profit organization or the owner of the website does not have the opportunity to check how reliable the programs that protect the site from hacking are or how qualified the employees of the organization that owns the site are. As a result, a relationship that is based on trust will be impossible if the patient, consumer, or any other person acting in a different social role cannot expect the most stringent and reliable measures to protect their personal information from the person who accumulates such information constituting a secret.

In this regard, it is unreasonable to require the site owner to take simply the customary measures to protect information constituting a medical or other secret. It is advisable to assign the risks associated with illegal access by third parties to information consisting of banking secrets, medical secrets and other types of secrets to a person who, by virtue of his entrepreneurial or other professional activities, collects or stores that information in digitized form.

As a result, the owner of a website, or any other person, who, by virtue of his or her professional activity, collects or stores information constituting medical, banking or other secrets is responsible for the disclosure of that information and for any illegal access to that information by a third party, regardless of fault.

The legislation of the BRICS countries does not contain detailed rules on imposing the risks of unauthorized access by third parties to information that is stored in digitized form by a subject of professional activity. At the same time, the general rules that state that the subject of professional activity having access to personal information must ensure the security of this information, allow us to draw a conclusion about liability on the basis of the risk involved.

One such provision can be found, for example, in Article 111 of the Civil Code of China, which states:

A natural person's personal information is protected by law. Any organization or individual that needs to access other's personal information must do so in accordance with law and guarantee the safety of such information, and may not illegally collect, use, process, or transmit other's personal information, or illegally trade, provide, or publicize such information [Article 111 Civil Code of the People's Republic of China].¹⁰

In Russian law, a similar general standard is established by the norms establishing the concepts of medical secrecy and banking secrecy, as well as by Article 24 of the Law on Personal Data.

The doctrine recognizes that liability for damage caused by actions that create an increased risk of harm to others is permissible in both public and private interests. First, liability without fault (known as "strict liability" in English-language sources) encourages the person engaging in a potentially harmful activity to take the utmost precautions. Secondly, strict liability provides greater protection for the victim than liability based on guilt.

Responsibility established on the basis of risk (strict liability) for a person who, due to entrepreneurial or professional activities, stores or is responsible for actions related to one or more types of secrets protected by law, can be deduced from a systematic interpretation of the norms of paragraph 3 of Article 401 of the Civil Code and Article 1100 of the Civil Code.

At the same time, the negligence or even the intent of the person to whom the information relates should also not be underestimated. Consider a scenario in which a bank or a medical organization was provided with information about a person, or a person published information about his or her diagnosis and treatment on social networks and later deleted it. Proven gross negligence reduces the amount of damages to be compensated; in other words, if intent is proven to disclose information constituting a medical, banking or other secret, a claim for compensation for damage caused by disclosure may be denied.

¹⁰ Civil Code of the People's Republic of China, adopted at the Third Session of the Thirteenth National People's Congress on 28 May 2020 (Jan. 15, 2023), available at <http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf>.

5. Forms and Methods of Protecting Privacy

5.1. Self-Defense of Personal Non-property Rights

Self-defense measures play an important role in the protection of intangible personal benefits. In the literature, self-defense of civil rights is defined as the actions of people and organizations to protect civil rights and legally protected interests, which are performed by them independently, without seeking help from the state and other competent authorities.¹¹ Self-defense measures include both factual and legal measures.¹²

In the era of digitalization, some of these measures of an actual nature will likely include certain site settings, requirements for posting on the site, registration on the site and so forth.

For example, the site owner may allow comments and reviews only from registered users, and may also require the registration of a real name and surname as well as the submission of documentation proving the identity of the user as prerequisites for registration. This will serve as a sort of self-defense to prevent anonymous users from spreading information determining honor, dignity and business reputation. As examples of typical situations, we can cite the narratives of two different cases considered by the Supreme Court of the Russian Federation.

In the first case, a surgeon demanded that negative reviews written about him be removed from the website of a medical organization. The case was sent for a new trial since the courts could not determine what the attitude of patients were toward the process of conducting surgical operations and their outcomes, whether these events actually took place or not, whether it was their evaluative opinion or a statement of facts, and in the event that they were statements of facts, then whether they were relevant or not corresponding to reality (Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 26 April 2022 No. 5-KG22-28-K2). It was important that the reviewers' identities not be revealed.

