# User self-protection strategies of digital freedom

*Julia* Andreeva[1*], *Margarita* Mihaylova[1], *Irina* Nezhelskaya[2], and *Yana* Chizhkova [1]

[1]Kazan (Volga) Federal University, 35 Kremlyovskaya Str., 420008, Kazan, Russia
[2]Public Relations Department of the Ministry of Internal Affairs for the Republic of Tatarstan, 19 Dzerzhinskogo Str., 420111, Kazan, Russia

**Abstract.** In the context of the tumultuous development of the information field which is spinning out of control of social systems, the threat over the individual information space is increasing; the loss of privacy, which arose due to the deep digital footprint, leads to the violation of personal boundaries and human safety. Digital freedom is increasingly perceived as an opportunity to protect personal space in the virtual world. 'Cybercrime' is growing largely due to the openness of the information field. The objective of this study was to identify strategies of human coadaptation to the occurring transformations of the information field and self-protection of 'digital freedom'. The conducted experiment proved that digital freedom is associated with freedom from total digital control of actions (64%), as well as the possibility to perform any actions online (57%) and openly express one's opinion (33%). The majority of respondents (74%) indicates that self-protection strategies come down to the law-abiding or compliance with general rules; 61% and 60% of respondents, respectively, identify the tactics of attempting anonymity or misrepresenting digital footprint data as effective self-defense strategies; 48% of respondents assert that the most effective self-protection tactic is to anticipate potential consequences. The article also presents review of real cases of the criminological situation in the Republic of Tatarstan in the field of cybercrime and provides data from expert interviews.



## 1 Introduction

The digital realm is becoming the epicenter of all events, pivotal socialization processes and human activity within society. It is in the virtual space the criminality has migrated, rendering the application of self-defense strategies increasingly relevant. Only in 2023, Roskomnadzor documented 168 data breaches, exposing over 300 million records to public access. The proportion of "cybercrime" in the Russian Federation has escalated by more than 30% annually. Over half of these incidents involve fraud utilizing the "digital footprint"—personal data of the victims. According to Igor Ashmanov, President of the Human Rights, at a round-table discussion on "Protecting the Rights and Freedoms of Citizens in the Context of Digitalization,": "Over the past five years, financial losses due to

* Corresponding author: chukarina95@inbox.ru

cybercrime have amounted to approximately 500 billion rubles." [1]. A.E. Postnikova, Doctor of Law, expresses the opinion that: "Digital threats are becoming both irreversible and global in nature. For instance, the benefits of online banking and electronic real estate registries are overshadowed by the threats of fraud involving deposits, real estate, and total control over all financial transactions. The nature of risks and their degree of danger are not fully recognized by a vast number of people, who become victims of professional and creative criminals." [2]. The attitude of Russian state institutions towards the information environment at the beginning of the new century was characterized as spontaneous and poorly regulated. However, in recent years, there has been a trend towards increased state oversight and control in this area, driven by the need to protect state interests.

The scale of the digital world is so vast that controlling information "freedom" becomes a task for both corporations and individual citizens. According to forecasts from International Data Corporation (IDC), a global market intelligence firm for the information technology and telecommunications industries, by 2025, the volume of information on the internet will reach 163 zettabytes. The need for protecting both personal data and confidential state and commercial data is growing. Civilization stands on the threshold of a new paradox, where ensuring human freedom in a world of machines will be entrusted to the machines themselves (artificial intelligence). Research on this global and multifaceted topic can only rely on an interdisciplinary approach. In this study, the multidimensional concept of "digital freedom" will be examined from the perspective of individual information strategies: coping strategies for managing the digital footprint. It is these self-defense strategies for personal data, conscious management of the user's information behavior as a participant in the information field, that become a guarantee of digital freedom.

