Fighting against violations of the right to privacy in the virtual space: Ensuring the security of personal data

E. A. Humbatov

Baku State University,
23, ul. Zahida Khalilova, Baku, AZ 1148, Republic of Azerbaijan

For citation: Humbatov, Elnur A. 2024. "Fighting against violations of the right to privacy in the virtual space: Ensuring the security of personal data". *Vestnik of Saint Petersburg University. Law* 3: 654–664. https://doi.org/10.21638/spbu14.2024.307

In the article, the legal regulations on the fight against violations of the right to privacy in the virtual space and ensuring the security of personal data were studied. The formation of the global information society, the transformation of the Internet into an integral part of social life was observed with the increase of people's activity in the virtual space. On the one hand, it is characterized by positive aspects. Because in the virtual space, any person can easily meet the needs of daily life by using the opportunities provided as a user. For example, online shopping, online communication, searching for desired information in virtual space, etc. But on the other hand, the borderless nature of the virtual space, the use of anonymity (for example, through a fake profile) makes it difficult to detect and prevent violations committed in this space. In general, this raises the issue of protecting human rights and freedoms in the digital age, and among these rights and freedoms, the right to privacy has a special weight. Because people who use the virtual space provide their personal information to various platforms, or during communication, their personal life information remains in the virtual space, so that such information can later be used by criminals for illegal purposes. Therefore, protecting the security, confidentiality and completeness of information about personal and family life in the modern era is one of the most important tasks facing the world community. The author provided information about the most common types of violations of the right to personal integrity in the virtual space, and presented his suggestions on measures to combat them. In addition, the article analyzes the differences between the Anglo-Saxon and the European practice of personal data protection and draws conclusions about more successful practices.

Keywords: virtual space, right to privacy, personal data, confidentiality, integrity, availability, domain name, e-mail, spam, big data.

1. Introduction

The right to privacy, which was first mentioned in the famous article of 1890 by Samuel Warren and Brandeis (Rzayeva, Ibrahimova 2021, 104), is one of the rights that should be protected more in modern times. Because the formation of the virtual space, the lack of clarity of the boundaries of the Internet leads to the dissemination of information about the personal and family life of others at any time, as well as disclosure to third parties as a result of the failure to ensure the confidentiality of personal data provided during the use of the virtual space.

One of the main reasons for the increase in the violation of the right to privacy in the virtual space stems from the freedom that the Internet offers to its users. So, a person who violates the rights of others can easily hide in this space. Because there are still international problems such as determining the identity of the criminal. Along with technological developments, the personal values that constitute the rights of individuals change over time, so the types of violations of the right to privacy that occur on the Internet also change over time.

Personal information on the Internet is collected and stored by both public authorities and the private sector for a variety of legitimate purposes. Subsequently, many important decisions about the person are made based on that information. Therefore, it is important to keep personal data accurate, reliable and undistorted. In addition, keeping personal data in the system for an unnecessarily long time also goes against many rights (for example, the right to be forgotten).

Traditionally, the right to privacy has been analyzed in relation to a specific individual. But who is meant by a person in a virtual space or virtual world? — The concept of digital person or electronic person, which began to be discussed with the spread of Web 2.0 platforms, continues with the development of artificial intelligence, and continues to be discussed in the context of avatars with the application of Web 3.0 platforms, is one of the most discussed topics of our time.

2. Basic research

2.1. Classification of violations of the right to privacy in virtual space

The right to privacy in the virtual space can be violated in two cases: violations by the users themselves against other users or third parties who are not users of the virtual space; as a result of insufficient security in the virtual space and the commission of cybercrimes.

