CIVILTIESĪBU APAKŠNOZARE

LEGAL STATUS OF THE DIGITAL PROFILE OF THE CIVIL LEGAL RELATIONS' SUBJECTS

Anna Rozhkova,
Candidate of Economical Sciences,
Federal state budgetary institution of higher education "Pskov State University",
Associate Professor of the Pskov State University, Pskov, Russia
E-mail: annroz80@yandex.ru

Inna Andreyanova,
PhD in Law, docent, the Head of the Competence Development Department at Novgorod State University Named after Yaroslav the Wise, the Director of the Pskov Branch of the Russia's Society "Knowledge", the Public Chamber's Deputy Chairman of the Pskov Region, Russia
E-mail: jurist-i@mail.ru

Abstract

The aim of the work is a legal risk assessment to identify subjects of civil relations in order to implement commercial transactions safely using a digital profile. The paper attempts to assess the digital transformation of civil relations and the implementation of legal regulators for the protection and security of the subjects' digital profile of. The aspects of "digital profile's" definition interpretation as well the legal status separate signs for citizens and business entities of the notification procedure, differentiation of both rights to dispose and to use are reflected. The law enforcement practice of civil transactions in the course of digital resources' turnover, as well as the attraction and imposition of administrative penalties are proposed, and a number of conflicts is identified due to the latency of illegal actions, the lack of digital competent human rights bodies and digital investigative tools.

Keywords*: subject of civil legal relations, digital profile, disposal and use of digital profile, right of possession and right of use, notification procedure, digital security.*

Introduction

In terms of digital transformation of the economics and reforming the legal regulators, it is necessary to review the status of civil legal relations' subjects in terms of interpretation *the legal status of a digital profile, disposal and use of profile data* to implement the digital transactions and to ensure the digital security of the state authorities.

Digital transformation of civil legal relations is caused by *advantages and risks* in the conditions of technological infrastructure formation in access to professional integration platforms, software products, cloud solutions (for example, such as Counterparty of mining transactions; Counterwallet of transaction protocol, smart contracts, crowdfunding; Ethereum contracts, deposits, financial derivatives, and others). The advantage of a digital profile and its data for subjects of civil legal relations is a reduction in transaction costs for finding customers and partners for implementing digital transactions using platform constructors on the example of the "one electronic window" mode. However, access to digital resources is also considered as a technological risk in significant resource costs for acquisition, maintenance, consumption, and security. According to M. V. Starichkov, the cost growth up to $6 billion is due to the introduction of rules to limit the volume of data in industries such as banking, financial services, and insurance (BFSI)[1], as well as bans and restrictions to ensure public safety.

https://doi.org/10.17770/acj.v1i89.5319

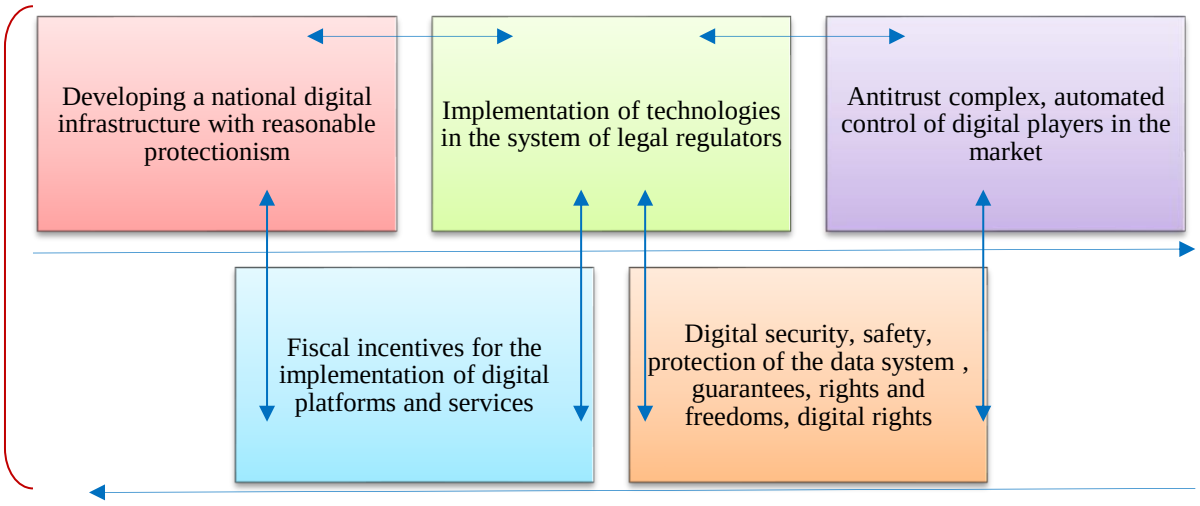

Fig. 1 Strategic directions of legal regulation on digital technology implementation

