IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 3, Issue: 1
2025

Self-Defense of Rights in the Digital Space: Legal Boundaries and Forms of Implementation

Egamberdiev Eduard Khajibaevich
Tashkent State University of Law

Abstract

This research is devoted to the analysis of the legal nature and implementation peculiarities of the self-defense of rights institutions in the digital space. The paper examines the conceptual foundations of digital rights self-defense established by Articles 11 and 13 of the Civil Code of the Republic of Uzbekistan, the legal boundaries of permissible actions, and various forms of their implementation in the digital environment. Using methods of legal and comparative analysis, the study investigates problems of determining the proportionality of protective measures, distinguishing between self-defense and arbitrary action, as well as the peculiarities of self-defense for various types of digital rights (personal data, intellectual property objects, digital property rights). Special attention is paid to technological, contractual, and organizational forms of self-defense in the context of the cross-border nature of digital relations. The research results allow the formulation of recommendations for improving legislation and law enforcement practice in the field of digital rights self-defense, as well as determining optimal strategies for the lawful behavior of subjects when protecting their rights in the digital space.

Keywords: Self-Defense of Rights, Digital Space, Smart Contracts, Personal Data, Intellectual Property, Digital Assets, Civil Code of the Republic of Uzbekistan

APA Citation:

Egamberdiev, E. (2025). Self-Defense of Rights in the Digital Space: Legal Boundaries and Forms of Implementation. *Uzbek Journal of Law and Digital Policy, 3*(1), 74–103. https://doi.org/10.59022/ujldp.292

I. Introduction

The digitalization of social relations radically transforms traditional legal institutions, adapting them to new technological realities and generating innovative mechanisms for the implementation of subjective rights. The institution of self-defense of rights, historically formed as a method of direct influence by an authorized person on the violator or their property, acquires fundamentally new content, forms, and boundaries in the digital space. The relevance of studying self-defense in the digital environment is determined by several interrelated factors. The exponential growth of digital assets and intangible goods creates a need for effective mechanisms for their prompt protection without recourse to jurisdictional authorities.

The cross-border nature of digital space creates significant jurisdictional obstacles for traditional forms of judicial protection, increasing the importance of independent actions by rights holders. The technological features of the digital environment (anonymity, scalability of violations, speed of information dissemination) transform the nature of offenses and require adequate response mechanisms. Statistical data indicate a steady increase in violations of digital rights: according to the Global Cybersecurity Outlook 2022, the number of cyber incidents increased by 125% over the past year, while traditional mechanisms of legal protection do not provide effective restoration of violated rights due to the length of procedures and the cross-border nature of violations.

The issues of self-defense of rights and protection of rights in the digital space have been studied in scientific literature from various methodological positions. Issues of protection of rights in the digital space were considered primarily in the context of separate categories of rights: protection of intellectual property in the digital environment was studied in the works of Lessig L., Litman J., Mazziotti G.; problems of personal data protection were analyzed by Solove D., Schwartz P., De Hert P.; issues of protection of property rights to digital assets were addressed in the research of Werbach K., Wright A., De Filippi P.

Significant contributions to the study of technical aspects of digital rights protection were made by the works of Schneier B., Boehme R., Anderson R., examining cryptographic and software-technical means of information protection. The formation of methodological foundations of digital law as an independent direction of legal research was carried out in the works of Murray A., Reed C., Benkler Y., Zittrain J., who laid the theoretical basis for analyzing the transformation of legal institutions in the digital era. The author of the article also described the legal nature of digital law, digital space (Egamberdiev, 2023b), objects in the digital world (Egamberdiev, 2021), internet of things (Egamberdiev, 2023a, 2023d), accounts (Egamberdiev, 2023c), and trade in virtual objects.

Despite a significant number of works devoted to individual aspects of rights protection in the digital environment, a comprehensive theoretical and legal study of

the institution of self-defense of rights in the context of digital space has not been conducted. Existing research is characterized by fragmentation, focusing either on general theoretical aspects of self-defense without taking into account the specifics of the digital environment, or on technical aspects of digital rights protection without their legal conceptualization. In scientific literature, there is no systematic analysis of the transformation of the traditional institution of self-defense in the conditions of digitalization, the legal boundaries of self-defense of digital rights have not been defined, and the forms of its implementation in various segments of digital space have not been systematized.

A particular gap is observed in the study of the relationship between technical protection measures and legal criteria for self-defense, which creates uncertainty in qualifying the actions of subjects of digital relations and complicates the formation of effective law enforcement practice. This research aims to fill this gap through a comprehensive analysis of the legal nature, boundaries, and forms of self-defense in digital space.

The central problem of the research is the fundamental transformation of traditional mechanisms of self-defense of rights in the digital space and the need to define their legal boundaries in new technological conditions. The digital environment radically changes the parameters for exercising the right to self-defense: factual actions of the authorized person are replaced by automated technical measures; direct impact on the violator is transformed into impact on information systems; temporal and spatial localization of self-defense measures gives way to their global and permanent nature. As a result, traditional legal criteria for self-defense (proportionality, temporal limitation) become inapplicable or require substantial adaptation to the conditions of the digital environment.

Legal uncertainty arises in qualifying technical protection measures as forms of implementing the right to self-defense, which creates risks both for rights holders (possibility of being held liable for exceeding the limits of self-defense) and for users of digital resources (unlimited technical restrictions under the guise of self-defense). Solving this problem requires developing an adequate theoretical and legal model of self-defense in digital space that takes into account the technological specifics of the digital environment and ensures a balance of interests of various participants in information relations.

The purpose of this research is to determine the legal boundaries and forms of implementation of self-defense of rights in digital space based on a comprehensive analysis of the transformation of this institution in the conditions of digitalization of social relations. To achieve this goal, the following tasks are set:

- To conduct a conceptual analysis of the institution of self-defense of rights in the context of the digital environment, to identify the specifics of its transformation under the influence of technological factors, and to determine its

place in the system of legal mechanisms for the protection of digital rights.

- To investigate the legal boundaries of self-defense of digital rights, including criteria of proportionality, limits of permissible technical measures, problems of distinguishing from arbitrary action, and peculiarities of legal assessment of preventive measures.
- To systematize the forms of implementation of self-defense in digital space, including technological, contractual, and organizational mechanisms, and to determine the peculiarities of their legal regulation.
- To identify and analyze key problems of legal qualification of self-defense actions in the digital environment, including determining the proportionality of protective measures, technical complexity of assessing legality, cross-border nature of self-defense, and issues of balancing the interests of different subjects.

The scientific significance of the research lies in the development of theoretical and methodological foundations for understanding the institution of self-defense of rights in digital space, identifying patterns of its transformation under the influence of digital technologies, and forming a conceptual model of legal regulation of self-defense of digital rights. The research contributes to the development of the general theory of protection of subjective rights, enriching it with an understanding of the specifics of implementing protective mechanisms in the digital environment. The obtained results contribute to the development of digital law as a new interdisciplinary field of legal research, forming a theoretical basis for analyzing the transformation of traditional legal institutions in the conditions of digitalization.

The practical significance of the research consists in the formation of scientifically based recommendations for improving legislation and law enforcement practice in the field of self-defense of digital rights. The results of the research can be used by the legislator in developing normative acts regulating issues of digital rights protection; by judicial bodies in resolving disputes related to self-defense in the digital environment; by rights holders in choosing optimal strategies for protecting their rights; by educational institutions in training specialists in the field of digital law.

II. Methodology

The research is based on a qualitative research approach, which is most adequate for analyzing complex legal phenomena in a dynamically developing digital environment. The choice of qualitative methodology is determined by several factors. The institution of self-defense in the digital space is in the formation stage, which requires flexible research tools capable of considering contextual features and identifying implicit interrelationships. The multifaceted nature of the problem, affecting legal, technological, economic, and social factors, implies the use of a comprehensive approach integrating various research methods.

