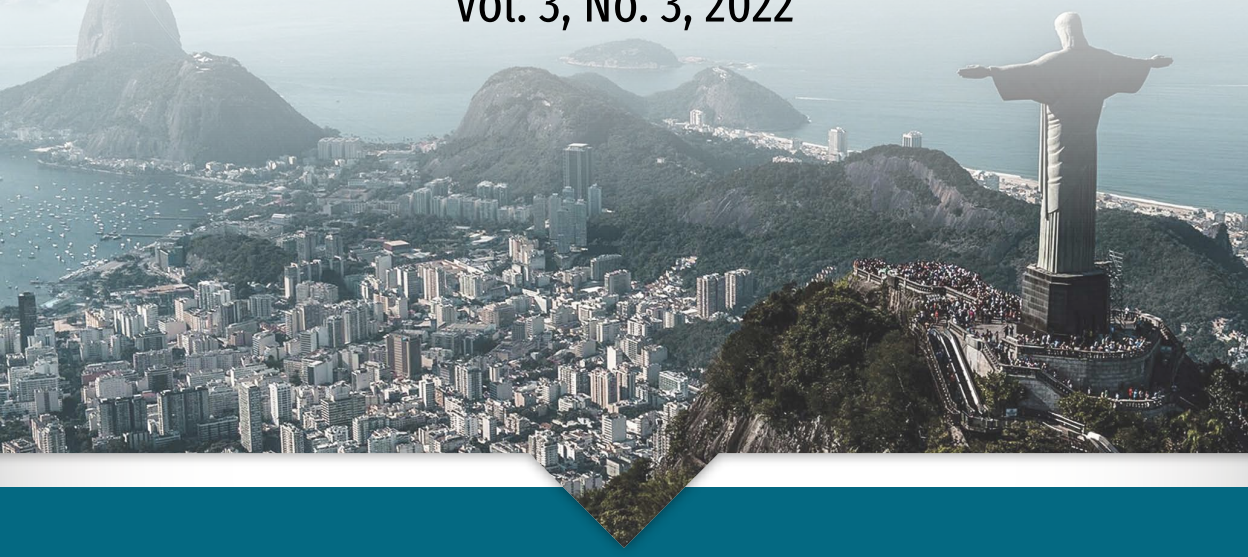
ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 3, No. 3, 2022



ARTICLES

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 3, No. 3, 2022

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 3, № 3, 2022

Contents

Articles

Содержание

Статьи

DIGITAL LAW JOURNAL

AIMS AND SCOPE

The purpose of the Digital Law Journal is to provide a theoretical understanding of the laws that arise in Law and Economics in the digital environment, as well as to create a platform for finding the most suitable version of their legal regulation. This aim is especially vital for the Russian legal community, following the development of the digital economy in our country. The rest of the world has faced the same challenge, more or less successfully; an extensive practice of digital economy regulation has been developed, which provides good material for conducting comparative research on this issue. Theoretically, "Digital Law" is based on "Internet Law", formed in English-language scientific literature, which a number of researchers consider as a separate branch of Law.

The journal establishes the following objectives:

- Publication of research in the field of digital law and digital economy in order to intensify international scientific interaction and cooperation within the scientific community of experts.
- Meeting the information needs of professional specialists, government officials, representatives of public associations, and other citizens and organizations; this concerns assessment (scientific and legal) of modern approaches to the legal regulation of the digital economy.
- Dissemination of the achievements of current legal and economic science, and the improvement of professional relationships and scientific cooperative interaction between researchers and research groups in both Russia and foreign countries.

The journal publishes manuscripts in the following fields of developments and challenges facing legal regulation of the digital economy:

1. Legal provision of information security and the formation of a unified digital environment of trust (identification of subjects in the digital space, legally significant information exchange, etc.).
2. Regulatory support for electronic civil turnover; comprehensive legal research of data in the context of digital technology development, including personal data, public data, and "Big Data".
3. Legal support for data collection, storage, and processing.
4. Regulatory support for the introduction and use of innovative technologies in the financial market (cryptocurrencies, blockchain, etc.).
5. Regulatory incentives for the improvement of the digital economy; legal regulation of contractual relations arising in connection with the development of digital technologies; network contracts (smart contracts); legal regulation of E-Commerce.
6. The formation of legal conditions in the field of legal proceedings and notaries according to the development of the digital economy.
7. Legal provision of digital interaction between the private sector and the state; a definition of the "digital objects" of taxation and legal regime development for the taxation of business activities in the field of digital technologies; a digital budget; a comprehensive study of the legal conditions for using the results of intellectual activity in the digital economy; and digital economy and antitrust regulation.
8. Legal regulation of the digital economy in the context of integration processes.
9. Comprehensive research of legal and ethical aspects related to the development and application of artificial intelligence and robotics systems.
10. Changing approaches to training and retraining of legal personnel in the context of digital technology development; new requirements for the skills of lawyers.

The subject of the journal corresponds to the group of specialties Legal Sciences 5.1.0. and Economic Sciences 5.2.0. according to the HAC nomenclature.

The journal publishes manuscripts in Russian and English.

FOUNDER, PUBLISHER:

Maxim I. Inozemtsev
76, ave. Vernadsky, Moscow, Russia, 119454

Founded:	The journal has been published since 2020
Frequency:	4 issues per year
DOI Prefix:	10.38044
ISSN online:	2686-9136
Mass Media Registration Certificate:	ЭЛ № ФС 77-76948 of 9 Oct. 2019 (Roskomnadzor)
Distribution:	Content is distributed under Creative Commons Attribution 4.0 License
Editorial Office:	76, ave. Vernadsky, Moscow, Russia, 119454, +7 (495) 229-41-78, digitallawjornal.org, dlj@digitallawjournal.org
Published online:	30 Sep. 2022
Copyright:	© Digital Law Journal, 2022
Price:	Free

REGION GROUP OF COMPANIES With support of REGION Group of Companies

ЦИФРОВОЕ ПРАВО

ЦЕЛИ И ЗАДАЧИ

Цель электронного журнала «Цифровое право» (Digital Law Journal) — создание дискуссионной площадки для осмысления в научно-практической плоскости легализации цифровых технологий, особенностей и перспектив их внедрения в нормативно-правовое поле. Особенно остро эта задача стоит перед российским сообществом правоведов в связи с развитием цифровой экономики в нашей стране. С этой же задачей сталкивается и остальной мир, решая её более или менее успешно. В мире сформировалась обширная практика нормативного регулирования цифровой экономики, она даёт хороший материал для проведения сравнительных исследований по этой проблематике. В теоретическом плане цифровое право опирается на сформировавшееся в англоязычной научной литературе академическое направление «интернет-право», которое ряд исследователей рассматривают как отдельную отрасль права.

Задачами журнала являются:

- Публикация исследований в области цифрового права и цифровой экономики с целью интенсификации международного научного взаимодействия и сотрудничества в рамках научного сообщества экспертов.
- Удовлетворение информационных потребностей специалистов-профессионалов, должностных лиц органов государственной власти, представителей общественных объединений, иных граждан и организаций в научно-правовой оценке современных подходов к правовому регулированию цифровой экономики.
- Распространение достижений актуальной юридической и экономической мысли, развитие профессиональных связей и научного кооперативного взаимодействия между исследователями и исследовательскими группами России и зарубежных государств.

В журнале публикуются рукописи по следующим направлениям развития и задачам, стоящим перед нормативным регулированием цифровой экономики.