Digital transformation of business-processes is synchronized with the corporatization of legal relations due to the accumulation of the software products, digital resources, Big Date, and personal data's markets by leading companies, thereby creating risks of a dominant position that contradicts the law provision[2]. In addition, legal risks arise for business entities in the absence of their legal guarantees, protection, and security due to the *redirection of digital competencies in favour of IT* companies. In this regard, for the purpose of legal protection of competition in the digital market, legal guarantees of digital security, legal regulators determine the procedure for implementing digital automated systems (EGISSO) in the exercise of authority by the state authorities (see Fig.1) in the development of a centralized national digital infrastructure.

In connection on trends, the subject of the study is the legal risks associated with the legal nature's transformation of the digital transactions' status of subjects; the object of the search is the legal understanding of the digital profile as a tool for protecting the data of the civil relations' subject.

Body

Let's define several legal regulators for establishing the legal status of the individuals and business entities' digital profile, some of which shall enter into legal force in 2020-2021.

According to the Decree of the Russian Federation Government dated 29.10.2019 N 1382 in terms of *security standards* of the digital economy, the imperative of *identifying* a digital profile is established. In accordance with the Order of the RF Ministry of labor dated 28.05.2019 N 362, in order to establish the *identification procedure* the following is provided:

- transfer of legal information to subjects of legal relations on the principle of access, completeness and reliability on digital state platforms;
- unified monitoring and control of accounts by a centralized system;
- notifiable and verifiable database order.

In accordance with the RF Government Resolution N 1311 dated 11.10.2019 on personification, identification of physical persons and means of business entities' individualization, in order *to control* the exchange of traffic and legitimate details, the registry is fixed by the legislator in parts: the ID, the point of traffic exchange DataLine-IX (Internet Exchange Point, IX) peering, IP - address of the subject.

Separately for individuals, according to Ablameyko M. S.[3], personal data of the digital profile includes "physiological and biological features of a person for identification and data processing with the written consent of the subject", including the provision of personal ID cards while initiating the Belarusian integrated service and accounting system (BISRS).

In Russia in the draft Law N 750699-7 – FZ dated 16.10.2019 it is planned to secure *legal status of* personal data composition *digital profile* by using biometric data of the unified system, for the

purpose of digital legal competence and capacity to execute transactions with the use of a reinforced qualified signature, protection of rights and guarantees of contractual relations' the parties. The digital profile includes personification, identification, and double authentication, as well as an automated system for verifying the information of the legal entity.

According to the draft Federal law N 747513-7: "A digital profile is a collection of information about citizens and legal entities that are located in various state information systems." However, in ensuring the legality and criteria for access to" special data", we assume the need to establish a conciliation and notification procedure. This procedure shall create conditions for personal security of legal entities, protection of private integrity, commercial and banking secrets of business entities. Therefore, it is proposed to clarify the definition: *"A digital profile is a collection of personal information that is located in various state information systems while ensuring compliance with the notification and conciliation procedure."*.

For the purpose of interpreting the legal nature, let's consider the definition of "digital profile" from the point of view of private and public laws, in order to distinguish the rights to a digital profile. From the point of private law's view in the context of non-property rights, the digital profile is the subject of copyright ownership and disposal in accordance with article 1229 of the RF Civil Code. Thus, part 1 of article 1229 of the RF Civil Code states: "a citizen or legal entity that has an exclusive right ... on the means of individualization, shall use ... at own discretion in any way not contrary to the law."

In accordance with the regulation of article 3 of Law N 152-FZ[4], the subject of public law is the procedure for establishing, processing and controlling the personal data of a digital profile as well as the procedure for using and guaranteeing security in order to ensure the actions' legality of digital profile's administrators and users. It is obvious that the administrator is a subject of legal relations as a bearer of digital profile data, and the user is the counterparty of the digital transaction, as well as government agencies, including operators.