The absence of established practice and the limited empirical data on issues of self-defense of digital rights makes the application of quantitative methods, requiring

statistically significant samples, premature. The qualitative approach allows forming a holistic understanding of the phenomenon under study through an in-depth analysis of its legal nature, forms of manifestation, and contextual connections.

The research applies a complex of methods providing a comprehensive analysis of the problem. Doctrinal analysis of legal concepts is used to determine the theoretical foundations of self-defense of rights, to identify its essential characteristics, and to research the transformation of this institution in the context of digitalization. This method includes critical analysis of scientific literature, conceptual modeling, and systematization of theoretical approaches to understanding self-defense in traditional and digital environments.

Comparative legal analysis of the legislation of Uzbekistan and foreign countries is applied to identify general trends and national peculiarities of legal regulation of self-defense of digital rights. Within this method, a comparison of normative provisions regulating issues of self-defense, technical protection measures, and responsibility for violation of digital rights in various legal systems is conducted. Special attention is paid to the legislation of countries with developed digital economies (USA, EU, United Kingdom, Japan, South Korea), as well as post-Soviet states having legal traditions similar to Uzbekistan.

Analysis of judicial practice on issues of self-defense of digital rights is used to identify practical problems of law enforcement and emerging approaches to qualifying self-defense actions in the digital environment. Within this method, decisions of national courts of Uzbekistan are studied, as well as landmark precedents of foreign jurisdictions forming standards for assessing the legality of self-defense in the digital context. The method of legal modeling is applied to determine the permissible boundaries of self-defense and to forecast the legal consequences of various forms of its implementation in the digital environment. This method includes building theoretical models of interaction of subjects in the process of self-defense of digital rights, analysis of legal risks, and development of optimal legal constructions for regulating the corresponding relations.

The sources of data for the research are normative legal acts, judicial practice, and scientific publications. The normative base of the research includes: constitutional provisions on the protection of rights and freedoms; norms of civil legislation regulating issues of self-defense of rights (Articles 11 and 13 of the Civil Code of the Republic of Uzbekistan); sectoral legislation in the field of information technologies, intellectual property, personal data protection; international treaties and agreements in the field of protection of rights in the digital environment.

Judicial practice as a source of data includes decisions of national courts of Uzbekistan on issues of protection of digital rights, as well as landmark precedents of foreign courts forming standards for assessing the legality of self-defense in the digital context. Scientific publications used in the research cover monographs, scientific articles, dissertation research on issues of self-defense of rights, protection of digital

rights, information security, legal regulation of the digital economy, published over the last 10 years.

The research has certain limitations that must be considered when interpreting its results. The dynamic development of digital technologies causes rapid obsolescence of specific technical solutions and forms of implementation of self-defense, which requires focusing on conceptual principles and models rather than on detailed analysis of specific technologies. The limited empirical data on the practice of self-defense of digital rights in Uzbekistan creates the necessity to extrapolate foreign experience taking into account national specifics. The interdisciplinary nature of the problem requires addressing technical aspects of digital technologies, which may create methodological difficulties in their legal conceptualization. Fourth, the absence of established terminology and conceptual apparatus in the field of digital law creates risks of terminological uncertainty, which requires special attention to definitions and the categorical apparatus of the research.

The research is conducted in compliance with the ethical principles of scientific activity. In the analysis of judicial practice, the confidentiality of personal data of process participants is ensured, unless otherwise provided by legislation or the decision is not published in official sources. When using scientific publications, correct citation and references to sources are carried out with respect for copyright. The research does not involve experiments or other actions violating the rights of subjects of digital relations or creating a threat to information security. When formulating recommendations for improving the practice of self-defense, potential risks of abuse of protective mechanisms and the need to ensure a balance of interests of various participants in digital relations are taken into account.

III. Results

A. Conceptual Foundations of Self-Defense of Rights in the Digital Space

The institution of self-defense of rights in the modern legal order represents a complex legal mechanism that allows subjects to independently exercise protection of their rights and legitimate interests without recourse to jurisdictional authorities. The traditional understanding of self-defense, enshrined in civil legislation, was formed in the conditions of the physical world and is oriented predominantly toward material objects of legal relations. In accordance with Article 13 of the Civil Code of the Republic of Uzbekistan, self-defense of civil rights is permitted under the condition that the methods of protection are proportionate to the violation of the right. However, digital space as a special environment for interaction of legal subjects significantly transforms traditional notions of self-defense, generating new forms and methods of implementing this right.

The conceptual specificity of self-defense of rights in the digital space is determined by the fundamental features of the digital environment: immateriality of objects, cross-border nature, anonymity of interaction participants, automation of

processes, and dynamism of changes. These characteristics of digital space form a new paradigm for the implementation of the right to self-defense, where traditional legal constructs undergo significant transformation. Research (De Filippi & Wright, 2018) shows that in the digital environment, there is a convergence of technical code and legal norms, as a result of which technical means of information protection actually become an instrument for implementing the right to self-defense. This merger of technology and law gives rise to the phenomenon of "code is law," in which program code acts not only as a means of communication but also as a regulator of behavior of participants in digital relations.

In the context of the digital environment, self-defense of rights acquires a dual nature: on the one hand, it retains its legal essence as a method of protecting subjective rights; on the other hand, it is implemented predominantly through technical mechanisms, which themselves can be objects of legal regulation. In this regard, it seems necessary to expand the traditional definition of self-defense, including in it not only actions of a factual nature but also the use of software and technical means aimed at preventing, suppressing rights violations, and restoring the violated state in the digital environment. Researchers Murray, A. (Murray, 2019) and Hildebrandt, M. (Hildebrandt, 2020) in their works substantiate the necessity of forming a special legal regime for self-defense of digital rights, taking into account the automated nature of protective mechanisms and their potential impact on the rights of third parties.

Thus, self-defense of rights in the digital space can be defined as a complex of independent lawful actions of an authorized person, as well as their application of technical and software means, aimed at preventing, suppressing violations of their rights and legitimate interests in the digital environment, as well as restoring the situation that existed before the violation of the right, without recourse to competent state authorities. This definition takes into account both the legal nature of self-defense and the technological context of its implementation in the digital space, which allows forming adequate legal mechanisms for regulating the corresponding relations.

The digital transformation of social relations significantly changes the paradigm of implementing the right to self-defense, necessitating a revision of established legal concepts. The traditional understanding of self-defense as direct influence of a person on the violator or their property acquires a new dimension in the digital environment, where physical impact is replaced by technological solutions, and temporal and spatial parameters of interaction of legal subjects lose their significance. Critical analysis of the transformation of the institution of self-defense allows identifying several key directions of conceptual changes.

First, there is a significant expansion of the preventive function of self-defense in the digital space. If in the traditional understanding, self-defense is predominantly aimed at suppressing an already begun violation of rights, then in the digital environment, the emphasis shifts to preventing potential violations through the creation of technological barriers. Research (Cohen, 2019) confirms the thesis that in

the digital ecosystem, preventive mechanisms of self-defense (encryption, authentication, authorization) acquire paramount importance, since the restoration of violated digital rights is often extremely difficult due to the properties of information as an object of legal relations. The preventive nature of self-defense in the digital environment necessitates a revision of the criterion of proportionality of protection to the violation, as the assessment of proportionality of preventive measures to a not yet committed violation presents a complex legal problem.

Second, in the digital space, there is an automation of the implementation of the right to self-defense through software and technical means functioning without the direct participation of the rights holder. Programmable protection mechanisms (DRM systems, smart contracts, automatic violation detection systems) independently identify violations and apply the provided technical sanctions. As noted by Werbach (Werbach, 2020), the automation of self-defense gives rise to the fundamental problem of the relationship between technical code and legal norms, since software algorithms can implement protective mechanisms without taking into account legal principles of proportionality, good faith, and prohibition of abuse of rights. Automated self-defense systems, unlike humans, are not capable of taking into account the complex context of arising legal relations and adapting their actions to specific circumstances, which creates risks of violating the rights of bona fide users.