1. Нормативное обеспечение информационной безопасности, формирование единой цифровой среды доверия (идентификация субъектов в цифровом пространстве, обмен юридически значимой информацией между ними и т. д.).
2. Нормативное обеспечение электронного гражданского оборота; комплексные правовые исследования оборота данных в условиях развития цифровых технологий, в том числе персональных данных, общедоступных данных, Big Data.
3. Нормативное обеспечение условий для сбора, хранения и обработки данных.
4. Нормативное обеспечение внедрения и использования инновационных технологий на финансовом рынке (криптовалюты, блокчейн и др.).
5. Нормативное стимулирование развития цифровой экономики; правовое регулирование договорных отношений, возникающих в связи с развитием цифровых технологий. Сетевые договоры (смарт-контракты). Правовое регулирование электронной торговли.
6. Формирование правовых условий в сфере судопроизводства и нотариата в связи с развитием цифровой экономики.
7. Обеспечение нормативного регулирования цифрового взаимодействия предпринимательского сообщества и государства; определение «цифровых объектов» налогов и разработка правового режима налогообложения предпринимательской деятельности в сфере цифровых технологий. Цифровой бюджет; комплексное исследование правовых условий использования результатов интеллектуальной деятельности в условиях цифровой экономики. Цифровая экономика и антимонопольное регулирование.
8. Нормативное регулирование цифровой экономикой в контексте интеграционных процессов.
9. Комплексные исследования правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники.
10. Изменение подходов к подготовке и переподготовке юридических кадров в условиях развития цифровых технологий. Новые требования к навыкам и квалификации юристов.

Тематика журнала соответствует группе специальностей «Юридические науки» 5.1.0 и «Экономические науки» 5.2.0 по номенклатуре ВАК.

В журнале публикуются рукописи на русском и английском языках.

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

Иноземцев Максим Игоревич
119454, Россия, Москва, просп. Вернадского, 76

История издания журнала:	Журнал издается с 2020 г.
Периодичность:	4 выпуска в год
Префикс DOI:	10.38044
ISSN online:	2686-9136
Свидетельство о регистрации средства массовой информации:	№ ФС 77-76948 от 09.10.2019 (Роскомнадзор)
Условия распространения материалов:	Контент доступен под лицензией Creative Commons Attribution 4.0 License
Редакция:	119454, Россия, Москва, просп. Вернадского, 76, +7 (495) 229-41-78, digitallawjournal.org, dlj@digitallawjournal.org
Дата публикации:	30.09.2022
Копирайт:	© Цифровое право, 2022
Цена:	Свободная

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2022-3-3-8-19

ARTICLES

CRYPTOGRAPHY AND LAW: THE CASE OF BRAZIL

Oscar V. Cardoso

School of Federal Judges of Rio Grande do Sul
55, Manoelito de Ornellas st., 1702, Bairro Praia de Belas, Porto Alegre, Brazil, 90010-230

Abstract

In a digitalised environment under conditions of reduced limits and boundaries between physical and virtual worlds, people's daily activities increasingly migrate to cyberspace. For this reason, legal issues relating to encryption, deciphering and codebreaking become increasingly topical. Due to the increased vulnerability of a wide range of people to exploitation, digitalisation implies an urgent need to develop measures for preserving privacy in digital life. Increasing vulnerabilities experienced in the social environment due to the Internet and network interactions can be attributed to the erasure of boundaries between people, which is facilitated by access to their data. In terms of providing general protection to online users, digital contracts, routine bank transfers and communications serve as an example. Cryptography, which allows the encoding of a message in an unintelligible format for those who do not have the appropriate key, represents one of the safest techniques for securely transmitting information online. In order to examine the relations between law and cryptology, the present work analyses Brazilian legal acts governing cryptography. Here, as well as defining cryptography, the main objective is to determine its main aspects and key features in order to examine the main legal issues and pecularities of legal regulation. It concludes that cryptography, as a mean to protect privacy on the Internet, does not exclude the necessity of law, but, on the contrary, legal regulation is essential to provide legal certainty to the cryptographic techniques.

Keywords

digital law, cryptography, cryptology, information security, digital signature, cryptocurrency

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Cardoso, O. V. (2022). Cryptography and law: The case of Brazil. *Digital Law Journal*, *3*(3), 8–19. https://doi.org/10.38044/2686-9136-2022-3-3-8-19

Submitted: 14 Apr. 2022, accepted 1 Aug. 2022, published 30 Sep. 2022

СТАТЬИ

КРИПТОГРАФИЯ И ПРАВО: ОПЫТ БРАЗИЛИИ

О.С. Кардозо

Федеральный университет Рио-Гранде-ду-Сул
90010-150, Бразилия, Порту-Алегри, р-н Фарроупилья,
просп. Паулу да Гама, 110

Аннотация

В условиях постепенного сокращения ограничений в цифровой среде и исчезновения границ между физическим и виртуальным мирами значение киберпространства для повседневной деятельности людей все более увеличивается. По этой причине необходимость изучения правовых аспектов обеспечения безопасности в сети, в частности шифрования, расшифровки и взлома источников информации, становится чрезвычайно актуальной. В связи с повышенной уязвимостью большинства людей в процессе осваивания новых технологий цифровизация влечет за собой потребность в разработке средств для сохранения конфиденциальности их частной жизни. Интернет и сетевое общение сделали социальную среду более уязвимой, стерев многие границы во взаимодействии между людьми и облегчив доступ к их данным. Ярким примером необходимости охраны прав участников гражданского оборота служат ежедневное заключение договоров в Интернете, осуществление рутинных банковских переводов и ведение коммуникации в цифровом поле. Одним из средств, гарантирующих безопасность передачи информации в сети, является криптография, позволяющая зашифровать сообщение для тех, у кого нет специального ключа. В статье анализируются правовые акты Бразилии, регламентирующие криптографию, для выяснения соотношения права и криптологии. Основная цель статьи — определить, что представляет собой криптография как явление, выявить ее основные черты и особенности, чтобы отметить основные проблемы и особенности правового регулирования. В результате автор приходит к выводу, что криптография как средство защиты информации в сети не исключает необходимость правового регулирования: напротив, правовая регламентация криптографических технологий необходима для обеспечения определенности в защите прав участников оборота.

Ключевые слова

цифровое право, криптография, криптология, информационная безопасность, цифровая подпись, криптовалюта

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Кардозо, О. В. (2022). Криптография и право: опыт Бразилии. *Цифровое право, 3*(3), 8–19. https://doi.org/10.38044/2686-9136-2022-3-3-8-19

Поступила: 14.04.2022, принята в печать: 01.08.2022, опубликована: 30.09.2022

Introduction

Cryptography is usually associated with methods for hiding and securely transmitting information. However, it can also be used to guarantee the veracity and authenticity of information by preventing its modification (or exposing any alterations). Therefore, the proper and safe application of cryptography depends on its regulation: the law delimits and limits the uses of cryptography, by defining what is — and what is not — lawful. For instance, digital payments in electronic commerce, the general functioning of the financial system (debit and credit cards, financial transactions in ATMs, applications, etc.) and even the sending of messages by e-mail could not be conducted in a reliable and safe way in the absence of regulation by law.

In addition to being a crucial tool in information security, encryption can also be used for purposes such as authenticating a digital signature or determining the validity of a contract.

In this connection, the currently insufficient regulation of cryptography applications causes legal certainty creates a need for legal bases for its standardisation, including in contracts.

The present work analyses conceptual and historical aspects of cryptology, cryptography and cryptanalysis in the Brazilian legal context, evaluating coherence and identifying gaps by examining practical acts and cases (digital signature, privacy protection on the Internet, data protection and cryptocurrencies).

Cryptology: Conceptual Aspects

In essence, cryptology is the study of methods for hiding, storing, communicating and revealing information. In etymological terms, the expression has Greek origins (*kryptós lógos*) and means "hidden word". The main objective of cryptology is to secure (and potentially ensure the secrecy of) communication between more than one person (i.e., a sender and receiver). While preserving the secrecy of information is relevant to cryptology, it is not inherent to it. Its primary value, therefore, is to use cryptological techniques to ensure the security of information transmitted in messages (Dizon & Upson, 2021).

When used to prevent information from being accessed by an unauthorised person or system, cryptology has three components: confidentiality, integrity and availability (CIA triad).

Cryptology can also be used to ensure:

a) ensuring that the receiver of the message is able to verify the integrity of a message, i.e., if it has modified in any way;
b) authentication of messages, i.e., allowing the receiver to know with certainty who is the sender;
c) non-repudiation, i.e., the sender of the message cannot deny its sending and authorship.

Thus, whether information is confidential or not, including with restricted or limited access or other classification, the need for its storage, transmission or other form of secure use or communication, results in the application of cryptological techniques, both in terms of concealing and providing access to information.