A survey conducted on behalf of the BBC World Service in 2009-2010 (27,973 respondents in 26 countries) by the international polling company GlobeScan, using telephone and in-person interviews, revealed that people worldwide view access to the internet as a fundamental right, a force for good, and a majority of them do not want governments to regulate it: "78% of internet users believe the internet has brought them greater freedom." However, respondents also noted concerns about digital fraud (32%), violent content (27%), privacy threats (20%), and so on [3]. The rapid development of the global information field, its complexity, and openness create conditions for seeking adaptation strategies not only from the perspective of social and state institutions but also from the perspective of private citizens as self-defense strategies.

## 2 Scientific review

The concept of "digital freedom" emerged at the beginning of the century, yet there is still no single definition of this phenomenon. Among the most common interpretations are: information accessibility (the ability to request and receive any information), the digital equivalent of freedom of speech (openness of expression, impunity for self-expression), freedom and uncontrollability of choices (actions), with many considering digital freedom in the context of freedom of action, creativity, and communication. Digital freedom can be viewed as "digital equality" between different social and economic groups, the right to protection from cyber threats. Russian researcher L.N. Meshkova, reflecting on this phenomenon, writes: "Due to its openness and interactivity, the digital environment and online communication tools expand the space for freedom of speech, for demonstrating initiative, for realizing one's economic and political independence. On the other hand, the problem of technological, administrative, and economic regulation and control of the information and communication space arises." [4]. Some authors, analyzing the possibilities of the new digital reality, which increasingly incorporates interactive forms of activity

(learning, communication, creativity), attribute the expansion of horizons for any activity to the phenomenon of digital freedom. For example, according to J.M. Balkin, new technologies create new forms of freedom and cultural participation, but this access creates the paradox of "constraining the exercise of that freedom and participation." [5].

Upon entering the digital realm, a user leaves behind a certain stereotype of opinion or pattern of behavior (digital footprint), and in the future, may find it difficult to escape that role. Another paradox lies in the fact that a user can only enter the digital space as a realm of possibilities by leaving their digital footprint, that is, by relinquishing anonymity (confidentiality), which serves as a guarantee for certain freedoms, such as freedom of opinion.

Another Russian researcher, A.G. Myasnikova, believes that freedom should be understood as freedom of will or a certain independence of the individual in decision-making: "the ability of a person to set goals and achieve them through their own efforts." [6].

Initially, the phenomenon of free access to information and the ability to express one's own viewpoint on the internet existed without any limitations. Later, the meaning of the term was expanded to include the protection of personal data and confidentiality. However, it cannot be said that users of modern technology possess "digital freedom" in its entirety. The conclusions of philosopher Jean Baudrillard proved prophetic, predicting that the global information field would become uncontrollable, as it is created by the participation of large masses, who will themselves be held captive by the trends of the "big pot" of information: "The entire chaotic accumulation of the social revolves around this porous object, this simultaneously impenetrable and transparent reality, this nothing - around the masses...The masses are those blinded by the game of symbols and enslaved by stereotypes, those who will accept anything as long as it is spectacular. Will and representation no longer reign over the masses, but they are confronted by a surge of diagnostics, pure insight. They are caught in the boundless realm of information and statistics: one must grasp their mood, ascertain their position, and incite them to utter some kind of prophecy." [7]. The concept of "freedom" has become fundamental and key to philosophy and law. The origin of this concept dates back to the ancient world. For example, in the Old Slavic language, "svoy" meant selfhood, independence. In many Sanskrit languages (ancient Indian language), "poti" meant lord. Literally, it means one's own lord. Freedom, as a philosophical and psychological concept, describes a state of the subject in which he or she and their will are the determining cause of actions and choices. In ethics and theology, the understanding of freedom is linked to the presence of human free will, while in philosophy, it is considered a category denoting "the possibility of activity and behavior in the absence of external goal-setting." [8]. In the legal field (constitutions and laws), "freedom" is enshrined as a right (possibility, givenness) of specific behavior: freedom of speech, freedom of religion. The phenomenon of "freedom" was also explored by I. Kant, who defined freedom as "the key, the keystone of the arch of the entire building of the system of pure reason." Immanuel Kant identified the interconnection between freedom and legal order, arguing that a person is free if they must submit not to another person but to law as a universal, equal for all: "Freedom is independence from the arbitrary will of another. As long as it does not interfere with the freedom of others, in accordance with a universal law, it is the natural innate right of every human being, belonging to them by virtue of their human nature." [9]. There is a contradiction inherent in freedom: "natural necessity and the possibility of the existence of both independently of each other, but also without hindering each other." [10]. This paradox finds a new explanation in the digital society: a user cannot access resources without limiting their will, their choice, without acknowledging and respecting the freedom of others [11].