Although Web 3.0 platforms are blockchain-based and appear to be areas where people freely produce and consume content in a decentralized structure, one of the limitations of this freedom in the legal system is to respect the rights and freedoms of others. Thus, users can enter the educational areas, socializing areas, concerts, festive events, culture and art exhibition areas, and playgrounds provided by the virtual space platforms with their avatars and use the content presented to them. The interaction of users' avatars with other avatars while enjoying these contents, behavior and mobility while consuming the contents may be limited by the platform. In the virtual world, the user also has the opportunity to create his own content by purchasing a domain registered on the blockchain. Among the rules that the user must follow when creating this content, it is prohibited to post content that violates the right to privacy of others: create an avatar using someone else's name or image so that other users can see it; to do actions that harm the honor and dignity of the person with the created avatar; post information about someone else's personal life in the content; to reveal the activities of another user's avatar in the virtual space without his permission and knowledge, etc.

Here we have to take into account whether the owner of the information about personal and family life is a public person. Going public will naturally limit the area of private life. In short, the privacy of a person's private life is limited by its disclosure to the public. For example, the personal life of politicians and artists is limited by their recognition by society.

Of course, this does not mean that their private lives are completely disclosed, the limits of the right to private life to be protected will be determined by the judge for each specific case according to their life experiences. In addition, the published information about these persons must be true and there must be a connection between the publicity of that person and the disclosed events related to his private life. The information disclosed must be significant in terms of the person's status in public life. Information about employees of state bodies is often published in the press. This is a normal situation. Because the main task of the media is to inform the society. However, this does not give the media a reason to publicize all the details of the personal and family lives of those persons. Article 21 of the Law on Media[1] does not specify publicly known persons as an exception, and Art. 14.1.8 prohibits the dissemination of information directly related to personal and family life.

As we mentioned, the second case of violations is related to the lack of full security. Although the security policy is considered one of the important elements in the service contracts related to the virtual world, failure to ensure the completeness, confidentiality and availability of data in many cases leads to the non-protection of personal data, as well as to the commission of cybercrimes. Here we should mention software that is hidden in useful programs or hidden as another file. For example, software such as Trojan horse software and chameleon are added to the useful software that most computer users would want to have and then start damaging the system (Dulger 2004, 38). Chameleon records the names and passwords of all users in the system in its secret file. It then sends a message that the system will be temporarily shut down for maintenance. In doing so, the person using this software accesses the said secret file and obtains the usernames and passwords of the users.

In addition to recording and listening to people's conversations in electronic environments, with the possibilities provided by the Internet infrastructure and social media, it can also be used on social platforms such as Instagram* and Facebook*. Providing it to other parties on metaverse platforms such as Decentraland, Sandbox, GoArt is also a violation of the right to privacy.

According to the generalization of legal regulation and doctrine, internal and external threats to the right to privacy in virtual spaces can be distinguished. Internal threats are committed from within the virtual world, either by users or by entities that control the operation of the platform. External threats include violations committed by persons outside the virtual world (for example, hackers).

2.2. Specific types of violations of the right to personal integrity in virtual space and combating them

Cases of violation of the right to privacy in virtual space vary depending on the personal information included in the content of this right. The current paragraph will address specific types of infringement of personal rights through domain names, e-mail, spamming, and postings on websites.

First of all, we would like to address the issues related to the person's name and surname. As mentioned, domain names are one of the important elements for virtual space. In many cases, the choice of domain names violates the privacy rights of other people by using

[1] Law of the Republic of Azerbaijan on Media. Accessed August 9, 2024. https://e-qanun.az/framework/49124. (In Azerbaijani)

* Meta is recognized as an extremist organization in the Russian Federation.

their names. Domain name protection is provided differently in each state. In Germany, for example, a domain name is legally protected by provisions relating to the right to privacy (Topaloglu 2005, 159). In the United States and the United Kingdom, this protection is mostly provided under the rules governing trademark law (Topaloglu 2005, 159)[2]. Although there is a regulation regarding trademarks in Azerbaijan (Law on Trademarks and Geographical Indications, Art. 32)[3], it is not allowed to use the name, surname or pseudonym of a well-known person in connection with the use of another person's name[4].