It should be noted that in accordance with Chapter 3 of Law N 152-FZ, the rights of a personal data subject to access to data, automated processing and rights to promote transactions are secured. However, this interpretation[5] does not allow to disclose the private and public rights of a subject of civil legal relations of a digital profile. In this case, the legal nature of the digital profile's intersectoral nature allows to establish special private rights and public entitlements of subjects. In this regard, the author's wording on the definition of subjects of the digital profile is proposed: *"Administrators are the right holders of the digital profile who have the right of personal data disposal and, or by means of individualization in accordance with the law. Users are entities that have obtained access to the digital profile and use the data in a notification and conciliation manner by the copyright holder, which does not contradict the law, for the purpose of monitoring and guaranteeing security".* The proposed recommendations may supplement the provisions of articles 6 and 10 of Law N 149-FZ[6].

Let's return to the definition of the digital profile "set of data"[7]. Because of the classification information of the subject; the special characteristics of the legal status of physical entity and economic entity; a conciliation and notification order to the digital profile applicability; the special rights and powers of entities to manage and use digital profile, it is proposed to identify the separate formulations of a digital profile of physical entity and economic entity.

According to the RF Civil Code's § 4 of chapter 76, the means of individualization refer to business activity, which also applies to an individual entrepreneur who has an intersectoral legal status in the availability of civil and business rights. Therefore, for such citizens – individual entrepreneurs, personal data will also be included in the means of individualization. Due to these features, it is proposed to supplement the norm of part 1 of article 1229 of the RF Civil Code as follows: "1. A citizen or a legal person having the exclusive right to means of individualization of *a digital profile*, may use *a digital profile*, at its discretion, not any illegal. The copyright holder may, at own discretion, allow or prohibit the others using *the digital profile* individualization tool." This wording it is not contrary to article 12 of the RF Civil Code, paragraph 10 of the RF Supreme Court's[8] Resolution of Plenum ("According to the meaning of the RF Civil Code's articles 1 and 14 the self-defense of civil rights may be expressed, including the person impact on property both of his own and in his lawful

possession") and part 2–4 of article 1 of the Federal law "On amendments to certain legislative acts (regarding procedures for identification and authentication) on the granting of digital rights and measures of identification and authentication" draft.

In general, taking into account the identified special legal features, the author's understanding of the digital profile of subjects is offered. For individuals: *"A digital profile is a set of personal and biometric data of an individual that is located in various state information systems, which are the subject of copyright ownership and disposal based on the principles of legality, reliability, availability, authentication, completeness, while ensuring compliance with the notification and conciliation procedure in order to protect the rights of holders and users of a digital profile."* For business entities: *"A digital profile is a set of digital means of individualization of a person that are located in various state information systems, which are the subject of copyright ownership and professional disposal in order to ensure the legal capacity to perform digital transactions based on the principles of legality, reliability, availability, and double authentication."* At the same time, passwords and logins of *a digital profile*, acting as means of belonging to a specific user, allow to grant him digital access rights and security. These features of the *digital profile* correlate with the obligations of network (digital) operators of digital platforms not to disclose confidential content to third parties, including corporate digital profiles without notification and conciliation.

The legal status of the digital profile is determined by tracking the digital footprint: when confirming the consent of the reinforced digital signature in the implementation of electronic transactions with real estate, the implementation of small civil transactions with quick payment operations using a QR-code[9], the use of a corporate e-wallet (Federal law dated 03.07.2019 N 173-FZ). For example, in order to account the digital footprint while reducing the cost of "working with a single biometric system" (ESIA)[10], remote Digital client paths are provided without the personal presence of the borrower subject in the conditions of multi-modality "voice and face" of "a person alive" and detection of fakes. When performing digital transactions using decentralized solutions (BIockchain, Sidechains, Treechains) regarding property relations to Smart property, Transferable virtual property, data accumulation is provided. Therefore, in accordance with the Order of the RF Government dated 28.08.2019 N 1911-r, the following organizational and legal means are significant:

- agency with standalone programs - Distributed markets;
- implementation of the state information system (GIS);
- service model of a cloud platform for providing state and municipal services[11] to ensure the rights to security and access to reliable complete information for subjects.

According to the draft Federal law N 747528-7, the legal status of the subjects' digital profile of in the implementation of digital transactions is provided with security in the form of double authentication for individuals and a qualified certificate in the use of electronic signatures by legal entities.