Third, the subject composition of self-defense relations in the digital space is being transformed. If traditionally self-defense is carried out directly by the authorized person or their representative, then in the digital environment, many intermediaries emerge (platforms, service providers, software developers) participating in the implementation of protective mechanisms. Digital platforms actually become quasi-jurisdictional bodies, implementing self-defense measures on behalf of rights holders based on their internal rules. A complex system of delegation of authority for the protection of rights emerges, which blurs the boundaries between self-defense and protection of rights by third parties, which requires appropriate legal conceptualization.

Finally, the very understanding of rights violation in the digital space is being transformed. The digital environment generates new forms of encroachments on the rights of subjects that have no analogues in the physical world (unauthorized access, copying information without depriving the rights holder of access, data manipulation). Accordingly, the understanding of permissible methods of self-defense also changes, which must take into account the specifics of digital violations.

The legal regulation of the institution of self-defense of rights in the legislation of the Republic of Uzbekistan has a multi-level structure and is based on constitutional principles of protection of human rights and freedoms. The foundation of legal regulation consists of Articles 11 and 13 of the Civil Code of the Republic of Uzbekistan, according to which self-defense of civil rights is permitted without recourse to competent authorities, provided that the methods of protection are

proportionate to the violation of the right. These norms have a general character and do not contain specific provisions regarding the implementation of the right to self-defense in the digital space, which creates certain difficulties in law enforcement practice when qualifying the actions of subjects of digital relations.

Special regulation of certain aspects of self-defense of digital rights is contained in a number of sectoral laws of the Republic of Uzbekistan. The Law "On Electronic Digital Signature" establishes the right of subjects to use cryptographic means of information protection, which actually represents a form of technical self-defense of digital rights. The Law "On Personal Data" provides for the right of the subject of personal data to demand blocking, destruction of their data, as well as to take other measures to protect their rights. The Law "On Electronic Commerce" contains provisions on the right of participants in electronic commerce to apply technical means to protect their interests in electronic transactions.

The Law "On Copyright and Related Rights" is of great importance for the implementation of the right to self-defense in the digital space, which establishes the right of rights holders to use technical means of protection of copyright and related rights, and also establishes a prohibition on actions aimed at circumventing such technical means of protection. These norms actually legalize technological mechanisms of self-defense of intellectual rights in the digital environment, which corresponds to international standards in this field. However, detailed regulation of the limits of use of technical means of protection and their correlation with the rights of bona fide users is absent in the legislation.

Analysis of the legislation of the Republic of Uzbekistan shows that the regulatory framework in the field of self-defense of digital rights is in the process of formation and does not fully take into account the specifics of digital relations. It should be noted that there is fragmentation of regulation, lack of a systematic approach to determining the legal boundaries of self-defense in the digital space, and insufficient detailing of criteria for the legality of technical protection measures. These shortcomings create legal uncertainty for subjects of digital relations and hinder the implementation of effective mechanisms for self-defense of rights.

Certain gaps in legal regulation are partially filled by judicial practice. The Supreme Court of the Republic of Uzbekistan in a number of its resolutions has addressed the issues of application of Articles 11 and 13 of the Civil Code and criteria for the legality of self-defense. However, the specifics of digital relations and the peculiarities of implementing the right to self-defense in the digital environment have not yet received detailed explanation in the acts of the highest judicial instances, which also indicates the need to improve the regulatory framework in this area.

International experience in regulating self-defense of digital rights is characterized by a variety of approaches, determined by differences in legal systems and the level of development of digital technologies. Comparative analysis of foreign legal regimes allows identifying the main trends and models of regulation that can be

taken into account when improving the national legislation of the Republic of Uzbekistan.

The European model of regulating self-defense of digital rights is based on the principle of balancing the interests of rights holders and users of information. The General Data Protection Regulation (GDPR) establishes a comprehensive system of rights for data subjects, including the right to delete information ("right to be forgotten"), the right to restrict processing, the right to data portability, which actually represent forms of self-defense of personal data. The EU Directive on Copyright in the Digital Single Market of 2019 expanded the possibilities for rights holders to self-defend their rights, but at the same time established limitations for technical protection measures, which should not impede the implementation of exceptions to copyright. As noted by Hugenholtz (Hugenholtz et al., 2021), the European approach to technical protection measures is characterized by the desire to maintain a balance between effective protection of rights and ensuring access to information in the public interest.

The American model of regulating technical measures for self-defense of digital rights has historically been oriented towards prioritizing the interests of rights holders. The Digital Millennium Copyright Act (DMCA) contains broad powers for rights holders to apply technical measures to protect their rights, including the "notice and takedown" procedure for prompt removal of content that infringes copyright. At the same time, in the USA, judicial practice is actively developing, limiting excessively aggressive forms of technical self-defense. Research conducted by Asay (Asay, 2015) shows that American courts are gradually forming the doctrine of "copyright misuse," limiting the application of technical protection measures that go beyond the exclusive rights of the author.

Asian countries, in particular South Korea, Japan, Singapore, are developing a model for regulating self-defense of digital rights, combining elements of European and American approaches. The legislation of these countries provides for detailed regulation of technical protection measures, procedures for notification of violations, and responsibility of internet intermediaries. A feature of the Asian model is the active role of the state in forming the technological infrastructure for self-defense of digital rights. For example, in Singapore, there is a state system for certification of technical means of information protection, which ensures the compliance of protective mechanisms with established standards.

International treaties in the field of intellectual property (WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty) establish minimum standards of legal protection for technical measures used by rights holders for self-defense of their rights. Article 11 of the WIPO Copyright Treaty obliges member states to provide legal protection and effective legal remedies against the circumvention of technical means used by authors to protect their rights. At the same time, international acts leave significant discretion to states in determining specific mechanisms for implementing these standards.

Analysis of international experience shows that effective regulation of self-defense of digital rights requires a comprehensive approach that takes into account the technological specifics of the digital environment, the need to balance the interests of various participants in information exchange, and ensure legal certainty. The most promising appears to be a risk-oriented approach to regulating self-defense, in which legal restrictions on technical protection measures are differentiated depending on the degree of their potential impact on the rights and legitimate interests of third parties.

B. Legal Boundaries of Self-Defense of Digital Rights

The criterion of proportionality of defense to the violation is a fundamental principle determining the legal boundaries of self-defense in both traditional and digital environments. The legislative establishment of this criterion in Article 13 of the Civil Code of the Republic of Uzbekistan is aimed at preventing abuses in the exercise of the right to self-defense and ensuring a balance of interests of participants in civil legal relations. However, in the digital space, the application of the proportionality criterion faces significant difficulties due to the specifics of information relations. Grimmelmann's research (Grimmelmann, 2015) identifies key problems in determining proportionality in the digital environment: disproportionality of the scales of potential harm and protective measures, difficulty in assessing harm to intangible goods, asymmetry of technological capabilities of participants in digital relations, and the cross-border nature of violations. As a result, traditional criteria for assessing proportionality, based on cost characteristics and material damage, prove to be of little applicability in the digital context.

Adaptation of the proportionality criterion to the conditions of the digital environment requires the development of specific assessment parameters that take into account the informational nature of digital objects and the peculiarities of their legal regime. In the work of Peukert (Peukert & Windisch, 2024), a multi-factor approach to determining the proportionality of digital self-defense measures is proposed, including an assessment of: (1) the degree of probability of a rights violation, (2) the potential scale of negative consequences, (3) the technical necessity of the measures applied, (4) the impact of protective measures on the rights and interests of third parties, (5) the availability of alternative methods of protection. Particularly significant is the analysis of the proportionality of technical protection measures in the context of possible impact on bona fide users, since in the digital environment, protective mechanisms often act indiscriminately, limiting the rights of a wide range of persons. The formation of adequate proportionality criteria requires joint efforts from the legislator, judicial practice, and legal doctrine to create a flexible and technologically neutral approach that could effectively adapt to dynamically developing digital technologies.