A person can use a third party name that has nothing to do with him as a domain name. In particular, the names of famous people are registered as domain names for racist propaganda and pornographic sites. How is the issue of liability resolved in such cases? The point is that the information posted on the websites www.whois.az and online.az about obtaining a domain name is incomplete. It is impossible to know concretely what is included in the Stoplist reflected in Art. 4.3 of the aforementioned Rules. Additionally, another type of domain name dispute arises when more than one person or entity wants to rightfully use the name. For example, when two people with the same first and last name want to open a site under their own names, or when two companies with different registration regions want to open a site under their own names, such a problem can arise. Domain names are unique, meaning that a registered domain name cannot be registered a second time. Since the domain name system, which is inherent in Internet law, applies the principle of "first come, first served", it is not possible to achieve a fair solution in all cases. In such cases, it should be determined which name has the right of priority, or if there is a danger of confusing the other name, this danger should be eliminated. In other words, when there are competing rights over domain names, the domain name should be allocated according to the principle of superior rights, not the principle of priority (Memish 2001, 515).

It should be noted that gaps and deficiencies in domain name registration can increase the number of violations of intellectual property rights and cybersquatting. Cybersquatting is generally the malicious registration of someone else's trademark on a domain name. Eliminating the inaccuracy in the definition of liability in the mentioned Rules can be a successful way to prevent the listed violations.

Illegal acquisition of domain names often leads to violations of intellectual property rights. In this regard, the domain name (gidasa.com) requested by Sabancı Holding to be returned was given by Tucows, one of the accredited organizations of ICANN (Internet Corporation for Assigned Names and Numbers), to a Turkish engineering student who received a doctorate degree at the University of Indiana, USA, prior to the application. At the date of the decision, the expression SA (Sabancı) is in the logo of Sabancı Holding and is registered as a trademark in Turkey and the European Union. On that date, Holding's company Gıdasa San and Tic. Inc. (Gıdasa Sabanci), which sells food products to Turkey and the world was also operating. In March 2003, Sabancı Holding decided to register the gidasa.com domain name, but it was announced that the said domain name was already in use and that the domain name was put up for sale on a website with that name. In accord-

[2] "Domain names and trademark law". *FindLaw.* 2024. Accessed August 6, 2024. https://www.findlaw.com/smallbusiness/intellectual-property/domain-names-and-trademark-law.html.

[3] Law of the Republic of Azerbaijan on Trademarks and Geographical Indications. Accessed August 9, 2024. https://e-qanun.az/framework/3293. (In Azerbaijani)

[4] Rules for registration and use of top-level domain names with country code "az", approved by Resolution No. 63 of the Cabinet of Ministers of the Republic of Azerbaijan dated February 25, 2019, Art. 4.3. Accessed August 9, 2024. https://e-qanun.az/framework/41574. (In Azerbaijani)

ance with the current regulations, Sabancı Holding's lawyers notified cikibas@indiana.edu that Sabancı's trademark rights were violated by the said domain name and that the domain name should be transferred to Sabancı Holding, but no results were obtained as a result of mutual correspondence. As a result, the Holding applied to the WIPO (World Intellectual Property Organization). In the decision, it was stated that the sale of the domain name by the domain name owner in accordance with Art. 4 of the Uniform Domain Name Dispute Resolution Policy (UDRP)[5] is a sign of bad faith, that Sabancı's SA logo is known worldwide, and that the domain name owner is also aware of it, therefore it was decided to return to the holding the domain name Sabancı Holding[6].

Violation of the right to privacy by using e-mail. Electronic mail is a letter sent to its addressee through electronic carriers. There may be some difficulties in proving a violation of the right to privacy by sending e-mails. Internet service providers or service providers that offer email services can detect a computer's IP address. However, even if the IP number is identified, it is possible to send e-mail through other computers using Trojan horses or similar malware. In this case, determining from which computer the IP address from which the e-mail was sent does not allow the identification of the actual sender of the e-mail.