In another case (Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 25 May 2021 5-KG21-32-K2, 2-6217/2019), it could not even be established whether the surgeon in question had actually performed any surgical procedures. The case was also sent for further consideration.

Based on the results of the resolution of these disputes, it is clear that site settings that allow only registered users to leave reviews would prevent anonymous reviews (or

¹¹ Igor A. Aksenov, *The Practice of Applying Legislation on the Protection of the Rights and Legitimate Interests of Individuals in the Implementation of Activities for the Repayment of Overdue Debts: Trends and Results*, 4 Bull. Enforcement Proc. 64 (2017).

¹² Andrei A. Gromov, *Commentary to Article 14 of the Civil Code of the Russian Federation*, in Artem G. Karapetov (ed.), *The Main Provisions of Civil Law: Commentary to Articles 1–16.1 of the Civil Code of the Russian Federation* 1469 (2020).

at least reduce the risk of such anonymous reviews) and make it easier to verify whether the doctors actually provided medical care to the persons who left reviews. The reviews would also be more valuable in terms of their relevance in such a situation.

5.2. Compensation for Moral Damage as a Way to Protect the Right to Privacy

For all of the importance of self-defense, the jurisdictional form of protection is more visible to both the right holder and the infringer. In the event that the disclosure of information constituting banking, medical or other secrets causes property damage, the person has the right to demand compensation for the damage caused according to the provisions of Article 15 of the Civil Code.

If, under the circumstances of the case, such a method of protection as a requirement to restore the situation that existed before the violation of the right appears acceptable (for example, changing the information previously entered by the Credit Bureau in the credit history of a person, due to the fact that an unidentified person, using personal information, concluded a contract on behalf of that person), this requirement can also be used. Both the claim for damages and the claim for the restoration of the situation that existed before the violation of the right are claims of a property nature (even if the claim for the restoration of the situation that existed before the violation of the right is not subject to monetary value). In the event that a person incurs no property damage but only moral and physical suffering, the most acceptable method of protection is a claim for compensation for moral damage.

Compensation for moral damage is a central part of the system of methods that are used to protect people's right to privacy.

Compensation for non-pecuniary damage is a legal instrument that gives the necessary completeness to the system of ensuring the security of intangible goods. Even the removal of illegally disseminated information or its refutation will not help a citizen to forget the moral suffering suffered. The experience of experiencing negative emotions is irreversible. Therefore, legal protection against the distortion of a citizen's public assessment and from a negative intrusion into the formation of his self-esteem will not be complete without monetary compensation for the moral suffering that inevitably arises from defamation.¹³

Moral damage is defined as compensation for moral suffering as well as responsibility for moral and physical suffering. It should be noted that the amount of compensation for moral damage depends on the circumstances of the case, including the degree of moral and physical suffering, the duration of the violation and the degree of guilt of the offender.

¹³ Natalia N. Parygina, *Compensation for Moral Damage in Defamation against a Citizen*, 10 Judge 24 (2018).

The problem with Russian judicial practice is that the amount of compensation awarded for moral damage is often insignificant. It is well known that the compensations exacted by the Russian courts are typically modest, especially when there is no evidence of substantial physical harm, but only moral suffering.

The issue of determining the appropriate amount of compensation has been discussed in the practices of the European Court of Human Rights.

The task of calculating the amount of compensation for non-pecuniary damage is complex. It is especially difficult in a case whose subject is personal suffering, physical or moral. There is no standard to measure pain, physical inconvenience, mental suffering and anguish in monetary terms (decision of 18 March 2010 in the case *Maksimov v. Russian Federation* (complaint no. 43233/02)).¹⁴

One possible explanation for the insignificance of compensation in the event of a violation of the right to privacy may be that the amount of the alleged compensation is compared with the compensation already awarded in connection with the injury. Therefore, we can agree that it is necessary to distinguish between moral damage in the strict sense of the word, which occurs when a person's non-property rights are violated, such as the right to a name, image, privacy and the moral (non-property) damage that a person may suffer from an infringement on his life and health.¹⁵