Technical measures for the protection of digital rights are software and hardware means that ensure control of access to digital rights objects and prevent actions that violate the rights of rights holders. Determining the legal limits of the application of technical protection measures is of fundamental importance for the

formation of a balanced system of self-defense in the digital space. Modern legal doctrine and legislation of various countries highlight several key limitations on the admissibility of technical protection measures. First, technical measures should not impede the implementation of legal exemptions and limitations of exclusive rights (fair use, fair dealing, exhaustion of rights). Second, they should not collect excessive information about users, violating legislation on personal data. Third, technical protection measures should not create threats to information security or the stability of the functioning of information systems.

Automated protection systems functioning on the basis of machine learning algorithms and artificial intelligence present a particular problem. Such systems are capable of independently identifying alleged violations and applying protective measures without human intervention, which creates risks of erroneous blocking of legitimate content and excessive restriction of users' rights. Research by Keller (Keller, 2013) reveals critical shortcomings of modern systems of automatic content filtering, including a high level of false positive triggering, inability to take into account contextual factors, and difficulties in determining legitimate cases of free use. The legal limits of automated protection systems should include requirements for transparency of algorithms, accountability of system operators, mandatory human control in disputed situations, and effective mechanisms for appealing erroneous decisions. The formation of adequate legal limitations on technical protection measures requires a deep understanding of the technological aspects of their functioning and a comprehensive interdisciplinary approach combining legal, technical, and ethical expertise.

Distinguishing lawful self-defense from unlawful arbitrary action presents a complex theoretical and practical problem in the context of digital space. The norms of Articles 11 and 13 of the Civil Code, establishing the criteria for the legality of self-defense, and the provisions of Article 229 of the Criminal Code of the Republic of Uzbekistan, defining the composition of arbitrary action, were formed in the conditions of physical reality and are oriented toward material objects of legal relations. In the digital environment, the boundaries between protecting one's own rights and unlawfully affecting others' information resources become blurred due to the specific properties of digital information. Research by Reed and Murray (Reed & Murray, 2018) highlights key factors complicating the distinction: the absence of physical boundaries of information objects, the multiplicity of copies of digital information, the need to use the technical infrastructure of third parties for implementing protective measures. As a result, actions for self-defense of digital rights can affect information systems and resources belonging not only to the violator but also to bona fide third parties, which creates risks of qualifying such actions as arbitrary.

Practical criteria for distinguishing between self-defense and arbitrary action in the digital environment should take into account not only the traditional criterion of

proportionality but also specific parameters of the digital context: the degree of selectivity of impact, minimization of side effects for third parties, transparency of applied measures, compliance with technological standards and protocols. Research by Lemley and Reese (Lemley & Reese, 2004) proposes using the "least intervention test," according to which only those self-defense measures that are minimally necessary to stop the violation and do not create unreasonable obstacles to the normal functioning of information systems are recognized as lawful. Particularly relevant is the development of legal guarantees against the use, under the guise of self-defense, of technical measures actually aimed at obtaining unlawful advantages or restricting competition in the digital environment. The formation of balanced criteria for distinguishing between self-defense and arbitrary action in the digital space requires coordination of efforts of the legislator, law enforcement agencies, and the technical community to develop technologically neutral and at the same time practically applicable legal solutions.

Preventive measures of self-defense acquire special significance in the digital space due to the specifics of informational objects, restoration of rights to which after a violation is often difficult or impossible. The traditional understanding of self-defense, oriented predominantly toward suppressing an already begun violation, faces the need to adapt to conditions where the prevention of violation is a more effective way of protecting digital rights. The legal assessment of preventive measures of self-defense is complicated by the fact that at the time of their application, the violation has not yet occurred, which makes it difficult to assess the proportionality of protection to potential violation. Research by Wu (Wu, 2016) reveals a fundamental problem in determining the proportionality of preventive measures: the need to balance between the uncertain risk of future violation and the specific limitation of rights arising as a result of the application of protective mechanisms. Unlike reactive measures aimed at suppressing a specific violation, preventive measures usually have a generalized character and potentially affect a wide range of subjects, including bona fide users.

The legal assessment of preventive measures of self-defense should be based on a multi-factor analysis that takes into account the specifics of the digital environment. The key criteria for the legality of preventive measures include: the presence of a real threat of rights violation, based on objective data; technical necessity and sufficiency of the chosen protective mechanisms; minimization of negative impact on user experience and functionality of digital products; differentiated approach to various categories of users; availability of mechanisms for prompt correction of errors and restoration of lawful access. Of particular importance is the assessment of the long-term consequences of the widespread application of preventive measures for the development of technological innovations, scientific research, and the realization of fundamental rights to access information and freedom of creativity. The formation of a balanced approach to the legal assessment of preventive measures of self-defense requires consideration not only of the private interests of rights holders but also of public interests related to ensuring the open and innovative nature of the digital

ecosystem.

C. Forms of Implementation of Self-Defense in the Digital Space

Technological protection measures represent the most widespread and effective form of implementation of self-defense in the digital space. Technological measures are understood as software and technical tools and methods that ensure control of access to information, prevention of unauthorized use of digital objects, and monitoring of user actions. Cryptographic data encryption is a basic element of technological self-defense and is used to ensure the confidentiality of information during storage and transmission. Modern encryption algorithms (AES, RSA, ECC) provide practically insurmountable protection, provided that key management rules are observed. Biometric authentication (facial recognition, fingerprints, voice, iris) ensures verification of the user's identity and prevents unauthorized access to digital assets. Biometric systems provide a higher level of security compared to traditional authentication methods; however, their application raises questions about the protection of biometric data and compliance with the principle of proportionality in the collection of personal information.

Blockchain and distributed ledger technologies form a new paradigm of self-defense of digital rights, based on the principles of decentralization, cryptographic verification, and immutability of records. Blockchain systems ensure the protection of data integrity, transparent tracking of transaction history, and automatic execution of conditions through smart contracts. According to research by Finck (Finck, 2019), blockchain technologies allow implementing the concept of "self-executing rights," where legal protection is incorporated directly into the technological infrastructure. Digital Rights Management (DRM) systems represent comprehensive technological solutions for controlling the use of protected content. Modern DRM systems include methods of encryption, watermarks, digital fingerprints, licensing mechanisms, and copy prevention. Despite their technical effectiveness, DRM systems are criticized for excessive restrictions on user rights and interference in the private sphere. Research by Karapapa (Karapapa, 2020) reveals a discrepancy between the technical capabilities of DRM systems and the legal boundaries of exclusive rights, when technological restrictions go beyond the legitimate prerogatives of rights holders, hindering the implementation of exceptions to copyright and the principle of exhaustion of rights. Legal regulation of technological protection measures should ensure a balance between the effectiveness of protection and the preservation of fundamental principles of information exchange.

Contractual mechanisms of self-defense are based on the autonomy of the will of the parties and allow rights holders to establish additional conditions and restrictions on the use of digital content or services. End User License Agreements (EULA) and Terms of Service are the main contractual instruments defining the rules of access and use of digital products. In the digital environment, these agreements are often implemented through "click-wrap" or "browse-wrap" models, where the user's

consent is implied when performing certain actions (clicking the "Agree" button or simply using the service). Research by Loos and Luzak (Loos & Luzak, 2016) reveals problems with the effectiveness of such agreements: information asymmetry between the rights holder and the user, complexity and volume of agreement texts, lack of real opportunities for negotiating terms. Statistical data show that less than 1% of users carefully read license agreements, which calls into question the awareness of consent and the validity of such contracts from the perspective of classical contract doctrine.

Smart contracts represent an innovative mechanism of contractual self-defense, combining legal and technological elements. Smart contracts are self-executing software protocols functioning on the basis of blockchain technologies that automatically implement the terms of an agreement between parties upon the occurrence of specified circumstances. The main advantage of smart contracts lies in eliminating the need for trust between parties and ensuring the inevitability of execution of the terms of the agreement. Research by Savelyev (Savelyev, 2016) analyzes the legal aspects of smart contracts and highlights their key legal features: automatic execution, irreversibility of operations, limited possibilities for making changes and terminating the contract. These characteristics give rise to new legal challenges, including problems of determining applicable law, legal qualification of program code, correlation of program logic and legal formulations, and responsibility for errors in the code. Of particular complexity is the question of the limits of autonomy of smart contracts and the necessity of mechanisms of external control, especially in cases where automatic execution can lead to disproportionate or unfair results. The development of legal doctrine regarding smart contracts requires an interdisciplinary approach combining expertise in law, computer science, and economics.