The unauthorized access or reading of a person's e-mail or the monitoring of a person's e-mail traffic is a violation of the right to privacy. But is it a violation to monitor what is sent and received from the person's e-mail at the organization where he works? Since there is no direct legal regulation on this issue, it is necessary to draw a conclusion based on general provisions. Accordingly, it would not be illegal to monitor an employee's e-mail and Internet use only if the quality of the job warrants it and the employee's consent is obtained (Erdemir 2019, 75). However, it is important not to disclose personal information known to the employer at this time. The point is that the protection of the right to privacy is not established as a principle in the Labor Code of Azerbaijan[7]. Although the employer's obligation to protect commercial secrets is imposed (Art. 10 (d), 72 (d) of the Labor Code), the employer's duty to protect the confidentiality of the employee's personal information is not defined. Even, none of the actions listed in the Note part of Art. 290 regarding moral damage can be considered as a violation of the right to personal integrity. Therefore, if the employer shares the employee's personal data without his permission, he will be held liable in general manner. When it comes to whether e-mail data and correspondence fall within the scope of the right to privacy, correspondence is unequivocally considered personal information. If we comment with reference to Art. 2 of the Law on Personal Data[8], since e-mail data are considered personal data, their illegal acquisition will be considered an infringement of the right to privacy.

It is also possible to obtain personal information by sending spam emails and using various malicious programs when the email is opened, which is considered an invasion of personal life. It is no coincidence that cyberbullying, which manifests itself in different

[5] "Uniform Domain Name Dispute Resolution Policy (UDRP)". *Internet Corporation for Assigned Names and Numbers.* Accessed August 9, 2024. https://www.icann.org/resources/pages/help/dndr/udrp-en.

[6] "WIPO Arbitration and Mediation Center, Administrative panel decision, Sabanci v. iu, Case No. D2003-0498". *World Intellectual Property Organization.* 2023. Accessed August 6, 2024. https://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0498.html.

[7] Labor Code of the Republic of Azerbaijan. Accessed August 9, 2024. https://e-qanun.az/framework/46943. (In Azerbaijani)

[8] Law of the Republic of Azerbaijan on Personal Data. Accessed August 9, 2024. https://e-qanun.az/framework/19675. (In Azerbaijani)

forms in parallel with the development of technologies, is one of the most common cases of interference in personal life. Cyberbullying is behavior by one person or group that systematically harms or harasses another person or group over the Internet or other communication technologies. Cyberbullying is a type of attack that is difficult to detect because it takes place on the Internet and is often perpetrated using fake accounts. Since such actions are considered cybercrimes, we will not interpret them so broadly. A detailed classification of these crimes is given in Shinder's presentation (Shinder 2002), and most scholars (Gorodov 2012; Bachilo 2013; Bachilo, Lapina 2016) who have conducted research in the field of information law have referred to that classification.

2.3. Ensuring the security of personal data in virtual space: Legal measures

Due to the rapid development of information systems, it is both important and difficult for legal regulations to quickly adapt to these developments. Big data applications, which find patterns among our digital footprints containing our personal data and perform analysis to generate highly probable predictions using artificial intelligence, accompanied by advances in information science, have many benefits as well as disadvantages for society. As the virtual space is already a large source of information that can be used for many purposes in ways developed by information professionals, it is increasingly difficult to maintain a balance between the personal and public interest in the security of personal data and security and confidentiality. However, we must bear in mind that legal regulations and cyber security measures alone cannot be the solution. The most important problem in the field of personal data protection is that individuals do not have enough information about the conditions under which the personal data they provide or voluntarily share in the virtual space is protected and for what purposes it is used.