The problematic field and complexity of the phenomenon of "digital freedom" have been the subject of numerous interdisciplinary studies. It has been examined in the context of increasing total control over consumer behavior and a new understanding of digital rights [12]. The paradoxical nature and problematic aspects of freedom from the perspective of the ethics of the digital world were investigated by the American philosopher J. Tasioulas [13]. Studying the strategies for regulating the digital space and the influence of society on the implementation of the digital freedom concept, some authors have come to understand the processes of self-regulation [14]. Fully ensuring the constitutional rights and freedoms of individuals in the information sphere not only requires constant and meticulous work "ahead of the curve" in the system of legal regulation but also presupposes the development of relevant scientific approaches of a conceptual nature, which would not be limited to another system of prohibitions, but would be based on a socially and politically conditioned balance of private and public interests [15].

With the development of information technologies and available mass communication tools, the possibilities for abuse related to the use of collected and accumulated information about individuals have increased. In everyday life, people leave behind so-called virtual "breadcrumbs": digital information about who they call, where they go, what food they prefer, and so on. Based on these elements of people's lives, one can learn more than they themselves would like to reveal [16]. In the Russian Federation, a number of laws have been adopted that protect personal data ("On Personal Data" of July 27, 2006, No. 152-FZ, "Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data"). Currently, there are numerous mobile applications and internet resources, the use of which contributes to obtaining operationally significant information for investigating cases of cyber fraud [17]. However, more effective are measures to prevent any violations of information security: self-defense and recognizing digital threats.

This research examines digital freedom as the conscious and independent choice by users of information behavior strategies to ensure personal and social security. In this case, such user behavior is constructive and supports a humanistic principle of co-adaptation strategies between the user (human) and the digital world. During a period of rapid technological development, the freedom of action and will of citizens is not always guaranteed by social institutions. It is precisely personal information strategies that users can employ to achieve better results in ensuring security and self-control within the information space.

## 3 Methods

This research employed general scientific methods and methods for experimental hypothesis testing. Quantitative methods (user surveys) and qualitative methods were selected: in-depth interviews, case analyses. Expert interviews were conducted with representatives of law enforcement agencies, a cybercrime prevention specialist, a private detective agency employee, and an IT company specialist providing information security. Methods of respondent surveys and participant observation were also employed, and a video recording of the experiment was created. The result of this work was the creation of a television documentary project that was shown on the "Univer TV" student television channel at Kazan Federal University. The film "Under Fire" is a preventative project aimed at developing adaptive self-defense strategies against information threats. Mathematical statistics methods were used to analyze the experimental data of the quantitative experiment. The research involved 77 respondents, 65% of whom were women, and over 84% belonged to Generation Z (born between 2000-2015). According to generational theory, these individuals have possessed skills in managing the information field since early

childhood, and consequently, they possess skills in defending digital freedom, which they are able to recognize and develop.