Organizational measures of self-defense in the digital space represent a complex of administrative procedures and practices aimed at the prompt identification, documentation, and suppression of violations of digital rights. Digital space monitoring systems are a key element of organizational self-defense and include automated search for unlawful use of content, tracking of unauthorized access to information systems, and analysis of behavioral anomalies of users. Modern monitoring systems use machine learning technologies and pattern recognition to identify potential violations in large-scale information arrays. Research by Urban (Urban et al., 2017) reveals a growing trend toward automation of monitoring processes and shows that major rights holders identify thousands of potential violations daily through automated content tracking systems. Notification and warning procedures (notice and alert) allow informing potential violators about identified problems and providing an opportunity for voluntary elimination of violations before applying more serious sanctions.

Self-help takedown mechanisms represent a specific form of organizational self-defense, in which the rights holder initiates a procedure for removing unlawful

content without going to court. This mechanism is implemented through interaction with internet intermediaries (hosting providers, platforms, search engines) based on legislative requirements or voluntary agreements. The most well-known model is the "notice and takedown" procedure, established in the Digital Millennium Copyright Act (DMCA), which prescribes the removal of content upon reasonable notification from the rights holder with the possibility of subsequent challenge through a "counter-notice." Research by Seng (Seng, 2014) analyzes the effectiveness of this procedure and reveals critical shortcomings: a high level of false positive notifications, disproportionate impact on freedom of expression, insufficient procedural guarantees for users, and excessive administrative costs for internet intermediaries. In the European Union, the E-Commerce Directive and the Directive on Copyright in the Digital Single Market establish similar mechanisms, but with higher requirements for the validity of notifications and procedural guarantees. Improving organizational measures of self-defense requires developing standardized protocols for interaction between rights holders and internet intermediaries, increasing the transparency of procedures, and strengthening mechanisms of independent control to prevent abuses.

D. Peculiarities of Self-Defense of Various Types of Digital Rights

Self-defense of personal data acquires special significance in the conditions of the digital economy, where personal information becomes a key asset and the object of numerous transactions. The specificity of personal data as an object of legal protection determines the peculiarities of the mechanisms of their self-defense. First, the difficulty of defining the boundaries of personal data in the digital environment, where new forms of personal information are constantly being generated (metadata, behavioral data, location data), creates uncertainty regarding the object of protection. Second, the asymmetry of informational capabilities between data subjects and processing operators significantly limits the practical possibilities for implementing the right to self-defense. Research by Solove (Solove, 2021) shows that most users do not possess sufficient technical knowledge and resources for effective control over their data in the digital environment. Technical measures for self-defense of personal data include the use of encryption tools, anonymization, private browsing of internet resources, ad blockers, and trackers. A special category consists of "Privacy by Design" technologies, integrating mechanisms for protecting personal data directly into the architecture of information systems and digital products.

Legal mechanisms for self-defense of personal data are based on a complex of special rights of subjects, enshrined in legislation on the protection of personal data. The EU General Data Protection Regulation (GDPR) and similar national laws provide data subjects with broad powers to control their information: the right of access to data, the right to rectification, the right to erasure ("right to be forgotten"), the right to restriction of processing, the right to data portability, the right to object to processing. The implementation of these rights actually represents a form of self-defense, allowing the subject to restore control over their personal data without

recourse to state authorities. Research by Ausloos (Ausloos et al., 2019) analyzes the practice of implementing the right to be forgotten in the EU and reveals significant problems of effectiveness: complexity of request submission procedures, long consideration periods, ambiguous criteria for satisfying requirements, limited territorial effect of decisions. A serious challenge for self-defense of personal data is the cross-border nature of information processing, when the subject's data is processed in different jurisdictions with different levels of protection. In such conditions, self-defense requires coordination of the subject's actions in several legal systems, which significantly reduces its effectiveness. A promising direction for the development of mechanisms for self-defense of personal data is the concept of "information fiduciary" proposed by Balkin (Balkin, 2020), according to which data operators should be considered as trustees of the subjects, bearing fiduciary obligations to protect their information interests.

Self-defense of intellectual property objects in the digital space is characterized by particular complexity due to the fundamental properties of digital information: ease of copying without loss of quality, minimal marginal costs of reproduction, difficulty in tracking distribution. These characteristics radically change the economics of creation and use of intellectual products, requiring adaptation of traditional protection mechanisms to new technological realities. The most common form of self-defense of digital intellectual property objects are technical protection measures (TPM) - software or hardware solutions that control access to works and limit the actions that can be performed with them. Digital Rights Management (DRM) systems combine various technical means of protection and provide comprehensive protection of content in accordance with the rules established by the rights holder. Research by Mazziotti (Mazziotti, 2008) shows that DRM systems transform the traditional model of copyright, replacing legislative regulation with technical restrictions that directly control the use of works. This transformation gives rise to a fundamental conflict between the technical capabilities of rights holders and the legally established limitations of exclusive rights.

Alternative models of self-defense of intellectual property in the digital environment are based on using the capabilities of digital technologies themselves to create new mechanisms for protecting rights. Digital marking and tracking systems, including watermarks, digital fingerprints, and metadata, allow identifying the rights holder and tracking the use of works in the digital space. Blockchain technologies provide reliable fixation of authorship and transfer of rights to intellectual products, creating a distributed and immutable register of information about intellectual property objects. An innovative direction of self-defense is the use of open licenses (Creative Commons, GNU GPL), which do not restrict the distribution of works but establish certain conditions for their use based on copyright. This model of "open content" actually uses legal mechanisms to protect the public domain and create information resources for collective use. Open licenses form an alternative economic model for the distribution of intellectual products, based not on access control, but on additional

sources of monetization (additional services, personalization, community support).

Self-defense of property digital rights represents a specific area where technical protection mechanisms actually become an integral part of the property right itself. Cryptocurrencies and digital tokens function within distributed ledgers, where possession and disposal of assets is ensured by cryptographic methods without the participation of a central regulator. The specificity of self-defense in this field is determined by the features of blockchain technologies: decentralized nature of the system, irreversibility of transactions, transparency of the register, pseudonymity of participants. The main mechanism for self-defense of property digital rights is a cryptographic system of keys, where possession of a private key actually certifies the right to dispose of digital assets. Technical means of storing and managing private keys (hardware and software wallets, multi-factor authentication systems, access recovery mechanisms) represent the infrastructure of self-defense in the ecosystem of digital assets. Research by Haeringer (Haeringer et al., 2018) analyzes the economic model of decentralized self-defense in blockchain systems and shows that the absence of a central arbiter creates a fundamentally new paradigm of rights protection, where security is ensured by a consensus mechanism and economic incentives of network participants.

A special problem of self-defense in the field of digital assets is the question of legal qualification of technical protection measures and their relationship with traditional legal mechanisms. Unlike intellectual property objects or personal data, where technical measures complement legal protection, in the case of cryptocurrencies and tokens, technical code actually replaces legal regulation. As noted by Werbach (Werbach, 2018), blockchain implements the concept of "lex cryptographica" (cryptographic law), where the rules of the system are encoded in a technical protocol and automatically executed without the possibility of external intervention. This model raises fundamental legal questions about determining the legal nature of self-defense in blockchain systems, the limits of autonomy of technical code, and the possibility of legal qualification of blockchain's technical mechanisms as a form of implementation of subjective rights. Research by Raskin (Raskin, 2017) highlights the problem of "digital arbitrary action" in blockchain systems, when technical protection measures can automatically implement sanctions going beyond the limits of lawful self-defense according to traditional legal standards. Of particular relevance is the question of the possibility of legal restitution in cases of erroneous or fraudulent transactions, technical failures, or vulnerabilities in smart contract protocols. Finding a balance between the technical autonomy of blockchain systems and the need to ensure legal protection of participants represents a key problem in forming an adequate legal regime for digital assets and mechanisms for their self-defense.