For such purposes, cryptology covers the fundamentals, definitions and techniques of concealing information (by the sender) and its adequate uncovering (by the receiver). While encoding forms one aspect of concealment, the scope of cryptology is not limited to encoding information and/or messages. Broadly speaking, cryptology covers any form of concealment (with or without encoding), the instruments or the logic used for this purpose.

The main species of cryptology are cryptography and cryptanalysis will be analyzed in the following. We will also consider steganography, which is considered as a kind of cryptography.

Cryptography: Conceptual Aspects

Cryptography comprises a method of encoding a message in an unintelligible format for anyone who does not have the proper key to decrypt it (Paar & Pelzl, 2010; Mollin, 2007). The word has Greek origins (*kryptós gráphein*) and means "hidden writing". Therefore, cryptography has been described as "the science of keeping secrets secret" (Delfs & Knebl, 2007). Thus, encryption is used as a cryptographic technique for hiding a message.

Encryption uses codes and ciphers to convert data into a format that is incomprehensible to anyone who does not have a key for decoding it, i.e., converting the encoded data back into its original format. Therefore, the main concepts in cryptography are code and cipher, which refer to different actions.[1]

A code comprises a rule that replaces part of the information with another object of the same type or another. For example, when encrypting a message, the code can change the order of the letters of the alphabet, or replace letters with numbers or symbols etc.

One of the best-known encryption codes is the Morse code, created in 1835 by Samuel Finley Breese Morse, which replaces alphanumeric characters (letters and numbers) and punctuation marks with graphic signs (dots, dashes, and spaces). Although not recognised as such by its many users, the American Standard Code for Information Interchange (ASCII) is perhaps the most universally used code. This code, which is used on all personal computers and other devices, replaces alphanumeric (letters and numbers) and special characters with seven-bit binary numbers (that is, those formed by the numbers 0 and 1).

A cipher, which comprises a key or algorithm used for the encryption and decryption of a message, has the same purpose of the code, i.e., to replace the information with another object of the same type or another. While a code and a cipher are both used to hide a message by replacing its information with another object, the main difference between a code and a cipher consists in the cipher using a key to achieve this purpose.

A plaintext is the original message prior to any changes. By encrypting a plaintext, a ciphertext is produced. Thus, an encryption algorithm performs the function of converting a plaintext into a ciphertext, while a decryption algorithm converts the ciphertext back into a plaintext.

Thus, the process of transforming a plaintext into ciphertext is called encryption or enciphering, the encrypted message is called a cryptogram, while the reverse process of transforming ciphertext into plaintext is called decryption or deciphering (Mollin, 2007). Therefore, the sender of an encrypted message uses an encryption algorithm, while its receiver uses a decryption algorithm.

Classifications

There are two main approaches for classifying cryptography:

a) based on the technique used to conceal the message;
b) based on the key used to encrypt the information.

The use of encryption methods is mainly based on two techniques:

i. transposition cipher, which reorders the characters of a message according to a predetermined logic. Some examples of transposition ciphers are rail fence techniques, in which the message is written in diagonal lines, and rectangular, when the message is written horizontally in a particular number of columns;

[1] Simmons, G. (n.d.) *Cryptology*. Encyclopedia Britannica. Retrieved January 11, 2022, from https://www.britannica.com/topic/cryptology

ii. substitution cipher, which changes the characters of a message. An example of a substitution cipher is the Caesar cipher (or exchange cipher), which modifies a letter of the alphabet by substituting it with another located in a certain fixed position.

While in a substitution cipher, the characters maintain their position in the sentence but change their identity (that is, the position and number of characters in each word do not change, but their representation changes), in a transposition cipher the characters change their position in the sentence but maintain their identity (the representation of the character does not change, but its position and amount in each word changes).

The second classification of cryptography divides it into symmetric (private or secret key) and asymmetric (public key) (Paar & Pelzl, 2010):

iii. symmetric cryptography (private or secret key) uses the same key to encrypt and decrypt the message; that is, the encryption and decryption of information occurs inside the message, which must be kept secret by the sender and receiver. This ensures a rapid response to encryption and encryption since the sender and receiver of the message use the same (private) key.

On the other hand, the sending of a private key to the receiver must occur in a secure manner to prevent unauthorised people from accessing it and the decrypted message. Therefore, sharing the private key is difficult to use this type of encryption. The main algorithms used for the private key are the block symmetric key (which divides the message into blocks of equal size in terms of bits) and flow (which affects the message bit by bit);

iv. asymmetric cryptography (public key) uses different keys (one public and one private) to encrypt and decrypt the message. Thus, either data encrypted with a public key can only be decrypted with the corresponding private key, or data encrypted with a private key can only be decrypted with the corresponding public key.

Encryption keys can also be used to ensure the integrity of information by ensuring that information signed by a private key is not modified and can be accessed by a public key. The main examples of this use of cryptography are digital signatures and time stamps.

Steganography: Conceptual Aspects

Steganography is a technique used to conceal a message in a non-secret object (hidden writing). Despite being a different type, it is usually considered as a form of cryptography, which can be divided into true secret writing (cryptography in a strict sense) and covert secret writing (steganography) (Mollin, 2007). The word also has Greek origins (*steganós gráphein* means "covered writing").

Steganography is especially used to hide text messages in different files (with image, video, audio, text etc.) in order to allow the circulation of confidential content, which can be accessed by anyone who knows how to access the message.

Digital files facilitate the use of steganography due to consisting of ordered sequences of bits (binary digits) stored in a file, as occurs, for example, in image pixels.

While cryptography and steganography are both used to ensure information confidentiality so that information is not accessed by unauthorised persons or systems, they do not ensure its integrity — that is, that the message will reach the receiver without any change in the information.

Cryptanalysis: Conceptual Aspects

The main objective of cryptanalysis, which is also an expression of Greek origin (*kryptós analýein* means "open word" or "enlightened word"), is to discover or recover information encrypted or

concealed despite lacking possession of the key or the form of concealment. Therefore, it is also known as the "*art of breaking*" cryptographic systems (Paar, 2010).[2]

To achieve its objective, cryptanalysis accomplishes in three stages:

a) identification: checks the existence of a hidden message and which code or system was used for this purpose;
b) cracking: testing of codes or other ways to identify the hidden content of the message;
c) configuration: stage of identifying the hidden content of the message.

Legal Regulation of Cryptography in Brazil

The use of cryptology and its distinct types (especially cryptography) depends on its legal regulation (Liguori, 2022).[3] The law itself can be the object of cryptography, in the so-called "cryptographic law" or "smart regulation", which proposes the use of a self-executable code as a new mean of legal regulation, which replaces a person's (that is, the legislator's) ability to predict the future with lines of code protected by cryptography (Deakin & Markou, 2020).

Considering the need for balance and updates in this relationship between law and technology, we proceed to an analysis of the main legal acts in Brazil (Salvador et al., 2019).

Digital Signature

The first legal Act in Brazil to regulate the application of encryption techniques is the *Medida Provisoria* (MP) no. 2.200-2/2001 (hereinafter — MP 2.200-2/2001), which established the Brazilian Public Key Infrastructure (ICP-Brasil) consisting of a hierarchical chain of trust validation to digital certificates for digital identification.[4] ICP-Brasil's main objective is to guarantee the authenticity, integrity and legal validity of electronic documents, support applications and applications enabled with digital certificates — and, consequently, secure electronic transactions (article 1 of the MP 2.200-2/2001).[5] Thus, Brazil has a public digital certification infrastructure, which is maintained and audited by the National Institute of Information Technology, a federal agency that plays the role of the Root Certification Authority.

Cryptography is also mentioned in article 6 of MP 2.200-2/2001[6]: each digital certificate can be issued by an accredited Certification Authority (CA), with the creation of a pair of cryptographic keys by the holder — that is, a public key and a private key.