## 4 Results and discussions

An analysis of crime in the field of information and telecommunications technology (ITT) in the Republic of Tatarstan revealed the following. From 2019 to 2023, the number of cybercrimes more than doubled. In 2019, 8,042 crimes in this category were registered, while in 2023, 17,738 were registered, representing 32% of all registered crimes in the Republic of Tatarstan. In 2023, the amount of material damage caused by criminal cases in this category reached 4.418 million rubles. In 2024, the growth of registered crimes in this area reached 40.8% compared to the same period last year. The crime clearance rate was 19.4%. Measures were taken to increase the number of crimes referred to court (35.4%). In 2023, the Ministry of Internal Affairs of the Republic of Tatarstan identified 3,012 individuals involved in ITT-related crimes. Of these, 1,887 individuals committed fraud and theft from accounts in the ITT sphere. Tatarstan holds the 7th position among all regions of Russia, trailing only regions such as Moscow and the Moscow region, Saint Petersburg and the Leningrad region, and Krasnodar Krai [18]. In the first four months of 2024, the Ministry of Internal Affairs of the Republic of Tatarstan identified 1,131 individuals involved in ITT-related crimes, including 581 citizens who committed theft from accounts and fraud in the ITT sphere. This figure is the highest among the Volga Federal District. Since 2019, the Ministry of Internal Affairs of the Republic of Tatarstan has established a specialized investigative and operational group to combat crimes in the field of information and telecommunications technology. They have developed methodological recommendations and work algorithms for uncovering and investigating these types of crimes, which have been forwarded to territorial police departments for study and use in operational activities [19].

Therefore, criminal strategies for using citizens' digital footprints, violating the boundaries of personal digital freedom, are systemic in nature. Preventative measures rely on the development of individual self-defense strategies for citizens.

Expert interviews clarified criminal strategies and investigated potential methods and algorithms for information self-defense.

Expert 1: Ramis Gazimov, Deputy Head of the Department of Criminal Investigation of the Ministry of Internal Affairs of the Republic of Tatarstan, Deputy Head of the Specialized Investigative and Operational Group of the Ministry of Internal Affairs to Counter Crime in the IT Sphere:

"Everyone leaves a digital footprint. All our documents, ownership certificates, are stored digitally. This means that at some point, criminals could potentially gain access to this information. There are no absolutely secure messaging apps, and with the right resources, criminals can gain access to all of your contacts. However, in a large number of crimes, individuals willingly provide access keys and money to fraudsters. In the fall of 2023, crimes were committed against a number of university employees and government officials in Kazan. The Specialized Investigative and Operational Group of the Ministry of Internal Affairs on IT Crime is currently investigating eight criminal cases against 15 suspects for the fraudulent acquisition of funds from 614 citizens. Criminals use psychological tactics to exert informational pressure and induce anxiety. The Ministry of Internal Affairs is implementing enhanced preventative measures by educating citizens about criminal schemes. These measures are essentially self-defense and self-management of information behavior."

Expert 2: Evgeny Shchepin, Member of the Association of Russian Detectives and the "World Association of Detectives":

"Eighty percent of information is available in open sources. It simply requires analysis. Analytical or digital data analysis involves the use of open sources, such as social media. There are also closed crypto channels. A socially active person leaves a digital trail everywhere, from ordering goods and services to receiving fines. It is impossible to go a single day in the 21st century without recording your geolocation. Users leave traces through social networks, as well as crypto channels where information stolen from various sources is disseminated."

Expert 3: Tatiana Nikonova, Lead Information Security Consultant at the "Innostage" Group:

"We ourselves publish information about ourselves: social media posts, usernames, emails. We subscribe to newsletters and provide information about where we live, work, and study. We don't always consider whether it is necessary to publish this data. All of this can be used by third parties. Even if information is shared within a small circle or a closed group, it leaves a trace in the information field. This is the fault of unscrupulous organizations or groups of individuals who spread this information. Anything uploaded to the internet can be found. The most significant data leak was the "Yandex Food" leak. This leak can be used to discover not only ordering preferences, but also alibis and alternative addresses. It is difficult to eliminate your digital footprint in the modern world. However, individuals always have the right, both under the Constitution and our laws, to refuse to provide personal data. Despite this right, it is not possible to refuse to present all personal data."

Survey and interview findings revealed the following results: an analysis of online content revealed a dominant theme of positive connotations associated with "digital freedom." These include the ability to express opinions freely, access information, and be free from censorship. Users highlighted the importance of digital freedom for personal self-actualization. However, concerns were also expressed regarding the spread of misinformation, online harassment, and manipulation of public opinion.

An examination of user comments on the concept of "digital footprint" revealed widespread anxiety about the collection of personal data, threats to privacy, and surveillance by both government and private entities. While some users acknowledged the inevitability of a digital footprint in the contemporary world, they advocated for greater transparency and control over data usage. Questions concerning the right to "erase" one's digital footprint and the protection of personal data were raised.