5.3. Possibility of Changing the Protection Method for More Complete Protection

The amount of compensation for non-pecuniary damage should be determined taking into account the personality of the offender. However, the fact is that the amount of compensation is frequently determined without taking into account the economic inequality that exists between those who did not provide proper confidentiality and those who suffered as a result of this lack of confidentiality. In most cases, the amount of compensation will be calculated as if the tortfeasor and the victim were in an equal position and an equal situation. This is a differentiated approach in which the amount of compensation varies depending on the degree and nature of suffering as well as the duration of the offense. However, the identity of the offender is not taken into account. At the same time, neither the current legislation nor the clarifications of the Plenum of the Supreme Court of the Russian Federation prohibit taking into account the economic inequality that exists between the tortfeasor and the victim in order to determine the amount of compensation. This characteristic could be taken into account as "other circumstances." The list of

¹⁴ ECHR Ruling of 18 March 2010 in the case of *Maksimov v. the Russian Federation* (complaint no. 43233/02), 8 Bulletin of the European Court of Human Rights (2010).

¹⁵ Alexandra M. Lobacheva, *Determination of the Amount of Compensation for Moral Damage in Connection with Encroachments on Human Life and Health in France*, 3 Bull. Econ. Just. RF 116 (2020).

circumstances that the court may take into account when determining the amount of compensation in accordance with Article 151 of the Civil Code of the Russian Federation is long.

It is therefore reasonable to assume that the economic inequality between the tortfeasor and the victim must be taken into account. This will prevent subsequent violations and implement the preventive function of civil liability.

The concept of “punitive damages” in the English-language doctrine may serve as a useful guideline in determining the appropriate level of such liability. Punitive damages is an amount of money awarded to the plaintiff in excess of the damage caused to him or her and serves as a punishment against the defendant for especially outrageous behavior.¹⁶ Punitive damages are typically issued when the severity of the offense and the economic inequality between the tortfeasor and the victim induce the court not only to compensate the victim for the damage caused but also to punish the tortfeasor exponentially.

Punitive damages are a well-known theoretical concept in both Russian and foreign civil law. However, attitudes towards this concept vary from country to country. In the US doctrine, the attitude towards the concept of punitive damages is very positive. Punitive damages are used in disputes involving commercial organizations (including cigarette manufacturers, energy supply organizations) and consumers, as well as medical organizations and patients. UK jurisprudence and doctrine have taken a slightly more cautious approach to claims for punitive damages. It is proposed to limit the circumstances under which punitive damages can be recovered.¹⁷ In the French doctrine, the attitude towards punitive damages is even more wary.¹⁸

One advantage of the institution of punitive damages is the more serious protection provided to the victim. Of course, this has to do with the amount of compensation. In addition, the possibility of receiving exemplary increased compensation motivates the lawyer to represent the interests of the victim on the terms of the success fee. Thus, claims for which (without the possibility of recovering punitive damages) the plaintiff could not find a representative turn out to be more promising, and at the same time, the interests of the victim are protected.

The disadvantages of the institution of punitive damages are that, firstly, the most enterprising plaintiff receives protection as if for himself and other victims, while other

¹⁶ Sergey L. Budylin, *Punitive Damages. Now in Russia?*, 4 Bull. Civ. L. 19 (2013).

¹⁷ See Henry N. Butler & Jason S. Johnston, *Reforming State Consumer Protection Liability: An Economic Approach*, (2010) 1 Colum. Bus. L. Rev. 1 (2010).

¹⁸ François-Xavier Licari, *Prendre Les Punitive Damages Au Sérieux: Propos Critiques Sur un Refus d'Accorder l'Exequatur À une Décision Californienne Ayant Alloué des Dommages-Intérêts Punitifs* [Taking Punitive Damages Seriously: Why a French Court Did Not Recognize An American Decision Awarding Punitive Damages and Why it Should Have], 137 J. du Droit Int'l 1230 (2010) (Jan. 15, 2023), available at <https://ssrn.com/abstract=1664350>.

plaintiffs who have not filed a claim do not receive protection. Another drawback of the institution of punitive damages is that the possibility of paying compensation for punitive damages is taken into account by commercial organizations when determining the cost of providing services; in order to redistribute the risk of liability, a liability insurance contract is concluded, which is also taken into account when determining prices under contracts with consumers. Thus, it can be assumed that the possibility of filing a claim for punitive damages may entail a change in the terms of obligations not in favor of the person.