The digital rights of a profile are protected by a guaranteed measure of live signature by a written statement. Thus, according to the draft Federal law "On amendments to the Federal law "On personal data"" dated 18.09.2019, there shall be one written consent of a person to use personal data related to actions for different purposes. However, this circumstance is contradictory due to the "difference of purposes" of actions, which requires the establishment of actions based on one purpose in order to avoid violations of rights. generic characteristics of Thus, the Resolution of the Ninth arbitration court of appeal N 09AP-30182/2016-AK dated 16.08.2016, concerning the case N A40-17595/16 has installed: "Skartel, Ltd., providing transmission of employees' personal data to third parties, uses standard written form of consent to the processing of personal data of the employee for the multiple purposes of personal data processing that violates the requirements of paragraph 4 of part 4 of article 9 of the Federal law dated 27.07.2006 N 152-FZ "On personal data".

A simple violation, as improper data security provision by Decree N 4A-363/2019 4A-383/2019 dated April 24, 2019, concerning the case N 4A-363/2019 is proved in terms of leaving applications with personal data in public access to visitors, was the basis for bringing FSUE "Russian Post" to administrative responsibility in the amount of 25,000 rubles.

In general, the dynamics of situations[12] related to illegal actions, voice imitation, demonstrates the main types of threats to digital profile data leakage in Fig. 2, where there shown a 1,215-fold excess of malicious software tools relative to other types. The "man in the middle" attack (MitM attacks)[13] poses a threat in terms of simulating an interlocutor between the computer and the router during initialization, and there are leakage risks when transmitting confidential data from the IP-address. The "sorting" method and denial of service account for 42 % of the hazard level.

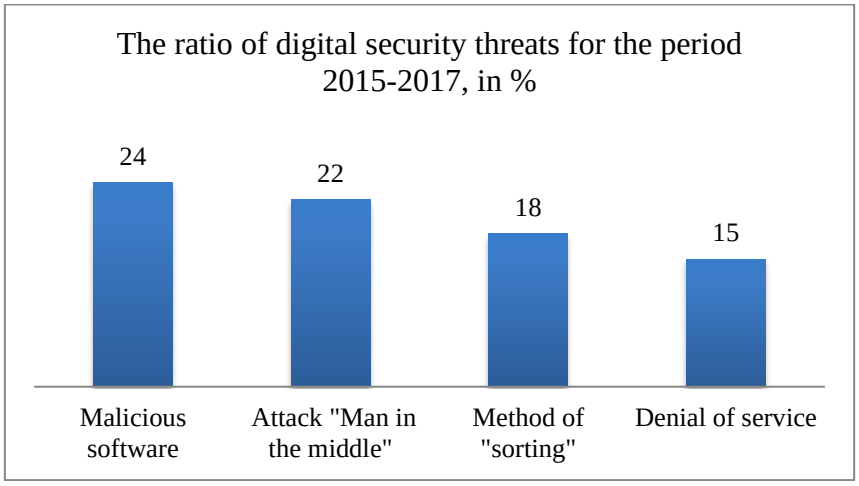

Fig. 2 The main types of digital security threats

According to the regulation of article 13.11 of the RF Code of Administrative Offences, administrative responsibility for illegal actions has a negligible level of punishability in the form of administrative fines. So, in terms of improper security[14]- these are only a warning or a fine, which collectively amounts to an average of 11,500 rubles for officials and business entities, which devalues the guarantees of the legal status of the security of the digital profile. Therefore, in accordance with the draft Federal law N 729516-7, for improper provision, including in accordance with the regulation of article 19.7 of the RF Code of Administrative Offences - failure of information provision or violation of deadlines, provides for amendments to the legislation to increase penalties for business entities and officials in the following positions:

- from 200 thousand to 500 thousand rubles for officials (for repeated violations – from 500 thousand to 1 million rubles);
- from 2 million to 6 million rubles for legal entities (for repeated violations – from 6 million to 18 million rubles).

In general, according to article 13 of the RF Code of Administrative Offences, for the reporting period of the first half of 2019 (see Fig.3) the main share is accounted for illegal actions committed by officials (66,36 %) and (23,5 %) – by economic entities. At the same time, the data in Fig. 3 shows that warnings exceed fines by 12,68 %, which indicates the need to increase the level of punishability of perpetrators.

According to the Federal law dated 02.12.2019 N 405-FZ to the regulation of article 13.11 of the RF Code of Administrative Offences – for failure to "ensure recording, systematization, accumulation, storage, refinement or extraction of personal data", the administrative punishment is reinforced: "for citizens in the amount from 50 thousand to 100 thousand rubles; for officials – from 500 thousand to 800 thousand rubles; for legal entities – from 6 million to 18 million rubles". At the same time, we normally observe an inaccuracy that "storage" can be interpreted as data accumulation. Therefore, we suggest a clarification: in the norm 13.11 to add duties for the operators of the information sphere in terms of protective actions for the security of digital profile data.