Survey data indicates that a majority of respondents associate digital freedom with the ability to maintain the confidentiality of personal information (Figure 1).

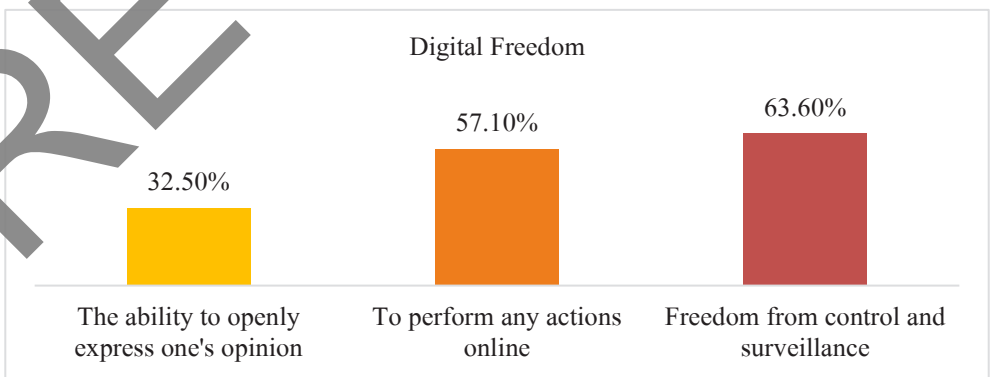


**Fig. 1.** Respondent perceptions of digital freedom.

Discussions with participants in a “VKontakte” group (315 group participants were interviewed)) revealed strategies for personal information management aimed at preserving the boundaries of individual freedom:

1. Action Forecasting: Prior to publishing any information, users weigh the pros and cons, anticipating the target audience and potential reactions to the post.

2. Anonymity: Employing avatars and pseudonyms, users strive to obfuscate or conceal personal information (full name, date of birth, address, place of work/study, personal data of friends, family, and acquaintances).

3. Law-abidingness: Adherence to platform rules and regulations. Efforts to regulate (prohibit) the sharing of personal data, including regular updates to user agreements.

4. Distortion of the data: Delaying publication for personal security reasons to maintain geolocation (movement) privacy.

5. Mention Settings: Disabling the ability to tag their profile in other users' posts or hiding the "mentions" tab from public access.

Survey data indicates that the following self-protection strategies are used by individuals aged 18-25 years old (Figure 2).

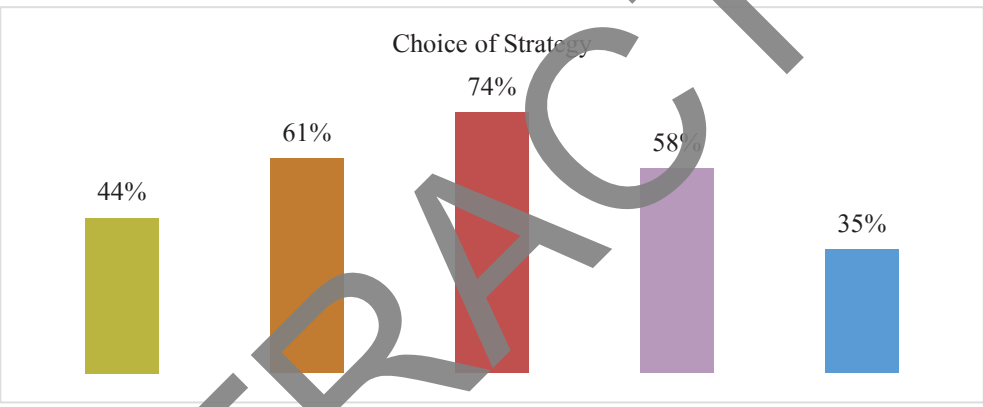


**Fig. 2.** Preferred strategies of respondents aged 18-25.

The data indicates that young individuals increasingly prioritize adherence to the general rules and regulations of online platforms, demonstrating a preference for streamlined user experiences over extensive customization of individual application settings.