A digital certificate, as regulated by MP 2.200-2/2001, uses asymmetric cryptography (or public keys) to ensure the integrity, authentication and non-repudiation of a digital signature. In this way, a person can use a private key to digitally sign a document, which can be accessed by anyone using the public key. With such a digital certificate it is possible to verify who actually digitally signed the document (authentication), preventing changes to it (integrity) and preventing the signer from denying authorship (non-repudiation). This does not necessarily involve the protection of

[2] Simmons, G. (n.d.) *Cryptology*. Encyclopedia Britannica. Retrieved January 11, 2022, from https://www.britannica.com/topic/cryptology

[3] On the advantages and disadvantages of legal regulation of cryptography, see chapters 5.2.1.1 and 5.2.1.2 of the book.

[4] Medida Provisoria No. 2.200-2, de 24 de agosto de 2001, Establishes the Brazilian Public Key Infrastructure (ICP-Brazil), Diário Oficial da União [D.O.U.] de 27.8.2001.

[5] Medida Provisoria No. 2.200-2, de 24 de agosto de 2001, Establishes the Brazilian Public Key Infrastructure (ICP-Brazil), Diário Oficial da União [D.O.U.] de 27.8.2001.

[6] Medida Provisoria No. 2.200-2, de 24 de agosto de 2001, Establishes the Brazilian Public Key Infrastructure (ICP-Brazil), Diário Oficial da União [D.O.U.] de 27.8.2001.

confidentiality, since a digital certificate can be used specifically for the purpose of publicizing the document and its public verification (as occurs, for example, in judicial decisions, in contracts and other acts).

In addition, a digital certificate can be used to verify the integrity and authenticity, or even the content of a digital or scanned document.

For example, sending a letter with receipt of confirmation can only contain the description of the object, but not its integral content (such as an extrajudicial notification). In turn, the digital sending (by email, message application or other way) of a document signed electronically (with cryptography) allows the verification of the content of the document, as well as its sender and overall integrity.

To permit these acts, it is necessary to regulate the legal form of electronically signing a document and the valid ways of sending or verifying that document, which is facilitated in Brazil by MP 2.200-2/2001.

In addition, the Electronic Signatures in Global and National Commerce Act[7], approved in 2000 in the United States, was the first Act in the world that regulate the certification digital and innovated by conferring to the digital signature the same legal validity of a written signature, i.e, one written on a physical substrate such as paper.

Privacy Protection Online

Although the Brazilian Internet Act (Act no. 12.965/2014) does not mention cryptography, it supports its use by assuring the rights and guarantees of Internet users, in article 7, I, II and III, including the inviolability of the privacy and the private life, the inviolability and secrecy of communication flow on the Internet (transmitted) and the inviolability and the secrecy of stored private communications (static).[8]

For example, SSL (Secure Sockets Layer) and TLS (Transport Layer Security) digital certificates on websites comprise security protocols that create an encrypted link between the server and the browser. This attests to the authenticity of a page and protects the confidentiality of the transmitted data and information. Although these certificates have long been used, for example, by banks and digital commerce, their use has been expanded to become a security guarantee for websites through their integration with the protocol for hypertext transfer. Thus, in addition to the standard HTTP (HyperText Transfer Protocol,), the HTTPS (HyperText Transfer Protocol Secure) protocol is integrated with SSL or TLS in order to use encryption in the communication between the user and the application on the Internet.

Article 13, IV, of the Brazilian Internet Act provides for encryption as one of the techniques used to guarantee the inviolability of data on the Internet, in record management solutions for safekeeping, storage and other data processing activities.[9]

In another example, the end-to-end encryption is used in message applications, with data encrypted only in the sender's device, or in the receiver's device. This method of encryption excludes the key from the service providers; that is, in order to prevent third parties from accessing data while being transferred from one device to another, it is provided only to the sender and receiver of the message. Therefore, no third party can access the message content (including the application

[7] Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001-7031 (2000).

[8] Act No. 12.965, de 23 de abril de 2014, Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil, Diário Oficial da União [D.O.U.] de 24.4.2014.

[9] Act No. 12.965, de 23 de abril de 2014, Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil, Diário Oficial da União [D.O.U.] de 24.4.2014.

developer him- or herself) because it is unintelligible to anyone who does not have the proper key for decrypting it.

In Brazil, the Supreme Court started to decide the ADPF 403 and the ADI 5527, in which the suspension and blocking of messaging services by court decisions are discussed, considering that messages are protected by encryption and not stored on the servers of the service, but only on users' devices.[10]

Protection of Personal Data

The Brazilian General Personal Data Protection Act (Act no. 13.709/2018 — LGPD)[11] does not contain any direct reference to encryption (Althabhawi et al, 2022). However, encryption can be applied based on several LGPD rules. Firstly, it is related to the concepts of anonymised data (article 5, III) and anonymisation (article 5, IX). While anonymised data does not contain or does not allow the identification of its subject, anonymisation is an activity of processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject. Thus, the LGPD does not make any provision for the anonymisation of data, but one of the techniques that can be used to anonymise personal data is encryption.

Data anonymisation is a method for protecting the controller due to removing the influence of LGPD on data processing, which can be carried out through encryption. In this case, the main purpose of encryption is not to provide privacy or greater security to the processing of data, but rather to make the LGPD inapplicable to the agent procesing operations.

In addition, by regulating security measures, practical rules and governance in Chapter VII (articles 46–51), the LGPD determines the use of cryptography as a security measure for protecting personal data from unauthorised access, including accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or illicit processing (article 46).

Cryptography is also legitimised by article 48, § 3º, of the LGPD, which regulates the communication of security incidents with personal data and stipulates incumbency on the part of the controller to demonstrate the adoption of "(...) appropriate technical measures that make the affected personal data unintelligible, within the scope of and within the technical limits of its services, to third parties not authorised to access them". Thus, even if there has been a security breach or unauthorised access to systems, files and other devices, the impossibility of third parties to access the encrypted data must be taken into account when evaluating the incident (and proving the absence of damage to the personal data subjects).

Cryptocurrencies

As a medium for conducting business transactions, the main functions of currency are:

a) value measurement: when used to assign a price to an object, such as products and services;

b) means of payment: a standardised form to be used in exchanges;

c) reserve method: use of currency as a reserve by its controller to manage the economy, thus explaining why not all banknotes and coins are in circulation but part of them is kept in reserve.

---

[10] S.T.F., Arguição de Descumprimento de Preceito Fundamental No. 403, Relator: Min. Edson Fachin, Ação Direta de Inconstitucionalidade No. 5527, Relator: Min. Rosa Weber.

[11] Act No. 13.709, de 14 de agosto de 2018, General Personal Data Protection Act (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018.

Currencies are classified in the ISO 4217, an international currency standard, by means of a three-letter capital code.[12] This code is used to standardise the identification of coins, some precious metals and certain financial units (such as special drawing rights) in international trade (such as bank transfers, the purchase of international plane tickets etc.).

A digital currency (electronic money, electronic currency or electronic cash) is the digital form taken by a particular currency. Therefore, in addition to banknotes and physical coins, a country can also have a virtual format of its currency.

Conversely, a cryptoasset is any cryptography-based asset, which relies on distributed data recording technology; that is, an asset with a digital form and use. It can be classified in terms of:

a) security tokens, which represent, in a digital environment, some physical securities. These are especially common in financial markets where they may be used for raising funds for a company, a new product or project, or to represent shares in an investment fund;

b) utility tokens, which comprise assets for accessing services or the provision of goods, which can be created by an organisation (such as, for example, fan tokens created by sports clubs for their members and fans, or tokens used in electronic games to purchase in-game products). Since these are not securities or financial assets, they can be created freely and do not depend on prior regulation by a Central Bank or a Securities and Exchange Commission;

c) cryptocurrency, which is a cryptoasset that performs the functions of a payment method, especially those of a currency unit, medium of exchange, store of value and unit of account (Uhdre, 2021).

In these cases, tokens perform contract functions, with the main objective of proving custody by whoever has its custody or is designated as their owner or possessor. Security tokens and utility tokens are also digital bearer securities because they represent rights (and their holders) and are considered safe, authentic and reliable due to the use of cryptography.