Should the model of punitive damages be used to improve the system of compensation for non-pecuniary damage? In other words, should the amount of compensation for non-pecuniary damage be determined in such a way as to not only compensate for the suffering of the victim but also punish the offender? The doctrine of China, for example, discusses the application of the institution of punitive damages in relations between the tortfeasor and the victim.¹⁹ We do not deny that the institution of punitive damages has its drawbacks; however, the economic disparity between the offender and the victim must be reflected in determining the amount of compensation. In the event that an organization receives and processes personal data, including information constituting medical, banking or other secrets, the organization must make every possible effort to protect that information in a way that ensures its confidentiality.

People have the right to expect that a commercial organization that accumulates, collects, stores or processes information relating to them while carrying out its income-generating activities will make every effort to protect this information. In order to motivate a commercial organization to exert the maximum effort, the risk of paying the customary minimal compensation for non-pecuniary damage is not enough; instead, the amount of compensation should be increased, taking into account the preventive function of civil liability. In this regard, the method of seeking compensation will be based on the model of punitive damages.

Conclusion

In the era of digitalization, people, as a rule, rightly expect that the personal data entrusted to one site will not then be used without restriction by a dozen other websites. In order to ensure the realization of these legitimate expectations, one should treat the obligations of a professional entity (commercial organization, individual entrepreneur or any other person carrying out professional activities) that involve the processing of personal data of a person or receiving information constituting a secret with the same level of strictness as the obligations of a commercial organizations to fulfill contractual obligations to consumers. The

¹⁹ Bu Yuanshi (ed.), *Chinese Civil Law* 164 (2013).

responsibility of the professional for the disclosure of information should be carried out regardless of fault, in accordance with the rules of strict liability. In addition, in the event that a person suffers moral damage as opposed to property damage, the amount of compensation should be determined taking into account the economic inequality between the tortfeasor and the victim and taking into account the preventive function of civil liability. In this case, the claim for compensation for non-pecuniary damage acquires a certain similarity to the claim for punitive damages, since the victim may receive compensation in an amount slightly larger than the suffering the victim has endured. This excess appears to be justified due to the economic and organizational inequality of the subjects of legal relations. People who share personal information with a commercial organization are unable to verify the reliability of the programs and tools that are used by the organization to protect their data. Therefore, the organization must be motivated to take the best possible precautions to protect the privacy of people's personal data, even if these best practices are relatively expensive.

References

- Aksenov I.A. *The Practice of Applying Legislation on the Protection of the Rights and Legitimate Interests of Individuals in the Implementation of Activities for the Repayment of Overdue Debts: Trends and Results*, 4 Bulletin of Enforcement Proceedings 64 (2017).
Bu Y. (ed.). *Chinese Civil Law* (2013).
Budylin S.L. *Punitive Damages. Now in Russia?*, 4 Bulletin of Civil Law 19 (2013).
Butler H.N. & Johnston J.S. *Reforming State Consumer Protection Liability: An Economic Approach*, 2010(1) Columbia Business Law Review 1 (2010). <https://doi.org/10.7916/cblr.v2010i1.2917>
Deutsch E. & Spickhoff A. *Medizinrecht: Arztrecht, Arzneimittelrecht, Medizinprodukte-recht, und Transfusionsrecht* (2014). <https://doi.org/10.1007/978-3-642-38149-2>
Lobacheva A.M. *Determination of the Amount of Compensation for Moral Damage in Connection with Encroachments on Human Life and Health in France*, 3 Bulletin of Economic Justice of the Russian Federation 116 (2020).
Ostanina E.A. *Is It Allowed to Quote Photos in Austria? Translation of the Decision of the Supreme Court of Austria Dated 26 Sept. 2017 No. 4 Ob 81/17S and Commentary to It*, 10 Bulletin of Economic Justice of the Russian Federation 49 (2018).
Parygina N.N. *Compensation for Moral Damage in Defamation against a Citizen*, 10 Judge 24 (2018).
Presnyakov M.V. *The Problem of Substantive Certainty and Constitutional Protection of Social Rights*, 6 Constitutional and Municipal Law 16 (2020).

Information about the authors

Elena Ostanina (Chelyabinsk, Russia) – Head, Department of Civil Law and Procedure, Chelyabinsk State University (129 Bratiev Kashirinykh St., Chelyabinsk, 454001, Russia; e-mail: elenaostanina@mail.ru).

Elena Titova (Chelyabinsk, Russia) – Director, Institute of Law, South Ural State University (National Research University) (47a Elektrostalskaya St., Chelyabinsk, 454038, Russia; e-mail: titovaev@susu.ru).