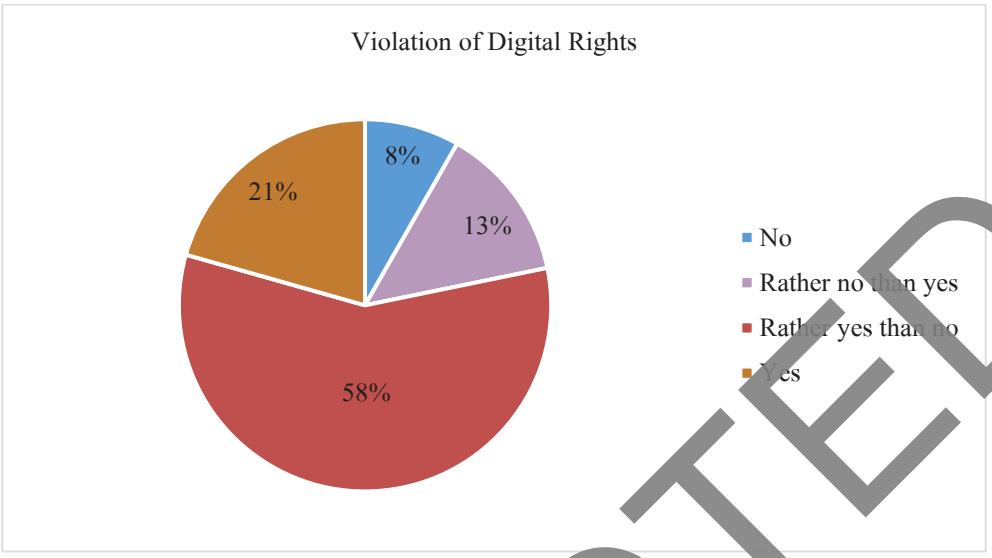


**Fig. 3.** Respondents' opinions on potential attempts to violate their digital rights.

The survey data indicated a relative sense of well-being regarding personal "digital freedom," which may suggest that members of the younger generation are successfully employing information self-defense strategies (Figure 3).

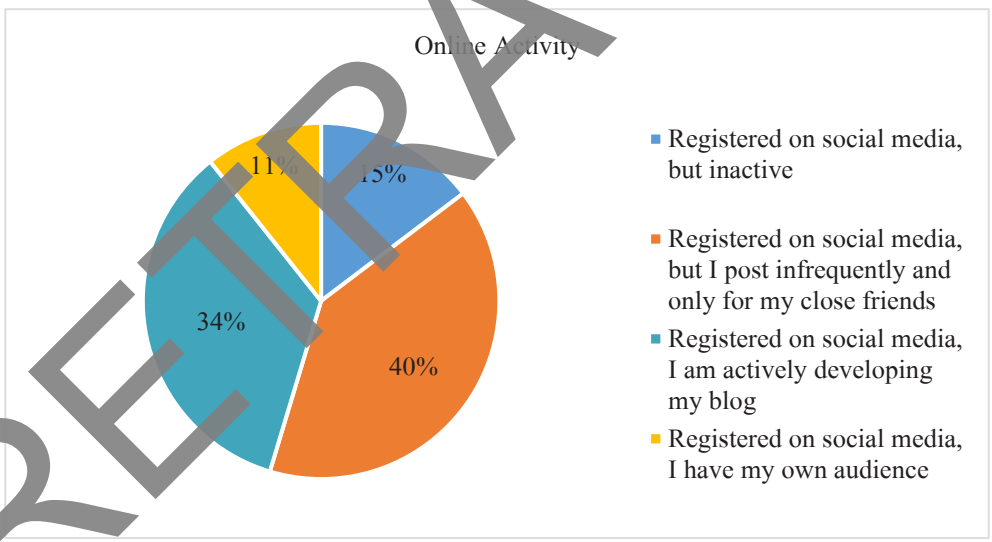


**Fig. 4.** The level of activity on the Internet.

The survey showed that the more active the user experience, the more strategies are used for conscious management of information behavior (digital footprint control) and self-defense of the boundaries of digital freedom (Figure 4).