More specifically, cryptocurrency is a kind of digital currency and cryptoasset, which is not regulated or managed by a country or a Central Bank due to being based on a decentralised system.

While a cryptoasset comprises any encrypted economic asset based on distributed data recording technology, a cryptocurrency is one of its types, consisting of a cryptoasset with the additional function of a payment method. As a kind of cryptoasset, cryptocurrency has a digital form and use; that is, it is created, used and circulated exclusively in digital media.

Cryptocurrency is formed by the same suffix "crypto" (originating from the Greek word *kryptós*) also seen in the expression cryptography (secret writing). Therefore, it represents a "secret currency" or "hidden currency". However, it is not a currency created to circulate in secret or confidentially. On the contrary, cryptography is used to secure the existence of the currency and its circulation; i.e., to support business conducted with the use of cryptocurrency via the provision of integrity, authentication and non-repudiation. For this purpose, blockchain technology is generally used to provide security for the storage and circulation of cryptocurrencies.

In Brazil, the regulation of cryptocurrencies is still incipient and has no legislative basis, but only infra-legal norms. There is legal basis in Brazil only for the creation of a digital or electronic currency. Act no. 12.865/2013 regulates payment arrangements and payment institutions that are part of the Brazilian Payment System (SPB).[13] In this context, article 6, III, 'g', authorises payment institutions to

[12] Group Six. (n.d.) Data Standarts. Retrieved July 26, 2022. https://www.six-group.com/en/products-services/financial-information/data-standards.html

[13] Act No. 12.865, de 9 de outubro de 2013, Diário Oficial da União [D.O.U.] de 10.10.2013.

convert physical money into electronic money (and electronic money into physical money) in order to manage the use of electronic money.

In addition, article 6, VI, of Act no. 12.865/2013 contains a legal definition of electronic money: "resources stored in an electronic device or system that allow the end user to carry out a payment transaction".

Based on this Act, the Central Bank of Brazil issued the Notice no. 25.306/2014, on February 19, 2014[14], whose main objective was to highlight the risks involved in trading "virtual currencies" or "crypted currencies".

A new alert on the risks existing in the safekeeping and trading of virtual currencies was issued by the Central Bank of Brazil in Notice no. 31.379/2017.[15]

The Brazilian Securities and Exchange Commission (CVM) issued Circular Letter no. 1/2018[16] on the possibility of investing in cryptocurrencies by investment funds regulated by CVM Instruction no. 555/2014 (which regulates the creation and operation of investment funds in Brazil).

Based on the absence of legal regulation in Brazil and the lack of consensus on the possibility and form of standardisation, the CVM concluded that cryptocurrencies are not financial assets (according to the definition of item V of article 2 of the CVM Instruction no. 555/2014)[17]; thus, they cannot be acquired by funds.

However, in the same year, the CVM issued Circular Letter no. 11/2018[18], in which it is explained that CVM Instruction no. 555/2014 does not prevent investment funds in Brazil from investing indirectly in cryptocurrencies, through the acquisition of funds shares, derivatives and other assets abroad that invest in virtual currencies, as long as they are in a country that authorises this type of investment.

In addition, Normative Instruction no. 1.888/2019 of the Federal Revenue Service of Brazil (RFB) imposes the duty to provide information on carrying out operations with cryptoassets (that is, cryptocurrencies and other species).[19] By regulating the duty to declare cryptoassets on the part of individuals or individuals and legal entities, the RFB indirectly recognises the legality of operations carried out with these assets, based on the constitutional principle of legality provided for in article 5, II, according to which whatever is not expressly prohibited by law is permitted ("no one shall be obliged to do or refrain from doing anything except by virtue of the law").

The article 5, I, of Normative Instruction RFB no. 1.888/2019 defines cryptoassets as "the digital representation of value denominated in its own unit of account, whose price can be expressed in local or foreign sovereign currency, electronically transacted with the use of cryptography and of distributed ledger technologies, which can be used as a form of investment, instrument for the transfer of values or access to services, and which does not constitute legal tender".

---

14 Notice No. 25.306, de 19 de fevereiro de 2014, Diário Oficial da União [D.O.U.] de 20.02.2014

15 Notice No. 31.379, de 16 de novembro de 2017, Diário Oficial da União [D.O.U.] de 17.11.2017.

16 Circular Letter No. 1/2018/CVM/SIN, de 12 de janeiro de 2018, Retrieved January 11, 2022, from https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0118.html

17 Instruction No. 555/CVM, de 17 de dezembro de 2014, Retrieved January 11, 2022, from https://conteudo.cvm.gov.br/legislacao/instrucoes/inst555.html

18 Circular Letter No. 11/2018/CVM/SIN, de 19 de setembro de 2018, Retrieved January 11, 2022, from https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html

19 Normative Instruction No. 1.888, de 3 de maio de 2019, Diário Oficial da União [D.O.U.] de 07.5.2019.

Finally, Bill no. 4401/2021, currently pending in the Brazilian National Congress, is aimed at the regulation of virtual assets and the activities of virtual assets service providers; this is in addition to changing the Crimes Against the National Financial System Act and Money Laundering Act.[20]

This Bill, which is expected to be approved in 2022, considers virtual assets as digital representations of value that can be traded or transferred by electronic means and used for making payments or for investment purposes.

Conclusions

Cryptography is a type of cryptology, which consists of the study of techniques for concealing, storing, transmitting and revealing information. It is used to prevent information from being accessed by people without authorisation, which is associated with information confidentiality. However, cryptography is not limited to confidentiality, but also ensures compliance with the integrity (keeps information unchanged and indicates any changes made), authentication (the receiver knows who the sender is) and non-repudiation (the sender of the message cannot subsequently deny its authorship) of messages.

While cryptography is not yet regulated in Brazilian law, it is envisaged in legislation as one of the possible methods of ensuring information security, good practice and governance (among others), supporting confidentiality, integrity, authenticity and non-repudiation of data, information and related activities.

The security provided by the application of encryption in the protection of data and information, whether stored or transmitted, especially in the digital environment, prevents unwanted incidents and demonstrates compliance with legal norms.

Having various uses, cryptocurrency is a kind of digital currency and cryptoasset, which is not regulated or managed by a country or a Central Bank due to being based on a decentralised system. While the cryptoasset comprises any encrypted economic asset based on distributed data recording technology, cryptocurrency is one of its types, consisting of a cryptoasset with the functionality of a payment method. As a kind of cryptoasset, cryptocurrency has a digital form and use; that is, it is created, used and circulated exclusively in digital media.

The wide use of digital currencies around the world, and their potential for illicit purposes, requires state acts that regulate their use in a safe and lawful manner.

For these reasons, although there is no legal basis to authorise business transactions and the practice of other acts with cryptocurrencies in Brazil, these are authorised based on the constitutional principle of legality, according to which what is not expressly prohibited by law is allowed.

This legislative gap is expected to be addressed in Brazil with the approval of Bill No 4401/2021, which regulates virtual assets and the activities of virtual assets services providers[21].

[20] Bill No. 4401, de 8 de julho de 2015, Retrieved January 11, 2022, from https://www.camara.leg.br/propostas-legislativas/1555470

[21] Bill No. 4401, de 8 de julho de 2015, Retrieved January 11, 2022, from https://www.camara.leg.br/propostas-legislativas/1555470

References

1. Althabhawi, N. M., Zainol, Z. A., & Bagheri, P. (2022). Society 5.0: A new challenge to legal norms. *Sriwijaya Law Review*, *6*(1), 41–54.
2. Deakin, S., & Markou, C. (2020). From rule of law to legal singularity. In S. Deakin, & C. Markou (Eds.), *Is law computable: Critical perspectives on law and artificial intelligence* (pp. 1-29). Hart Publishing.
3. Delfs, H., & Knebl, H. (2007). *Introduction to cryptography: Principles and applications.* (2nd ed.). Springer.
4. Dizon, M. A. C. & Upson, P. J. (2021). Laws of encryption: An emerging legal framework. *Computer Law & Security Review*, *43*, Article 105635. https://doi.org/10.1016/j.clsr.2021.105635
5. Liguori, C. (2022). *Direito e criptografia*: *direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia* [Law and cryptography: Fundamental rights, information security and the limits of legal regulation in technology]. Saraiva Jur.
6. Mollin, R. A. (2007). *An introduction to cryptography*. (2nd ed.). Chapman & Hall/CRC.
7. Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer.
8. Salvador, J. P. F., Liguori, C. A. F., Santos, G. K., & Guimarães, T. B. Criptografia e Direito: Uma perspectiva comparada [Cryptography and law: A comparative perspective]. In D. Doneda, & D. Machado (Eds.), *A criptografia no direito brasileiro* [Cryptography in Brazilian law] (p. 107-121). Thomson Reuters, Revista dos Tribunals.
9. Uhdre, D.C. (2021). *Blockchain, tokens e criptomoedas* [Blockchain, tokens and cryptocurrencies]. Almedina.