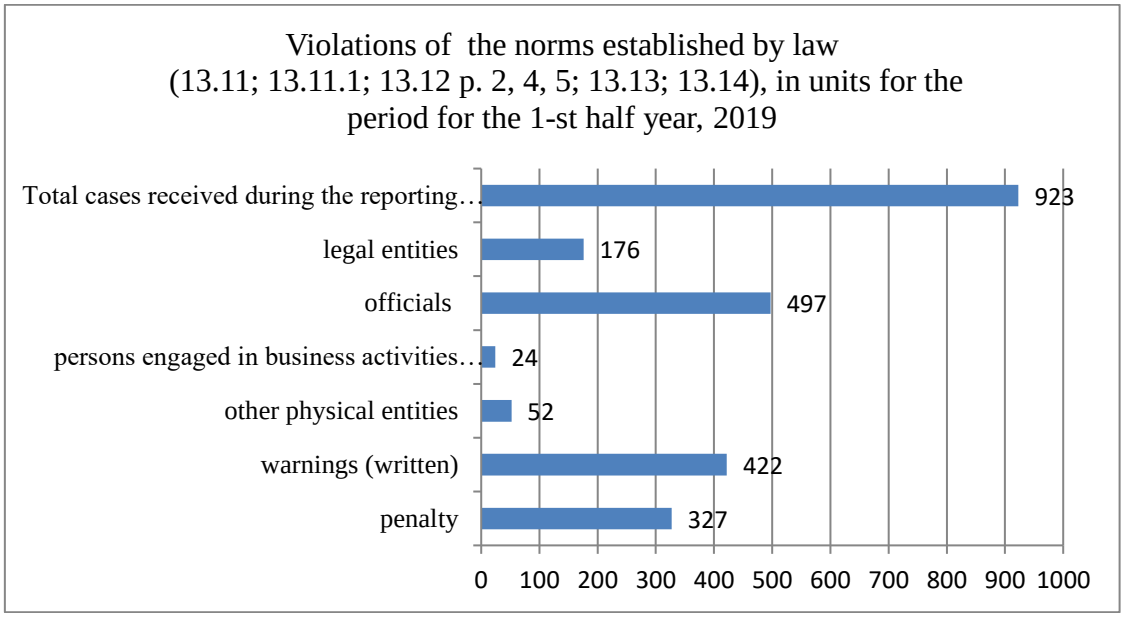

Fig. 3 Overview of the number of persons brought to administrative justice

In accordance with the regulation of the RF Code of Administrative Offences', article 3.11 a more stringent measure is provided – such as disqualification of officials for up to three years, and the RF Code of Administrative Offences' articles 3.8 and 13.12, 13.13 – deprivation the special rights for legal entities "not less than one month and more than three years." But article 273 of the RF Criminal Code reads: for spreading malicious programs by a person "using own official position" includes "disqualification to hold certain posts or practice certain activities for a term up to three years." However, there is a conflict under article 311 of the RF Code of Administrative Offences and RF Criminal Code of equal appointments article 273 for the terms of preventive measures on both administrative and criminal penalties – which suggests increasing the time up to the establishment of a total ban to hold office and to carry out certain activities, according to the article 273 of the RF Criminal Code.