IV. Discussion

A. Problems of Determining the Legitimacy of Self-Defense in the Digital Environment

Determining the proportionality of protective measures in the digital environment faces fundamental difficulties due to the specifics of information relations and the intangible nature of digital assets. Traditional criteria of proportionality, developed for the material world, are based on the commensurability of the value of the protected object and the harm caused to the violator, as well as on the spatial and temporal limitation of the applied protective measures. In the digital environment, these criteria lose their applicability due to several factors. First, the economic assessment of digital assets represents a complex methodological problem due to their intangible nature, scalability, and dependence of value on the context of use. Research by Timothy (Timothy et al., 2025) reveals fundamental difficulties in determining the economic value of data, algorithms, and digital content, which hinders the application of value-based criteria for the proportionality of protection. Second, in the digital environment, there arises a problem of multiplicity and heterogeneity of potential harm - from direct economic losses to reputational damage, privacy violations, loss of control over data, which are difficult to commensurate with the intensity of the applied protective measures.

Of particular complexity is the assessment of the proportionality of automated technical protection measures functioning without direct human participation. Automated systems implementing algorithmic logic are not capable of taking into account contextual factors and nuances of a specific situation, which leads to the application of unified protection measures regardless of the nature and seriousness of the violation. Research by Mantelero (Mantelero, 2022) analyzes the problem of "algorithmic proportionality" and shows that modern technical protection systems do not possess sufficient flexibility to comply with the legal principle of proportionality. Another aspect of the problem is the temporal unlimitedness of digital protection measures - unlike the physical world, where self-defense usually represents a short-term reaction to an immediate violation, technical protection measures in the digital environment can act for an indefinitely long time, creating permanent limitations for a wide range of persons. Solving the problem of proportionality requires developing special assessment criteria that take into account the informational nature of digital relations, the multi-factor nature of potential harm, and the temporal dynamics of protective measures in the digital space.

The technical complexity of assessing the legitimacy of self-defense actions in the digital environment represents a multi-aspect problem affecting both law enforcement agencies and the participants in digital relations themselves. Courts and other law enforcement bodies face the necessity of analyzing complex technical solutions, the functioning of which requires special knowledge in the field of computer science, cryptography, and network technologies. Research by Michael (Michael, 2011) reveals a systemic problem of the "technological gap" in the judicial system,

when judges do not possess sufficient competencies to evaluate the technical aspects of digital self-defense measures. This gap leads to the formation of simplified and technically incorrect legal positions that do not take into account the complex architecture and principles of functioning of modern information systems. Of particular complexity is the assessment of technical measures based on the newest technologies (artificial intelligence, machine learning, blockchain), the principles of which may be opaque even for specialists due to the "black box" of algorithms or the distributed nature of the system.

The problem of technical complexity is exacerbated by the high dynamics of development of digital technologies, when legal positions and assessment methodologies quickly become obsolete, not keeping up with technological innovations. Research by Mulligan and Bamberger (Mulligan & Bamberger, 2015) shows that the average period of relevance of technical standards in the field of information security is 1-2 years, while the formation of stable judicial practice requires a significantly longer period. This discrepancy in time scales creates constant legal uncertainty regarding new technical self-defense measures. An important aspect of the problem is also the technical complexity of distinguishing between protective, neutral, and offensive technical measures, when the same technologies can be used both for legitimate protection of one's own rights and for unlawful interference in others' information systems. A promising direction for solving this problem is the development of specialized judicial expertise in the field of digital technologies, the formation of interdisciplinary groups for evaluating complex technical solutions, as well as the development of technologically neutral criteria for assessing legitimacy, focusing on the results of applying protective measures rather than on their specific technical implementation.

Risks of exceeding the limits of necessary defense in the digital environment are determined by both technological features of digital protection measures and economic-legal incentives of participants in information relations. Technological risks are associated with the problem of "excessive protection," when technical measures do not possess sufficient selectivity and affect not only the immediate violation but also a wide spectrum of legitimate actions. Systems of content blocking, traffic filtering, and functionality limitation often implement the precautionary principle, preferring to block potentially unlawful content or actions even in the presence of doubts, which leads to a substantial number of false positive triggerings. Research by Leerssen (Leerssen, 2023) based on the analysis of the work of automated content filtering systems in the largest digital platforms shows that the level of false positive blockings can reach 30-40% of the total number of applied protective measures. This situation creates disproportionate limitations for bona fide users and has a "chilling effect" on the realization of fundamental rights in the digital environment.

Economic-legal incentives also contribute to exceeding the limits of necessary defense. The asymmetry of responsibility of internet intermediaries, when the risks of

responsibility for insufficient measures to combat violations significantly exceed the risks of responsibility for excessive limitations, creates structural incentives for a systematic bias toward excessive protection. Of particular danger is the risk of using the institution of self-defense to achieve unlawful goals: suppression of competition, limitation of legitimate criticism, creation of technological barriers to innovation. Research by Edwards (Edwards 2018) analyzes cases of abuse of "notice and takedown" procedures for removing negative reviews, critical materials, and competing products, which actually represents a form of digital arbitrary action under the guise of legitimate self-defense. Minimizing the risks of exceeding the limits of necessary defense requires developing a multi-level system of control: technological solutions for increasing the accuracy of protective measures, procedural guarantees for affected persons, economic incentives for balancing interests, and effective mechanisms for challenging excessive limitations.

B. Cross-Border Nature of Self-Defense of Digital Rights

The cross-border nature of digital relations generates fundamental conflict of laws problems in determining the applicable law when implementing self-defense of digital rights. Unlike traditional forms of self-defense in the physical world, where actions are usually localized within one jurisdiction, self-defense measures in the digital environment often affect multiple jurisdictions simultaneously. Technical protection measures implemented in the global network can impact information systems and users in various countries, which raises complex questions about which state's law should determine the legitimacy of such measures. Traditional conflict of laws connecting factors (lex loci delicti, lex loci protectionis) prove ineffective in the digital space due to the difficulty of determining the place where an action was committed or where its consequences occurred. Research by Svantesson (Svantesson, 2021) reveals systemic problems in applying traditional territorial connecting factors in the internet environment and shows that the absence of clear criteria for choosing applicable law creates a high degree of legal uncertainty for subjects implementing self-defense measures in a cross-border context.

Of particular complexity are cases where various elements of self-defense relations are distributed among different jurisdictions: the rights holder, the alleged violator, the server with content, the target audience, and technical means of protection can be located in different countries with different legal regimes. Research by Trimble (Trimble, 2018) analyzes the problem of "mosaic jurisdiction" in the digital environment and shows that any cross-border self-defense measure potentially must comply with the legal requirements of multiple jurisdictions, which is practically unfeasible due to differences in national approaches to the admissibility and limits of self-defense. This situation leads to the phenomenon of "legal hyperregulation," when the norms of dozens of legal systems with different, often contradictory requirements are potentially applicable to one relationship. A promising direction for solving conflict of laws problems is the development of special connecting factors for the

digital environment, based not on the territorial principle, but on a functional approach that takes into account the specifics of digital relations. Research by Zhang (Zhang, 2023) proposes the concept of "functional targeting," according to which applicable law is determined based on an analysis of the actual orientation of activities toward a specific market or audience, rather than the formal place of actions or location of technical infrastructure.