Information about the author:

Oscar V. Cardoso — Ph.D. in Law, Judge of Federal Regional Court of the 4th Region, Professor, Federal University of Rio Grande do Sul, Porto Alegre, Brazil.
ovcardoso@hotmail.com

Сведения об авторе:

Кардозо О. В. — Ph.D. in Law, судья Федерального регионального суда четвертого округа Бразилии, профессор Федерального университета Рио-Гранде-ду-Сул, Порту-Алегри, Бразилия.
ovcardoso@hotmail.com

https://doi.org/10.38044/2686-9136-2022-3-3-20-42

СТАТЬИ

ПРЕДЕЛЫ ГРАЖДАНСКО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИ ВЛАДЕЛЬЦЕВ МАРКЕТПЛЕЙСОВ ПЕРЕД ПОТРЕБИТЕЛЯМИ В РФ И США

К.К. Краулин

Национальный исследовательский университет «Высшая школа экономики»
109028, Россия, Москва, Большой Трехсвятительский пер., 3

Аннотация

В работе анализируются пределы гражданско-правовой ответственности владельцев агрегаторов за действия продавцов (исполнителей), предложения которых размещены на агрегаторе, перед потребителями в РФ и США. Задачами исследования является выявление основных тенденций регулирования деятельности владельцев агрегаторов и подготовка предложений по внесению изменений в российское законодательство с учетом опыта зарубежных правопорядков. Актуальность исследования обусловлена общемировым трендом на расширение пределов ответственности цифровых платформ, что подтверждается как отдельными законодательными инициативами последних лет, так и доктринальными исследованиями и дискуссиями в СМИ. В статье последовательно рассматриваются специальные нормы российского законодательства о защите прав потребителей, регламентирующие правовой статус владельцев агрегаторов. Затем анализируются наиболее значимые судебные споры, рассмотренные судами РФ и США, отражающие основные тенденции в сфере разграничения пределов ответственности владельца агрегатора как посредника и непосредственно самого продавца (исполнителя). Помимо этого, автор выявляет и обосновывает основные проблемы применения норм об ответственности владельцев агрегаторов в РФ и США. В частности, применительно к РФ обращается внимание на противоположные судебные решения относительно наличия правового статуса владельца агрегатора у одного и того же юридического лица, а также излишне формальный подход судов, зачастую учитывающих только буквальное содержание соглашений владельца сервиса с пользователями. По результатам исследования сделан вывод о необходимости расширения пределов ответственности владельцев агрегаторов в РФ. По мнению автора, справедливым будет введение субсидиарной ответственности таких субъектов перед потребителями, условия применения которой предлагается определить законом.

Ключевые слова

владельцы агрегаторов, ответственность владельцев агрегаторов, защита прав потребителей, цифровое право, цифровые платформы

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имело спонсорской поддержки.

Для цитирования Краулин, К. К. (2022). Пределы гражданско-правовой ответственности владельцев маркетплейсов перед потребителями в РФ и США. *Цифровое право, 3*(3), 20–42. https://doi.org/10.38044/2686-9136-2022-3-3-20-42

Поступила: 14.04.2022, принята в печать: 30.06.2022, опубликована: 30.09.2022

ARTICLES

LIMITS OF PRODUCT LIABILITY OF THE MARKETPLACE OWNERS IN THE RUSSIAN FEDERATION AND THE USA

Konstantin K. Kraulin

Higher School of Economics (HSE University)
3, Bolshoy Trekhsvyatitelskiy Pereulok, Moscow, Russia, 109028

Abstract

The paper analyzes the limits of product liability of the marketplace for the actions of sellers (performers) in both countries. Research objectives are to identify the main trends in regulating the business of marketplace owners and prepare proposals for amendments to Russian legislation in view of the foreign experience. The relevance of the study is due to the global trend to expand the limits of liability of digital platforms, as evidenced by individual legislative initiatives in recent years, as well as doctrinal studies and discussions in the media. The paper consistently analyzes the special provisions of Russian legislation on consumer protection, which determine the legal status of the owners of marketplaces. Then it reviews the most significant legal disputes in Russia and the USA reflecting the main trends in the field of defining the limits of liability of the owner of the marketplace as an intermediary and directly the seller (performer). Besides, the author identifies and substantiates the main enforcement problems of the responsibility of owners of aggregators in Russia and in the USA. In particular, the author describes the controversial decisions of Russian courts regarding the legal status of the «owner of the aggregator» in the same legal entity. The courts' formalistic approach based on the literal content of the marketplace owner's agreements with users is also mentioned. Finally, it is concluded that it would be fair to consolidate the subsidiary liability of the «owners of aggregators» at the legislative level.

Keywords

marketplaces, liability of the marketplaces, consumer protection, digital law, digital platforms

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study had no sponsorship.

For citation Kraulin, K. K. (2022). Limits of product liability of the marketplace owners in the Russian Federation and the USA. *Digital Law Journal, 3*(3), 20–42. https://doi.org/10.38044/2686-9136-2022-3-3-20-42

Submitted: 14 Apr. 2022, accepted: 30 June 2022, published: 30 Sep. 2022

Введение

В научно-исследовательских работах по вопросам цифрового права принято начинать изложение с констатации бурного развития технологий и их влияния на общественные отношения во всех сферах жизнедеятельности. Не изменяя традиции, хочется процитировать одно из определений судов общей юрисдикции, которое на уровне судебного правоприменения подчеркивает актуальность выбранной темы[1]:

«Одной из новых возможностей, открывшихся в результате развития средств коммуникации в целом и сети Интернет в частности, стала электронная торговля (коммерция). В связи с широким развитием рынка электронной коммерции появился специфический субъект цифровых экономических отношений — посредники по размещению на собственных сайтах за плату предложений предпринимателей о продаже товаров (услуг). При этом посредники в экономических правоотношениях, связанных с электронной коммерцией, не являются владельцами электронных продуктов, размещаемых на их сайтах»

С экономической точки зрения функция таких посредников (они же — владельцы агрегаторов, цифровые посредники, операторы цифровых платформ и пр.[2]), как справедливо обратил внимание А.А. Иванов, заключается в том, что они «соединяют самостоятельных экономических агентов — производителей и потребителей — посредством специальной инфраструктуры, обычно связанной с использованием сети Интернет» (Ivanov, 2017). В судебной практике агрегаторы определяются в том числе как «информационные ресурсы (платформы), на которых потребитель имеет возможность получить информацию о товаре (услуге), оформить заказ и оплатить его»[3]. В пояснительной записке к законопроекту, по результатам рассмотрения которого владельцы агрегаторов стали субъектами Закона о защите прав потребителей, агрегатор определяется как «информационный посредник, вступающий с потребителями в возмездные отношения, но сам при этом не заключающий сделки по купле-продаже товаров (возмездному оказанию услуг)»[4].

Безусловно, участие посредника актуально не только в отношениях с участием потребителя. Цифровизация общественных отношений и рынок e-commerce как одно из ее проявлений одинаково затрагивает и B2B[5], и B2G[6] отношения. В то же время представляется, что в настоящий момент

[1] Апелляционное определение Саратовского областного суда от 09.11.2021 по делу № 33-7872/2021, 2-620/2021.

[2] Далее в настоящем исследовании указанные и сходные с ними термины используются в синонимичном значении.