## 5 Conclusions

The digital space is increasingly influencing the life and activities, socialization of a modern person. Strategies for adapting to the new reality include compliance with safety

standards and preserving digital freedom. The digital space is an environment for committing real criminal acts. External regulation (control and state supervision) of the preservation of citizens' rights and freedoms has a number of limitations. Achieving complete "digital freedom" in the broadest sense is currently impossible. Personal self-defense strategies (predicting actions, conscious anonymity, compliance with general rules and regulations of platforms, changing settings, etc.) can significantly increase the level of personal information security, protect users from cybercriminals.

## 6 Acknowledgements

Publication based on the expense of the subsidy allocated to the Kazan Federal University for the project No. FZSM-2023-0022 'Digital socialization and digital competence of young people in the conditions of global systemic changes: regulatory technology, risks, scripts' within the state assignment.

## References

1. The damage from cybercrimes in Russia over five years was estimated at 500 billion rubles
2. A. E. Postnikov, Digital freedom and digital slavery: a constitutionalist's view. An Independent Newspaper (2024)
3. BBC Internet Survey: Free Polls/ BBC World Service, March 8, 2010. "BBC Internet Survey: Detailed Results" Archived 2013-06-01 in The Wayback Machine, BBC World Service (2010) https://en.wikipedia.org/wiki/Digital_rights
4. L. N. Meshkova, Context and Reflection: Philosophy about the World and Man **8.4A,** 79-88 (2019) DOI:10.34670/AR.2019.45.4.070
5. J. M. Balkin, Law and Society Approaches to Cyberspace, 325-382 (2017)
6. A. G. Myasnikov, Polis. Political Research **5**, 174-186 (2017) DOI: https://doi.org/10.17976/jpps/2017.05.12
7. J. Baudrillard, E. Cioran, The Matrix of the Apocalypse. The last sunset of Europe (2015)
8. M. L. Mozheiko, The Newest Philosophical Dictionary **3**, 1280 (2003)
9. M. Y. Vasilyeva, The Idealism of Immanuel Kant, 276 (2011)
10. M. Y. Vasilyeva, Power **7**, 96-101 (2015)
11. Yu. V. Andreeva, Self-development of personality in conditions of digital freedom and self-development of the digital world. Kazan Federal University, V. Andreev, Readings: Modern Concepts and Technologies of Creative Self-Development of Personality. A Collection of Articles by Participants of the All-Russian Scientific and Practical Conference with International Participation **5**, 16-20 (2020)
12. J. E. Cohen, Georgetown University "The Digital Freedom Movement: Rethinking Digital Rights in the Age of Mass Surveillance". Law and Social Inquiry (2016)
13. J. Tasioulas, University of Oxford "The Right to Digital Freedom: Philosophical and Legal Foundations". Oxford Journal of Legal Studies,(2019)
14. P. P. Baranov, North Caucasian Legal Bulletin **2**, 63-68 (2019) DOI:10.22394/2074-7306-1-2-63-69
15. V. A. Germanova, A. S. Atabekyan, Symbol of Science **12(3)**, 240-242 (2016)

16. V. V. Kramskoy, A. N. Kozodaeva, Countering the spread of cyberbullying: new opportunities in the investigation and ways to improve legislation. Law: History and Modernity **2 (15)** (2021) DOI: 10.17277/pravo.2021.02.pp.079-087
17. A. A. Kuznetsov, E. O. Galdina, CONSTITUTIONAL HUMAN RIGHTS AND FREEDOMS IN THE DIGITAL AGE. International Journal of Humanities and Natural Sciences. **3-1**, 160-162 (2022). DOI:10.24412/2500-1000-2022-3-1-160-162
18. Materials of the Expanded Board of the Ministry of Internal Affairs of the Republic of Tatarstan on the results of activities for 2023.
19. The data is provided at the request of the account of the Ministry of Internal Affairs of the Republic of Tatarstan.