Territorial aspects of self-defense in the global digital environment generate a complex of problems related to the extraterritorial effect of protection measures and their relationship with the principle of territorial sovereignty of states. Technical protection measures implemented on the internet often have a global impact regardless of the intentions of the rights holder, creating the effect of "global blocking" or "global deletion" of content. The indivisibility of digital infrastructure and technical features of the functioning of network services lead to a situation where self-defense measures that are legitimate in one jurisdiction can automatically extend to users in other jurisdictions, where similar restrictions would be considered illegitimate. Research by Buxbaum (Buxbaum, 2009) analyzes the phenomenon of "indiscriminate extraterritoriality" in the digital environment and reveals a systemic contradiction between the global nature of technical measures and the territorial principle of legal norms. This contradiction is most clearly manifested in cases where a rights holder, implementing self-defense of their rights in accordance with the legislation of one country, actually restricts the legitimate rights of users in other countries with a different legal regime.

The problem of territorial aspects of self-defense becomes particularly acute in the context of differences in national approaches to fundamental issues of information policy: the balance between protection of intellectual property and freedom of information exchange, the limits of permissible state intervention in the information sphere, the relationship between privacy and security. Differences in cultural, political, and legal traditions form significant divergences in national approaches to regulating digital space, which hinders the formation of universal standards of self-defense. In the absence of global consensus, rights holders face the necessity of choosing between several suboptimal strategies: applying the strictest protection measures that comply with the requirements of the most restrictive jurisdiction; territorial differentiation of protection measures, requiring complex technical solutions; limiting activities to the most loyal jurisdictions. A promising direction for overcoming territorial problems is the development of geoblocking and geofiltering technologies, allowing adaptation of self-defense measures to the legal requirements of specific jurisdictions. However, these technologies themselves generate risks of fragmentation of the global digital space and creation of "digital borders" contradicting the open nature of the internet.

C. Balance of Interests in the Implementation of Self-Defense of Digital Rights

The conflict between self-defense measures and the rights of bona fide users

represents a fundamental problem in implementing the institution of self-defense in the digital space. Technical protection measures applied by rights holders often have an undifferentiated character and affect not only violators but also bona fide users, creating barriers to legitimate access to information and digital resources. This conflict is most clearly manifested in the context of Digital Rights Management (DRM) systems, which can impede the implementation of legitimate exceptions to copyright: the doctrine of fair use, personal non-commercial use, use for educational and scientific purposes, creation of backup copies. Research by Aufderheide and Jaszi (Aufderheide & Jaszi, 2019) reveals a systemic contradiction between the technical capabilities of DRM systems, which can block virtually any use of a work without the permission of the rights holder, and the conceptual structure of copyright, which implies a balance between the monopoly rights of the author and the public interest in access to information. This contradiction is exacerbated by legislative prohibitions on circumventing technical protection measures even for legitimate purposes, which actually leads to an expansion of the scope of exclusive rights through technological mechanisms.

The asymmetry of informational capabilities and resources between rights holders and users adds particular acuteness to the conflict. While large rights holders can invest significant funds in the development and implementation of technical protection measures, individual users often have neither the technical knowledge nor the financial resources to effectively challenge illegitimate restrictions. Research by Elkin-Koren and Fischman-Afori (Elkin-Koren & Fischman-Afori, 2017) analyzes the structural imbalance of negotiating possibilities in the digital environment and shows that self-defense mechanisms create a system of "one-sided law enforcement," where the user is effectively deprived of the ability to effectively protect their legitimate interests. This situation is especially problematic for vulnerable categories of users: persons with disabilities, whom technical protection measures may hinder in using assistive technologies; educational and scientific organizations in developing countries, for which access to protected content is critically important but often limited by protective mechanisms; representatives of creative professions who use existing works to create new creative works within the framework of legitimate borrowing. Finding a balance between effective protection of rights and the interests of bona fide users requires a comprehensive approach, including the improvement of technical solutions for more differentiated application of protective measures, legislative establishment of exceptions to the prohibition on circumventing technical protection measures for legitimate purposes, and creation of accessible mechanisms for challenging illegitimate restrictions.

The interaction of public and private interests in the context of self-defense of digital rights represents a multi-aspect problem affecting the fundamental principles of regulating the information society. The private interests of rights holders are aimed at maximum protection of exclusive rights, prevention of unauthorized use of content, and monetization of digital assets. The implementation of these interests through

technical self-defense measures allows rights holders to effectively control the use of their works on a global scale without the need to resort to state law enforcement mechanisms. However, the active application of technical protection measures by private subjects potentially affects significant public interests, including ensuring access to knowledge and cultural heritage, development of education and science, stimulation of innovation, protection of competition, and prevention of monopolization of information markets. Research by Boyle and Jenkins (Boyle & Jenkins, 2021) reveals a fundamental contradiction between the short-term economic interests of rights holders in maximum protection of content and the long-term public interests in an open innovative environment, free information exchange, and productive use of intellectual resources.

Public interests in the context of self-defense of digital rights are manifested at several levels. At the level of information policy, states are interested in ensuring a balance between protection of rights and maintaining an open information environment necessary for economic development, scientific progress, and cultural diversity. At the level of protection of fundamental rights, the public interest lies in preventing excessive restrictions on freedom of expression, access to information, and the right to private life as a result of the application of technical protection measures. At the level of economic policy, public interests include preventing monopolization of digital markets through technological barriers, ensuring interoperability and competition, and stimulating innovation. The balance of public and private interests requires a multi-level approach, including the establishment of legislative limitations on technical protection measures to ensure public interests, the creation of alternative compensatory mechanisms for rights holders (systems of collective licensing, tax benefits), and the stimulation of voluntary initiatives to expand access to knowledge and cultural values.

The problem of abuse of the right to self-defense in the digital space acquires special relevance in conditions where technical protection measures and self-help procedures can be used not only for legitimate protection of digital rights but also for achieving illegitimate goals. Abuses take various forms: using notification and content removal procedures (notice and takedown) to suppress criticism, political statements, or competing products; applying technical restrictions not to protect copyright, but to create artificial barriers in the market and limit competition; presenting knowingly unfounded claims of rights violation to obtain license payments from persons who do not have resources for legal defense (so-called "patent trolling" in the digital environment).

Of particular danger is the use of technological mechanisms of self-defense for offensive actions against alleged violators or competitors. Technical measures, initially developed to protect one's own information systems, can be transformed into tools of active influence on others' systems or network infrastructure: blocking of IP addresses, DDoS attacks, introduction of malicious code under the guise of protective

mechanisms, automatic deletion of content on third-party platforms without sufficient evidence of violation. Preventing abuses of the right to self-defense requires a comprehensive approach, including: clear legislative regulation of permissible self-defense measures in the digital environment; effective procedures for challenging unfounded requirements and sanctions for unfair use of self-defense mechanisms; development of independent bodies for resolving information disputes, ensuring prompt and competent consideration of conflicts in the digital environment; technological solutions for increasing the transparency and accountability of self-defense measures.

D. Recommendations

Based on the conducted research, several recommendations can be formulated to improve the legal regulation of self-defense in the digital environment. First, it is necessary to modernize legislative norms on the self-defense of rights by considering the specifics of the digital environment. This includes introducing special provisions into the Civil Code of the Republic of Uzbekistan that detail the criteria for the legitimacy of self-defense of digital rights while taking into account the technological context of its implementation.

Additionally, the development of specialized legislation on technical measures for the protection of digital rights is crucial. This legislation should establish a balance between effective protection and the legitimate interests of users. It should define exceptions to the prohibition on circumventing technical protection measures for legitimate purposes such as education, scientific research, and ensuring access for persons with disabilities. Furthermore, it should establish requirements for transparency and predictability of technical protection measures for end users and regulate procedures for challenging excessive technical restrictions.

The procedural aspects of self-defense of digital rights also require improvement. This can be achieved through the regulation of the "notice and takedown" procedure by setting clear requirements for the validity of notifications and establishing effective mechanisms for challenging them. Additionally, sanctions should be introduced for the unfair use of self-defense mechanisms. To further enhance digital rights protection, specialized mediation bodies should be created to facilitate alternative dispute resolution in information-related conflicts.

International cooperation is another key area that needs to be strengthened. Uzbekistan should actively participate in the development and implementation of international standards for technical protection measures. Harmonizing national legislation with international norms in the field of digital rights protection will also be essential. Moreover, the creation of effective mechanisms for cross-border interaction is necessary to prevent and suppress violations of digital rights.