[3] Решения Курганского городского суда Курганской области от 15.09.2021 по делу № 2а-9770/2021; от 10.06.2021 по делу № 2А-7186/2021; от 24.12.2020 по делу № 2а-11954/2020.

[4] Пояснительная записка к проекту федерального закона «О внесении изменений в Закон Российской Федерации “О защите прав потребителей”» (законопроект № 126869-7). https://sozd.duma.gov.ru/download/14A92C2B-2B52-44B6-9145-4CA51DB8BB66

[5] B2B (business-to-business) — торговые отношения между юридическими лицами; нацеленность бизнеса производить товары и услуги для другого бизнеса, а не для рядового покупателя.

[6] B2G (business-to-government) — отношения, где одной из сторон выступают государственные клиенты (органы государственной власти, госкомпании и пр.).

вопросы, связанные именно с защитой прав потребителей (B2C-отношения), являются наиболее острыми и актуальными с точки зрения запроса общества и государства на их упорядочивание и урегулирование с учетом вызовов всеобщей цифровизации[7].

Нарушения прав потребителей повсеместно встречаются и в повседневной жизни (Gubaeva, 2020), однако в цифровой среде и в первую очередь в сети Интернет риски соответствующих злоупотреблений видятся еще более высокими. Как справедливо отмечает С.Г. Долгов, «цифровизация не только улучшила возможность пользования всевозможными сервисами, но и выявила серьезные проблемы, связанные с защитой прав потребителей» (Dolgov, 2021).

В Докладе Совета при Президенте РФ по развитию гражданского общества и правам человека «Цифровая трансформация и защита прав граждан в цифровом пространстве» от 1 декабря 2021 г. обращается внимание, что в современном мире, и в РФ в частности, сформировалось новое, ранее не известное явление — «цифровая власть», которая по своей роли и значимости в общественных процессах может рассматриваться как полноценная «параллельная» ветвь власти. Одним из основных субъектов такой власти, по мнению авторов данного доклада, являются цифровые платформы, которые «приобретают огромную власть над рынком и его "свободными" экономическими агентами», негативными последствиями которой являются в том числе существенное снижение социальных гарантий для лиц, чьи услуги (работы) агрегируются платформой, а также ценовая дискриминация потребителей[8].

«Цифровая власть» платформ-агрегаторов обусловлена целым рядом особенностей «платформенной экономики»[9]. Так, Организация экономического сотрудничества и развития (OECD) еще в 2019 г. сформулировала следующие экономические особенности платформ[10]:

- масштабирование без затрат (пер. с англ. scale without mass), то есть возможность ведения бизнеса во всем мире без необходимости физического присутствия;
- неограниченный охват (пер. с англ. potentially global reach), обусловленный трансграничным характером Интернета;
- перекрестное субсидирование (пер. с англ. cross-subsidisation), то есть возможность установления более высоких цен для одних потребителей и более низких цен для других;
- возможность использования практически неограниченных массивов пользовательских данных, в том числе в коммерческих целях и др.

Перечисленные особенности создают благоприятную среду не только для развития «прорывных инноваций» ("disruptive innovations")[11], но и для злоупотреблений как самими владельцами агрегаторов, так и их бизнес-партнерами в лице продавцов (исполнителей). В отличие от сделок, совершаемых потребителями в розничной торговле, в e-commerce возможности для эффективной и оперативной защиты прав покупателя или получателя услуги осложнены наличием посредника в лице платформы. Рядовой потребитель зачастую вынужден

---

7 См. об этом, например: Банк России. (2021). Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов. http://www.cbr.ru/content/document/file/131935/onrfr_2021-12-24.pdf

8 См.: Совет при Президенте РФ по развитию гражданского общества и правам человека. (2021). Цифровая трансформация и защита прав граждан в цифровом пространстве. http://www.president-sovet.ru/docs/doclad_SPCh.docx

9 От англ. "platform economy". Она же "sharing economy", "gig economy", "peer economy" и пр. См.: Chan, D., Voortman, F., & Rogers, S. (2019). *The rise of the platform economy.* Delloite. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/humancapital/deloitte-nl-hc-the-rise-of-the-platform-economy-report.pdf

10 OECD. (2019). An introduction to online platforms and their role in the digital transformation. https://doi.org/10.1787/53e5f593-en

11 Disruptive innovations, см. OECD (2019).

предпринимать значительно больше действий для идентификации своего контрагента и предъявления ему требований, при этом оператор платформы, который в действительности является бенефициаром совершаемых на ней сделок (Lobel, 2016), все еще не имеет достаточных юридических и экономических стимулов для того, чтобы оказывать такому потребителю содействие в защите его прав или минимизировать риски таких нарушений.

В связи с изложенным целью настоящего исследования является определение таких пределов ответственности владельцев агрегаторов, которые бы наиболее отвечали интересам общества и государства, с одной стороны, гарантируя должный уровень защиты прав потребителей, и с другой — не ограничили бы рынок цифровых платформ и IT-индустрию в целом, развитие которого в последнее время стало чуть ли не ключевым направлением государственной политики РФ.

Также хотелось бы обратить внимание, что использованные вместо эпиграфа к настоящему исследованию выдержки из определения Саратовского областного суда следует рассматривать не только как яркий пример удачной инкорпорации доктринальных изысканий (Semyakin, 2020; Suvorov, 2019)[12] в решения по конкретным спорам, а в первую очередь как объективное наличие запроса профессионального сообщества на научные исследования в сфере цифрового права, которые могли бы стать шлюзом для большого корабля российской судебной системы в его затянувшемся плавании к единообразной правоприменительной практике, которая бы учитывала не только букву закона, но и социально-экономические факторы динамично развивающегося рынка.

Результаты

Закрепленная в Законе о защите прав потребителей модель ограниченной ответственности владельцев агрегаторов видится несправедливой и нарушающей баланс интересов не только потребителей и бизнеса, но и онлайн- и офлайн-ретейлеров. Существующий иммунитет владельцев агрегаторов от ответственности за действия продавцов и исполнителей, де-факто являющихся их бизнес-партнерами, не соответствует существу экономических отношений между указанными субъектами и не отвечает общественным интересам.

Видится очевидным, что пределы ответственности владельца агрегатора не должны ограничиваться одним лишь предоставлением потребителю всей необходимой информации. Владелец агрегатора в определенных случаях должен нести ответственность за своих бизнес-партнеров, оказывающих потребителям услуги или продающих им товары.

Правильность такого подхода подтверждается и опытом США, где он постепенно получает все большее распространение в судебной практике различных штатов. Однако следует отметить, что специальные нормативные правовые акты, которые бы прямо закрепляли расширение ответственности владельцев агрегаторов, в США пока существуют лишь в форме законопроектов.

Представляется, что с учетом предпосылок, описанных в настоящем исследовании, и «цифровой власти» владельцев агрегаторов, указанные субъекты должны нести как минимум субсидиарную ответственность перед потребителями. При этом такая ответственность должна основываться не на гражданско-правовой квалификации отношений между потребителем,

[12] Процитированное в начале настоящего исследования определение одного из судов является не результатом «судебного правотворчества», а представляет собой компиляцию судом фрагментов научных статей М.Н. Семякина и Е.Д. Суворова. Что, однако, является исключительно позитивным.

владельцем агрегатора и продавцом (исполнителем), а на соответствии критериям, которые будут установлены в законе и в случае соответствия которым на владельца (оператора) платформы будет распространяться специальный правовой статус владельца агрегатора по аналогии с тем, как предусматривает абз. 13 преамбулы Закона о защите прав потребителей.

В связи с этим видится целесообразным дополнить Закон о защите прав потребителей положениями об ответственности владельцев агрегаторов, помимо тех, которые уже предусмотрены ст. 12 Закона о защите прав потребителей, и условиях ее применения. Заслуживающим внимания также видятся предложения отдельных исследователей дифференцировать пределы ответственности владельцев агрегаторов в зависимости от особенностей агрегируемых им товаров или услуг (например, услуг такси) (Shaidullina, 2020; Markelova, 2021). Данный вопрос также может стать предметом отдельного исследования.