In this context, giving up social media tools or living a life completely away from the technology of the time to escape the dangers is not a realistic approach. The fact that the data in the digital world has a great economic value, the requirement to share personal data and record them in digital systems in order to benefit from many services, and most importantly, the use of social media becoming a part of our life as a form of socialization have made it almost impossible to live an analog life away from it all. Lökke notes that in the 21st century, especially with our smartphones, leaving this system where we constantly release personal information into the digital environment will be considered a dubious act, and people who make such a choice will wonder if they have something to hide, and they will even attract the skeptical attention of the state or institutions (Løkke 2018, 11–12).

In today's world, even after meeting in the real world, the first step people take to solidify their feelings is to look at each other's social media accounts. Just as it has become common for us to convert moments related to our personal lives into data and transfer them visually and aurally to the virtual world on social media, it has become impossible for people to live in isolation from technology without using social media at all.

Personal data is used to refer to all information about individuals with specific or identifiable characteristics that cannot be accessed, used, reproduced or otherwise processed by others without the permission and knowledge of the owner. The scope of personal data is determined by the Law on Personal Data in national law.

Due to the gradual disappearance of confidentiality along with digitization and the consequences of technology-society interaction, the need to recognize and guarantee the right to personal data protection as a human right in itself has emerged.

With the creation of three-dimensional virtual environments, problems related to the protection of personal information on the Internet began to be discussed. There are two types of information in virtual space: information taken from the real world and displayed in virtual space; information about avatars, digital objects and services presented in the virtual space.

The virtual space, which provides users with a three-dimensional digital living space, contains a lot of personal information such as a person's name, picture, phone number, contact information, communication traffic data and habits. Currently, wearable technologies such as augmented reality-based contact lenses, clothing and gloves that provide heat and touch sensations are rapidly developing, especially with the introduction of three-dimensional virtual environments into our lives, through which eye movements, facial expressions and body temperature, heart rate and pulse data can be collected. Failure to fully ensure the security of all these personal data leads to their use for various illegal purposes. Such illegitimate purposes result in a violation of the right to privacy. However, assessing the legality of violations of the right to privacy in the virtual space has different aspects compared to violations committed in the physical world. At this time, it is necessary to examine the reasons for compliance from the point of view of the virtual space operator, user and third parties.

By giving confirmation when registering on the platform, the user generally accepts the terms of use of the platform, the scope of responsibility, the use of cryptocurrencies, payment terms, and so on are deemed to have accepted all such conditions. So, the person's consent is the most important point here. The expression of consent given must be within the framework of morality and must be clearly stated.

In cases of violation of the right to privacy in virtual space, the location of the violation is not limited to a specific geography. It is possible to commit various legal violations by accessing the Internet from devices with Internet access from anywhere in the world. Thus, there may be difficulties in determining the place where the violation took place and the identity of the person who committed the act. From this point of view, physical, digital and phygital liability are distinguished in violation situations. The final result ends with the determination of physical responsibility. However, until this result, digital responsibility is formed for any violation committed in the virtual space, and this form of responsibility continues until the real owner of a specific avatar is determined. Phygital responsibility (formed as a result of combining the words physical and digital) is formed by the influence of the virtual space as a transition to the physical world. For example, electronic devices already answer the questions we ask like ordinary people, which in itself is phygitalization.

The following principles should be followed when determining the scope and limits of physical responsibility, digital responsibility and phygital responsibility within the framework of a digital or electronic person:

— avatars in virtual universes should be designed in such a way that they do not harm a real person;

— in cases where there is no damage felt by a real person in the physical world, the responsibility should be determined within the framework of a digital or electronic person, keeping the veil of anonymity;

— unlimited liability should not be provided for technology producers.

At the end of every operation carried out in the digital environment, some kind of data record remains. The continuous production of a wide variety of large volumes of data from many different sources has given rise to the concept of Big Data. Big data is a collection of structured, semi-structured and unstructured data produced in high volume, speed and variety.