Conclusion

The research showed that the conceptual foundations of self-defense of rights in the digital space are significantly transformed under the influence of specific characteristics of the digital environment. The traditional understanding of self-defense as factual actions of an authorized person is expanded through the inclusion of technological mechanisms, which become the main instrument for implementing the right to self-defense in the digital context. The phenomenon of convergence of legal norms and technical code emerges, where software and technical means actually perform the function of law implementation and law enforcement. This transformation generates the need to adapt legal criteria of self-defense (proportionality, necessity) to the technological context of the digital space.

The analysis of legal boundaries of self-defense of digital rights revealed significant difficulties in determining the limits of legitimate actions of subjects. The criterion of proportionality of protection to the violation, which is key for traditional self-defense, requires substantial modification in the digital environment, where the assessment of the value of information objects and potential harm from violation has a multi-factor nature. A particular problem is determining the legitimacy of preventive self-defense measures, which acquire priority importance in the digital space but create risks of excessive restriction of the rights of bona fide subjects.

The research showed a variety of forms of implementing self-defense in the digital space, including technological measures (encryption, blockchain, DRM systems), contractual mechanisms (license agreements, smart contracts), and organizational procedures (monitoring, notifications, content removal procedures). Each of these forms has specific legal characteristics and requires a differentiated approach to determining the boundaries of legitimacy. Practice shows that the highest effectiveness is demonstrated by complex self-defense systems combining various forms and mechanisms.

The research revealed significant peculiarities of self-defense of various types of digital rights. Self-defense of personal data faces the problem of asymmetry of informational capabilities of subjects and the cross-border nature of information processing. Self-defense of intellectual property objects in the digital environment is transformed under the influence of technological possibilities for controlling the use of works and new economic models of content monetization. Self-defense of property digital rights in the context of cryptocurrencies and tokens forms a fundamentally new paradigm, where technical mechanisms directly determine the scope and content of property rights.

The analysis of problems of determining the legitimacy of self-defense in the digital environment confirmed the necessity of developing special legal assessment criteria that take into account the technological specifics of protective measures and their potential impact on the rights of third parties. A significant problem is the technical complexity of assessing the legitimacy of self-defense actions, requiring special knowledge and methods, as well as risks of exceeding the limits of necessary

defense due to the automated nature of the applied technical measures.

The research confirmed the cross-border nature of self-defense of digital rights and related conflict of laws problems of determining applicable law, territorial aspects of implementing protective measures, and the necessity of international cooperation in this field. Of particular importance is finding a balance of interests of various participants in digital relations: rights holders, bona fide users, and society as a whole, as well as preventing abuses of the right to self-defense.

Bibliography

Asay, C. D. (2015). Copyright's technological interdependencies. *Stanford Technology Law Review, 18*, 189.

Aufderheide, P., & Jaszi, P. (2011). *Reclaiming fair use: How to put balance back in copyright*. University of Chicago Press.

Ausloos, J., Mahieu, R., & Veale, M. (2019). Getting data subject rights right. *JIPITEC, 10*, 283.

Balkin, J. M. (2020). The fiduciary model of privacy. *Harvard Law Review Forum, 134*(1).

Bamberger, K. A., & Mulligan, D. K. (2015). Privacy on the ground: Driving corporate behavior in the United States and Europe (Chapter 1).

Boyle, J., & Jenkins, J. (2021). *Intellectual property: Law & the information society—Cases and materials* (5th ed.).

Buxbaum, H. L. (2009). Territory, territoriality, and the resolution of jurisdictional conflict. *American Journal of Comparative Law, 57*(2), 631-676.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Edwards, L. (Ed.). (2018). *Law, policy and the internet*. Hart Publishing.

Egamberdiev, E. K. (2021). Objects of the virtual world under German law. *YOUNG SCIENTIST*, (51), 284-287.

Egamberdiev, E. K. (2023a). Internet of things and blockchain in the field of data trading. In *Current issues of modern science* (pp. 163-167).

Egamberdiev, E. K. (2023b). Some problems of determining the civil-legal status of the virtual world and its objects.

Egamberdiev, E. K. (2023c). Online accounts as objects of social relations. *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences, 3*(8), 205-229.

Egamberdiev, E. K. (2023d). Internet of things technologies and personal data: Issues of property rights. *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences, 3*(1-2), 541-558.

Elkin-Koren, N., & Fischman-Afori, O. (2017). Rulifying fair use. *Arizona Law Review, 59*, 161–200.

Finck, M. (2019). *Blockchain regulation and governance in Europe*. Cambridge University Press.

Grimmelmann, J. (2015). The virtues of moderation. *Yale Journal of Law and Technology, 17*, 42–109.

Haeringer, G., & Halaburda, H. (2018). Bitcoin: A revolution? In J. Ganuza & G. Llobert (Eds.), *Economic analysis of the digital revolution*. FUNCAS.

Hildebrandt, M. (2020). Law, democracy, and the rule of law. In *Law for computer scientists and other folk*. Oxford University Press.

Hugenholtz, P. B., & Quintais, J. P. (2021). Copyright and artificial creation: Does EU copyright law

protect AI-assisted output? *IIC*, *52*, 1190–1216.

Karapapa, S. (2020). *Defences to copyright infringement: Creativity, innovation and freedom on the internet*. Oxford University Press.

Keller, P. (2013). *European and international media law: Liberal democracy, trade, and the new media*. Oxford University Press.

Khajibaevich, E. E. (2023). Civil law status of virtual world objects. *Eurasian Research Bulletin, 16*, 33-41.

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review, 48*.

Lemley, M. A., & Reese, R. A. (2004). Reducing digital copyright infringement without restricting innovation. *Stanford Law Review, 56*(6), 1345-1434.

Loos, M., & Luzak, J. A. (2016). Wanted: A bigger stick. On unfair terms in consumer contracts with online service providers. *Journal of Consumer Policy, 39*(1), 63.

Mantelero, A. (2022). Beyond data. In *Beyond data. Information technology and law series* (Vol. 36). T.M.C. Asser Press.

Mazziotti, G. (2008). *EU digital copyright law and the end-user*. Springer Science & Business Media.

Michael, A. (2011). *Innovation for the 21st century: Carrier* (1st ed.). Oxford University Press.

Murray, A. (2019). *Information technology law: The law and society* (4th ed.). Oxford University Press.

O'Leary, T. J., O'Leary, B. J., & O'Leary, D. P. (2025). A perspective on artificial intelligence for molecular pathologists. *The Journal of Molecular Diagnostics.*

Peukert, C., & Windisch, M. (2024). The economics of copyright in the digital age. *Journal of Economic Surveys*, 1–27.

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review, 1*, 304.

Reed, C., & Murray, A. (2018). *Rethinking the jurisprudence of cyberspace.* Edward Elgar Publishing.

Savelyev, A. (2016). Contract law 2.0: «Smart» contracts as the beginning of the end of classic contract law (*Higher School of Economics Research Paper No. WP BRP 71/LAW/2016*).

Seng, D. K. B. (2014). The state of the discordant union: An empirical analysis of DMCA takedown notices. *Virginia Journal of Law & Technology, 18*, 369.

Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review, 89(1).*

Svantesson, D. J. B. (2021). *Private international law and the internet.* Wolters Kluwer.

Trimble, M. (2020). Intellectual property law and geography. In I. Calboli & M. L. Montagnani (Eds.), *Handbook on intellectual property research*. Oxford University Press.

Urban, J. M., Karaganis, J., & Schofield, B. (2017). *Notice and takedown in everyday practice* (*UC Berkeley Public Law Research Paper No. 2755628*).

Werbach, K. (2018). *The blockchain and the new architecture of trust.* The MIT Press.

Wu, T. (2016). *The attention merchants: The epic scramble to get inside our heads.* Faculty Books.

Zhang, Y. (2023). The regulation of the digital markets. *International Journal of Education and Humanities, 9(2).*