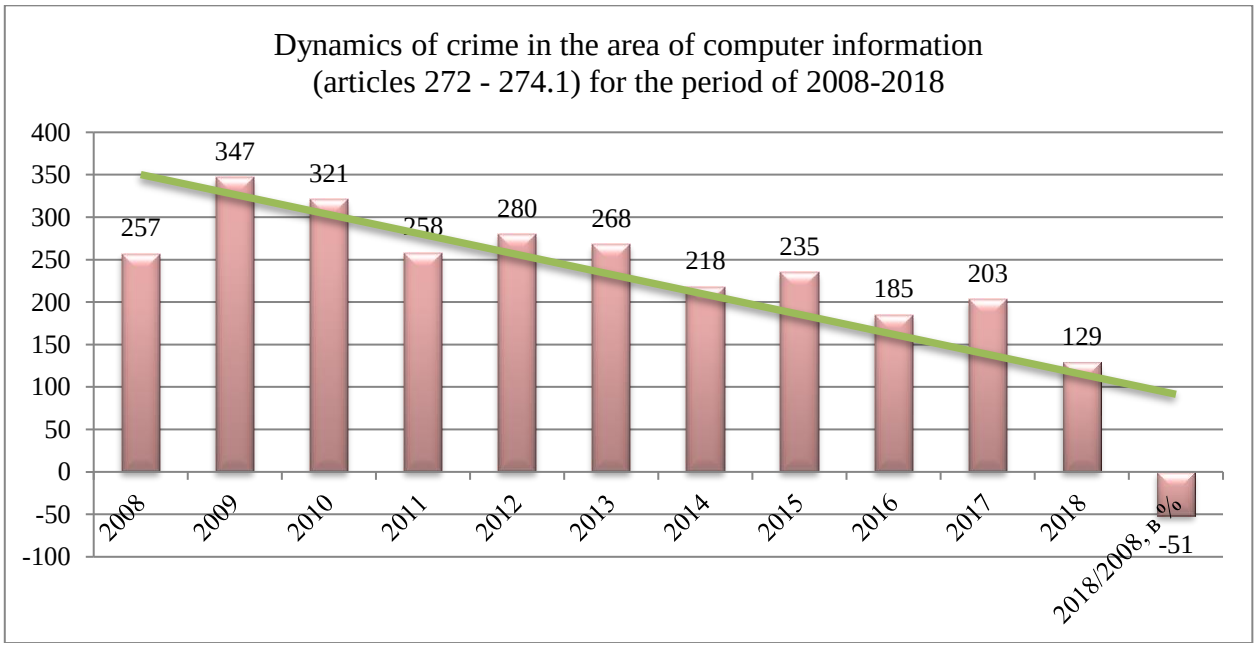

Fig. 4 Decreasing trend of computer crimes

In turn, article 272 of the RF Criminal Code for unlawful access to computer information, namely illegal access to personal, biometric data, as part of a digital profile[15], incriminates up to two

years in prison, with serious consequences – up to 7 years. However, the dynamics of crimes under article 272 of the RF Criminal Code for the period 2008-2018 (see Fig. 4)[16] has a declining trend of up to 51 % of the base period – which indicates, on the one hand, a positive fact, and on the other hand, a likely latency of crimes due to the lack of competence of regulators regarding the procedure for ensuring digital security.

For the period of the 1st half of 2019, data from the judicial department[17] (see Fig.5) demonstrate: the main penalty in the form of a fine is 18 %, in the form of liberty restriction – 28 %; a suspended sentence of imprisonment is 41 % due to extenuating circumstances established by the court (86 %) – which indicates a humane approach to the proceedings and is rather preventive in nature of punishments.