There are three main concepts (3 V's — volume, velocity, variety) that define big data: volume, velocity and variety. Big data reaches levels beyond terabytes and petabytes that cannot be stored in existing databases and cannot be processed by traditional data analysis methods. Therefore, storing and retrieving data requires innovative tools. Because the speed of production of big data is very high, the processes that will process and analyze this data must also be at the same speed as the production of big data. Therefore, speed is a very important factor for big data. Information is now presented on social media in non-traditional forms such as video, text, pdf and graphics, as well as through technology such as wearable devices. All these conditions the diversity of big data[9].

The success of big data analytics lies not in how much data is stored, but in its ability to analyze and predict behavior and patterns to generate information or knowledge. One of the best examples of this can be seen in a study done by doctor John Snow in the 19th century. In the 1854 plague epidemic in London, Snow determined that the source of the outbreak was a water pump on Broad Street, thanks to his analysis of the detailed mapping he created by scanning the outbreaks of the disease[10].

With the formation of big data, the issue of personal data security has come to the fore again. This is due to the application of the anonymization method. Anonymization is a process of applying technologies in the form of data aggregation or other forms to make it difficult to identify the data owner. In the Law on Personal Data, this process is recognized as anonymization and is the transformation of personal data into such a state that the identity of the data subject cannot be determined. For example, creating a code number instead of a person's first and last name is anonymized data. However, complete and irreversible anonymization of personal data seems almost impossible. Using big data techniques such as data mining, it is possible to combine data sets from different sources and create personally identifiable information (Akinci 2019, 36). Therefore, anonymized data can be retrieved when matched with other data sets using various methods. In particular, we should consider that big data uses multiple data sources and data is transferred to third parties. In this case, even if anonymized, the data remains with third parties. Therefore, in our opinion, anonymization is more valid for official websites and sources. For example, on the Unified Judicial Portal, court decisions are anonymized and placed on the site. However, no one guarantees that any case related to those decisions did not arouse interest in the public, so that news about it was not published during the court proceedings. Thus, anonymizing the court decision in that case does not deprive people of the opportunity to compare that decision with existing news.

[9] 3 V's (volume, velocity and variety). Accessed August 6, 2024. https://www.techtarget.com/whatis/definition/3Vs.

[10] John Snow: Data Cruncher and Public Health Crusader. Accessed August 6, 2024. https://www.historyofdatascience.com/john-snow-data-cruncher-and-public-health-crusader.

2.4. Current facts and case law

The need to protect our personal data or to monitor our personal data for public safety creates a security-privacy dilemma in data privacy. The event that shook the world agenda in 2013 and is called the Snowden incident or the US National Security Agency (NSA) scandal[11] is another very important incident that should be taken into account regarding the security of personal data in social media. Edward Snowden, a security expert at the US NSA and an agent at the CIA, disclosed the secret documents of the NSA and stated that he made observations using a program called Prizma, which provided direct access to information belonging to Google, Facebook*, Apple and other US companies for this intelligence agency. There are very interesting court cases in the US practice regarding the protection of the right to privacy in virtual space. First of all, let's note that the emergence of the right to privacy in the modern sense in the United States was related to the case of Griswold v. Connecticut in 1965[12]. Next, let's take a closer look at the Katz v. United States case[13], since it is purely about information transmission and falls within the scope of our research topic. In the case, Katz was charged with illegal transmission of information. The evidence underlying the indictment was obtained by Federal agents attaching a listening device to the outside of a public phone booth used by Katz. Katz appealed against the evidence, arguing that it was unfair to be charged based on it. The Court of Appeal rejected the appeal, noting that there was no physical interference with the phone booth itself. This laid the foundation for the Katz test of reasonable expectation of privacy, which has been invoked in subsequent court cases.

In the 2013 case Clapper v. Amnesty International[14], members of the press, lawyers, and non-governmental organizations challenged the Foreign Intelligence Surveillance Act (FISA) for electronic surveillance of non-US citizens abroad for intelligence purposes, arguing that it was unconstitutional. The District Court for the Southern District of New York granted summary judgment for the government, finding that the groups lacked standing to state their objections. The groups feared only abstract subjective surveillance and provided no evidence that they were subject to FISA. The U.S. Court of Appeals for the Second Circuit stated that the damage must be specific, actual, or imminent in order to establish a third article condition. The Court of Appeal overturned the decision that there was a reasonable fear of damage or expense to prevent such damage. However, the Supreme Court has held that potential future surveillance will not constitute the harm required by Art. III. This should of course be expected. It was determined that the Court of Appeals had not correctly adopted such a position in its previous decision, that such a decision would nullify the basic requirements of the third article.

---

[11] Edward Snowden: the whistleblower behind the NSA surveillance revelations. Accessed August 6, 2024. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[12] "Griswold v. Connecticut, 381 U.S.479" (1965). *Justia*. Accessed August 6, 2024. https://supreme.justia.com/cases/federal/us/381/479.

[13] "Katz v. United States, 389 U.S.347" (1967). *Justia*. Accessed August 6, 2024. https://supreme.justia.com/cases/federal/us/389/347.

[14] "Clapper v. Amnesty International USA". *Oyez*. Accessed August 6, 2024. https://www.oyez.org/cases/2012/11-1025.

* Meta is recognized as an extremist organization in the Russian Federation.

In the same year as Clapper, a federal court ruled against the mass collection of metadata by the United States. Thus, in Klayman v. Obama[15], the District Court of Columbia ruled in favor of the plaintiffs based on Katz's reasonable expectation test. Although the court also cited the Clapper case to demonstrate foreseeable damage, it concluded that the case was not identical because the plaintiffs could prove that their data had been collected.

In later cases, the issue of concreteness of already inflicted damage was brought to the center of attention, such concreteness was also emphasized in the Clapper case. For example, in the 2016 Supreme Court case Spokeo Inc. v. Robins[16], Spokeo had a website that provided personal information about individuals, such as a people search engine, contact information, and current professional statuses. Robins was one of those whose information was misrepresented through the website. He sued on behalf of himself and others who suffered from similar inaccuracies. Although the district court dismissed the case based on the standing doctrine, the Court of Appeals overturned the finding of actual damage, stating that the specific damage must be de facto, meaning that it exists in reality even if it is not directly felt.

Unlike the concreteness and inevitability criteria applied in the Anglo-Saxon system, since the right to personal integrity is recognized by convention in Europe (Art. 8 of the European Convention)[17], the ECtHR (European Court of Human Rights) has defined criteria and principles for the application of Art. 8 in its cases. Most of the court's early cases (Ben Faiza v. France[18], Centrum for För Rättvisa v. Sweden[19], Big Brother Watch and others v. United Kingdom[20]) concerned the surveillance of individuals through telecommunications, including the Internet. Simply because such surveillance aims to trace and detect crime, the ECtHR emphasized the discretionary powers of the state in protecting national security, taking into account the modern threats of global terrorism and serious cross-border crimes. In subsequent periods, most of the Court's cases regarding the violation of the right to privacy in virtual space have been interpreted in the context of Art. 10 and 8 of the European Convention.

3. Conclusions

The unlimited freedom of virtual space causes some users to behave unethically. Thus, with fake names and profiles on social media platforms, the right to privacy of individuals is violated, misconceptions are formed in the society, information and documents are shared without permission, ethical behavior such as swearing, insults, threats, discrimination, slander, blackmail, commercial and political manipulations and fraud is

[15] "Klayman v. Obama, 957 F.Supp. 2d 1" (2013). *Casetext*. Accessed August 6, 2024. https://casetext.com/case/klayman-v-obama-1.

[16] "Spokeo, Inc. v. Robins, 578 U.S., No. 13–1339" (2016). *Justia*. Accessed August 6, 2024. https://supreme.justia.com/cases/federal/us/578/13-1339.