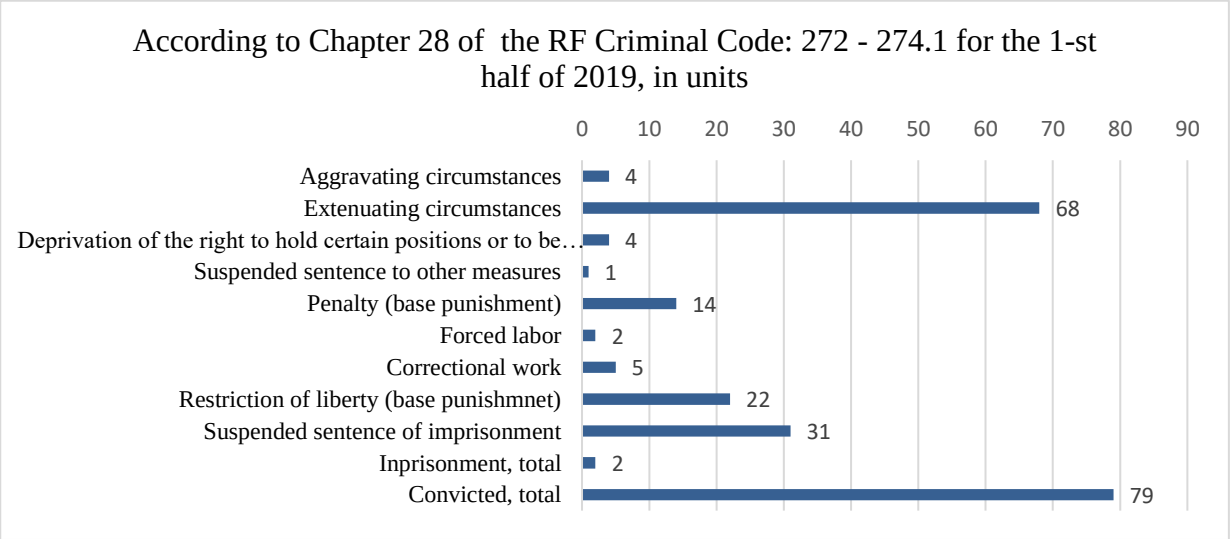

Fig. 5 The ratio of criminal punishment types to the circumstances

Unfortunately, in practice, civil legal relations of subjects are associated with the implementation of illegal commercial transactions, in which the copyright of the software copyright holders may be affected. Thus, by Resolution N 1-313 / 2019 dated 30.05.2019, a fine was imposed in case N 1-313/2019. For the illegal selling and delivery of commercial software services without permission (i.e., without a franchise), as well as for introduction of the malicious "hacking" programme "ArchiCAD.exe", taking into account extenuating circumstances, the defendant was charged with a criminal penalty of moderate severity, in the form of a fine of 20 thousand robles for violating the copyright protection of the software product's "ArchiCAD 12" copyright holder. At the same time, the fact of penetration into the digital profile of the copyright holder was the downloading of a software product without observing the notification and conciliation procedure. In this case, we assume that the solution to the problem of such actions as to purchase a product from the copyright holder is appropriate to introduce a digital offer for the conclusion of a franchise. As we can see, the regulator's establishment of a digital contractual relationship procedure will ensure the protection of the digital profile and the digital rights of the parties, instead of simply prohibiting access to the profile.

When assessing the corpus delicti, a fact was revealed demonstrating competence of law enforcement authorities' lack of regarding digital illegal manipulation of software products. So, Resolution N 1-99/2019 dated 24.05.2019 concerning the case N 1-99/2019 has identified the absence of a crime under the RF Criminal Code's paragraphs "b" part 3 article 146, part 1 of article 273, part 1 of article 272. At the same time, operational commissioners conducted investigative actions extracting the evidence for counterfeit products[18] for the purpose of illegal sale and making a profit by the defendant. The court received storage devices of computer information on licensing products for their further illegal installation (without the agreement with the right holder)[19], the video and information about using the software unauthorized hacking (without activation or purchase of the certificate)[20]. However, during the "Verification purchase" and the buyer's testimony, the evidence

obtained was not confirmed, and the state prosecutor found that there was no evidence of a crime, which was the reason for the termination of criminal proceedings for lack of the crime proof. This fact shows that digital crimes can be solved by legally granting additional digital powers, using digital search tools to obtain digital evidence.

Conclusions

In conclusion, we note the summary and results.

1. The relevance of the advantages and risks of civil legal relations' digital transformation is indicated.
2. Novelties of legislation in the implementation of digital technologies to determine the legal status of the digital profile, identification and authentication, regulation of digital rights and guarantees of subjects in the implementation of secure digital transactions are presented.
3. Clarifications are given on the interpretation of the "digital profile's" definition, specifying special features – which allow to disclose the legal status separately for individuals and legal entities of civil relations under the imperative of the conciliation and notification procedure.
4. The peculiarities of the digital profile' legal nature of a concerning copyright holding and its disposal are specified, in which the clarification of the rules of the RF Civil Code's part 1, article 1229 concerning the use of exclusive rights to digital profile is proposed.
5. The rights to the digital profile for administrators and separately for users are clarified, that allows to distinguish between private and public rights and establish special private rights and public right powers of subjects. In this context, the author's understanding interpretation of who the administrators and users of the digital profile are, is proposed.
6. Due to the different legal nature of information about citizens and business entities, clarifications to the regulation of the RF Civil Code's art. 1229 in the understanding of the digital profile's copyright holding are proposed, which will ensure digital rights of access and self-defense for subjects of civil relations in the implementation of digital transactions. Hence, the legal interpretation of the individuals and separately for economic entities' digital profile is given. In addition, the digital profile has the property of modification due to the accumulation of digital traces, which in turn depend on the situation and demands of civil relations' subjects.
7. Based on static analysis, the number of low levels of punishability problems was identified, limited to warnings and penalties, especially for officials responsible for public safety and carrying the administrative and competent resources. 8. Based on the judicial analysis, the positive dynamics of reducing computer crime and the use of preventive measures were revealed. However, it was found that because of unlawful actions' latency in digital format, the implementation of digital tools and digital competences for the fulfilment of search actions is required, as well as barring the access to establishment the order of digital contractual relationship by the controller. In general, the presented conclusions and proposals, in our opinion, will allow us to objectively interpret the understanding of digital processes and effectively apply the rules for the digital profile's security of civil legal relations' subjects.