[17] "European Convention on Human Rights" (1950). *European Court of Human Rights.* Accessed August 9, 2024. https://www.echr.coe.int/documents/d/echr/Convention_ENG/.

[18] "Ben Faiza v. France, Application no. 31446/12" (8 February 2018). *European Court of Human Rights.* Accessed August 6, 2024. https://hudoc.echr.coe.int/eng{%22itemid%22:[%22001-180802%22]}.

[19] "Centrum för Rättvisa v. Sweden, Application no. 35252/08" (19 June 2018). *European Court of Human Rights* Accessed August 6, 2024. https://hudoc.echr.coe.int/fre{%22itemid%22:[%22001-210078%22]}.

[20] "Big Brother Watch and Others v. The United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15" (13 September 2018). *European Court of Human Rights* Accessed August 6, 2024. https://hudoc.echr.coe.int/fre{%22itemid%22:[%22001-210077%22]}.

allowed. All this requires the strengthening of control over the activity of social network platforms, the domestic application of sanctions for the violation of human rights and freedoms in social networks, as well as the prevention of violations in advance by defining precise regulations and standards for the creation and operation of social networks.

One of the current problems related to the protection of human rights and freedoms in the virtual space manifests itself in the form of violation of personal integrity and intellectual property rights during the registration of domain names. So, there are the following disadvantages related to the registration of domain names in our republic: Firstly, since there are no restrictions on the use of other people's names and surnames during domain name registration (only well-known persons are restricted), a domain name can be created with any name, and at this time National administrator and registrar shall have no responsibility if a domain name is created using the name of a celebrity, even if the restriction is stipulated. Because the Rules of February 25, 2019 place the responsibility to other persons directly on the customer during the selection of the domain name (clause 4.7). This means that there is no mechanism for checking the validity and correctness of these names. The same situation exists when using a trademark in a domain name. This will lead to an increasing number of cybersquatting cases in our country. Therefore, a unified policy on the fight against the seizure of domain names should be developed, as well as the Stop-list should be clearly defined. For example, domain names can be accurately analyzed based on identifiable information (IP address, e-mail, address, first name, last name, etc.) and then allowed to be registered. This will also serve to prevent legal disputes due to infringement later.

References

Akinci, Ayshe N. 2019. *Büyük veri uygulamalarında kişisel veri mahremiyeti*. Specialization Thesis. Ankara.

Bachilo, Illaria L. 2013. *Information law*. 2nd ed., rev. Moscow, Iurait Publ. (In Russian)

Bachilo, Illaria L., Marina A. Lapina. 2016. *Actual problems of information law*. Moscow, Iustitsia Publ. (In Russian)

Dulger, Murat V. 2004. *Bilişim Suçları.* Ankara, Select Publ.

Erdemir, Irem. 2019. *Kişilik hakkının internet ortamında ihlali.* Ankara, Select Publ.

Gorodov, Oleg A. 2012. *Information law*. Moscow, Prospekt Publ. (In Russian)

Løkke, Eirik. 2018. *Mahremiyet: Dijital Toplumda Özel Hayat*. Istanbul, Koch University Publ.

Memish, Tekin. 2001. "Legal issues arising around domain names". *Bilişim Toplumuna Giderken Psikoloji, Sosyoloji ve Hukukta Etkiler Sempozyumu*, 513–527. Ankara.

Rzayeva, Gulnaz, Aydin Ibrahimova. 2021. *Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi.* Baku, Nurlar Publ. (In Azerbaijani)

Shinder, Debra L. 2002. *Scene of the cybercrime*. Canada, Syngress Publ.

Topaloglu, Mustafa. 2005. *Bilişim Hukuku.* Karahan Bookstore, Adana.

Received: April 16, 2024
Accepted: June 4, 2024

Author's information:

Elnur A. Humbatov — PhD in Law; elnur_88@inbox.ru