References

[1] Forecasts for the development of the cybersecurity market // URL: https://iot.ru/bezopasnost/prognozy-po-razvitiyu-rynka-kiberbezopasnosti (accessed 14.12.2019).
[2] Part 1 of article 5; part 9 of article 10 of Federal law "On protection of competition" dated 26.07.2006, N 135-FZ.
[3] Ablameyko M. S. Legal regulation of personal data with the introduction of id - cards and biometric passports // Constitutional law and administrative law. 2018. No. 1, PP. 14–20.
[4] Federal law dated 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data".
[5] Articles 14–16 of Law N 152 – FZ.
[6] Federal law dated 27.07.2006 N 149-FZ "On information, information technologies and information protection".

[7] Draft Federal law N 747513-7.
[8] The Resolution of Plenum of the Supreme Court dated 23.06.2015 N 25 "About application by courts of certain provisions of section I of the RF Civil Code".
[9] Bank of Russia's Instruction dated 16.07.2019 N 5209-U.
[10] On the unified biometric system of PJSC "Rostelecom" / https://bio.rt.ru/about/ (accessed 20.12.2019).
[11] Resolution of the RF PF Board dated 18.06.2019, N 350 P.
[12] Forecasts for the development of the cybersecurity market: "device manipulation, data and identity theft, data falsification, IP theft and network manipulation for hackers" // URL: https://iot.ru/bezopasnost/prognozy-po-razvitiyu-rynka-kiberbezopasnosti (accessed 21.12.2019). Hackers faked the voice and extorted more than $200,000 from a British firm // URL: https://tech.informator.ua/2019/09/03/hakery-poddelali-golos-i-vymanili-bolee-200-000-u-britanskoj-firmy/ (accessed 14.12.2019).
[13] Rusakov, A. O., Chaly, R. A. Methods of protection from "Man in the middle" attack in Wi-Fi networks // Actual problems of aviation and cosmonautics. 2016. #12. PP. 767–769.
[14] Part 3 of article 13.11 of the RF Code of Administrative Offences.
[15] Starichkov, M. V. The concept of "Computer information" in Russian criminal law // Bulletin of the East Siberian Institute of the Ministry of internal affairs of Russia. 2014. № 1. PP. 16–20.
[16] Judicial Department of the Supreme Court of the Russian Federation. The data of judicial statistics. http://www.cdep.ru/index.php?id=79&item=2074 (accessed 14.12.2019).
[17] Judicial Department of the Supreme Court of the Russian Federation. The data of judicial statistics. http://www.cdep.ru/index.php?id=79&item=5081 (accessed 14.12.2019).
[18] Article 271 of the RF Criminal Code.
[19] Article 273 of the RF Criminal Code.
[20] Article 272 of the RF Criminal Code.

Anotācija

Darba mērķis ir juridiska riska novērtēšana, lai identificētu civilo attiecību subjektus, droši veiktu komercdarījumus, izmantojot digitālo profilu.

Rakstā mēģināts novērtēt civilo attiecību digitālo pārveidi un juridisko regulatoru ieviešanu subjektu digitālā profila aizsardzībai un drošībai. Tiek atspoguļoti "digitālā profila" definīcijas interpretācijas aspekti, kā arī atsevišķas juridiskā statusa zīmes pilsoņiem un uzņēmējdarbības subjektiem paziņošanas procedūrā, atšķirības starp tiesībām rīkoties un izmantot.

Tiek izteikti priekšlikumi pilnveidot tiesībaizsardzības praksi attiecībā uz civiltiesiskiem darījumiem digitālo resursu apgrozījuma laikā, kā arī administratīvo sodu piesaiste un uzlikšana. Vēl rakstā identificēti vairāki konflikti nelikumīgu darbību kavēšanai kompetenta digitālā personāla trūkuma dēļ, kā arī digitālie izmeklēšanas rīki.

Atslēgas vārdi: civiltiesisko attiecību priekšmets, digitālais profils, digitālā profila atsavināšana un izmantošana, valdījuma un lietošanas tiesības, paziņošanas procedūra, digitālā drošība.