Вместе с тем само по себе закрепление в законе нового режима ответственности владельцев агрегаторов будет недостаточно эффективным до тех пор, пока в судебной практике не будут устранены имеющиеся противоречия, в том числе в части применения норм о владельцах агрегатора к тому или иному лицу.

Дискуссия

Ответственность владельцев агрегаторов по праву РФ

Понятие и правовой статус владельца агрегатора

В российском законодательстве отсутствует единое понятие субъекта, являющегося владельцем (оператором) цифровой платформы. В зависимости от сферы регулирования и нормативно-правового акта, которым оно обеспечивается, такие лица именуются:

- в законодательстве об интеллектуальной собственности — информационными посредниками[13];
- в законодательстве об информации — операторами информационной системы[14] (ввиду того, что любая платформа де-факто является информационной системой[15]);
- в антимонопольном законодательстве — хозяйствующими субъектами, владеющими цифровыми платформами[16];
- в законодательстве о деятельности финансовых или инвестиционных платформ — операторами финансовых или инвестиционных платформ[17];

[13] См.: ст. 1253.1 Гражданского кодекса Российской Федерации, Собрание законодательства Российской Федерации 2006, № 52, ст. 5496.

[14] П. 12 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Собрание законодательства Российской Федерации 2006, № 31, ст. 3448.

[15] П. 3 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Собрание законодательства Российской Федерации 2006, № 31, ст. 3448.

[16] См. т.н. «Пятый антимонопольный пакет»: пп. «б» п. 2 ст. 1 проекта Федерального закона «О внесении изменений в Федеральный закон "О защите конкуренции" и иные законодательные акты Российской Федерации»). https://regulation.gov.ru/projects/List/AdvancedSearch#npa=79428

[17] П. 2 ч. 1 ст. 2 Федерального закона от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы», Собрание законодательства Российской Федерации 2020, № 30, ст. 4737; п. 7 ч. 1 ст. 2 Федерального закона от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации», Собрание законодательства Российской Федерации 2019, № 31, ст. 4418.

- и, наконец, в законодательстве о защите прав потребителей — владельцами агрегаторов[18].

Примечательно, что не каждый оператор информационной системы, например, будет являться одновременно и информационным посредником, равно как не каждый информационный посредник будет являться владельцем агрегатора в понимании Закона о защите прав потребителей. Таким образом, вышеперечисленные термины хоть и охватывают одно явление, но несут в себе абсолютно различный правовой статус исходя из целей и области регулирования. Поскольку настоящее исследование ограничивается исключительно отношениями потребителя и платформы, далее правовой статус ее владельца (оператора) рассматривается именно через призму норм Закона о защите прав потребителей о владельцах агрегаторов.

В 2019 г. вступили в силу изменения в Закон о защите прав потребителей[19], установившие понятие владельца агрегатора и правовой статус таких субъектов, а также условия их ответственности[20].

Так, в соответствии с абз. 13 преамбулы Закона о защите прав потребителей под владельцами агрегатора понимаются организации и индивидуальные предприниматели, которые[21]:

- владеют программой для ЭВМ или сайтом и (или) страницей сайта в информационно-телекоммуникационной сети Интернет;
- предоставляют потребителю в отношении определенного товара (услуги) возможность одновременно ознакомиться с предложением продавца (исполнителя) о заключении договора купли-продажи товара (договора возмездного оказания услуг), заключить с продавцом (исполнителем) договор купли-продажи (договор возмездного оказания услуг);
- предоставляют потребителю возможность произвести предварительную оплату указанного товара (услуги) путем наличных расчетов либо перевода денежных средств владельцу агрегатора в рамках применяемых форм безналичных расчетов.

Отсутствие одного из указанных признаков означает, что организация не признается владельцем агрегатора для целей Закона о защите прав потребителей, а значит не подпадает под действие как Закона о защите прав потребителей в целом, так и отдельных его норм, посвященных владельцам агрегаторов.

Проблемы применения судами норм о владельцах агрегатора

Несмотря на вполне конкретные признаки владельца агрегатора, закрепленные в Законе о защите прав потребителей еще три года назад, одни и те же суды продолжают выносить диаметрально противоположные решения относительно наличия правового статуса владельца агрегатора у одного и того же юридического лица. Существующие противоречия в судебной практике можно наиболее наглядно отследить, проанализировав судебные дела в отношении владельцев сервисов заказа такси (агрегаторов такси).

Так, в феврале 2021 г. Девятый ААС пришел к выводу, что ООО «Сити-Мобил», которому принадлежит одноименный сервис заказа такси, является владельцем агрегатора[22].

---

[18] Абз. 13 преамбулы Закона Российской Федерации от 07.02.1992 №2300-I «О защите прав потребителей», Ведомости съезда народных депутатов РФ и Верховного совета РФ 1992, № 15, ст. 766

[19] Федеральный закон от 29.07.2018 № 250-ФЗ «О внесении изменений в Закон Российской Федерации «О защите прав потребителей», Собрание законодательства Российской Федерации 2018, № 31, ст. 4839.

[20] Ч. 2.1–2.3 ст. 12 Закона о защите прав потребителей.

[21] Абз. 13 преамбулы Закона о защите прав потребителей.

[22] Постановление Девятого арбитражного апелляционного суда от 05.02.2021 № 09АП-75687/2020 по делу № А40-184425/20.

В другом деле, рассмотренном в июле 2021 г. Девятый ААС в одном из дел пришел к выводу, что ООО «Сити-Мобил», которому принадлежит одноименный сервис заказа такси, не является владельцем агрегатора, так как, по мнению суда[23]:

1) Сервис не позволяет потребителям произвести предварительную оплату услуги по перевозке. При этом момент оплаты суд определил исходя из условий соглашения с пользователем, согласно которому оплата всегда производится только после завершения поездки.

2) Сервис не позволяет перевозчикам размещать предложения о заключении договора фрахтования, а потребителям ознакомиться с такими предложениями. Суд обосновал это тем, что потребитель получает информацию только об одном конкретном предложении перевозчика, который принял к исполнению заказ, а функционал сервиса не позволяет потребителям выбирать предложения различных перевозчиков.

Следует отметить, что указанные аргументы использовались представителями ООО «Сити-Мобил» и в рамках другого дела, также рассмотренного Девятым ААС[24], однако были отвергнуты судом. В свою очередь, в рамках этого дела эти аргументы, наоборот, легли в основу позиции суда[25].

Постановлением от 24.01.2022 № Ф05-24541/2021 по делу № А40-252913/2020 Арбитражный суд Московского округа все же отменил указанное постановление Девятого ААС и решил, что ООО «Сити-Мобил» все же является владельцем агрегатора, при этом никак не прокомментировав доводы суда апелляционной инстанции[26]. В мотивировочной части постановления суд округа ограничился цитированием условий получения доступа пользователей и перевозчиков к сервису и не дал им правовую оценку в контексте норм о владельце агрегатора, что, очевидно, не способствует формированию единообразной судебной практики.

В результате в еще одном деле, рассмотренном тем же Девятым ААС в феврале 2022 г., суд снова сделал вывод о том, что ООО «Сити-Мобил» не является владельцем агрегатора[27]. К таким же выводам Девятый ААС ранее пришел и в отношении ООО «ГетТакси Рус» (сервис заказа такси “Gett”) указав, что мобильное приложение не позволяет исполнителям размещать предложения потребителям о заключении договора, так как в приложении размещается лишь информация о заинтересованности потребителя в его заключении[28].

Примечательно, что в отношении владельца другого крупнейшего сервиса заказа такси «Яндекс.Такси» в практике арбитражных судов Московского округа[29], Второго

[23] Постановление Девятого арбитражного апелляционного суда от 02.07.2021 № 09АП-25963/2021 по делу № А40-252913/2020.

[24] Постановление Девятого арбитражного апелляционного суда от 05.02.2021 № 09АП-75687/2020 по делу №А40-184425/20.

[25] Постановление Девятого арбитражного апелляционного суда от 02.07.2021 № 09АП-25963/2021 по делу № А40-252913/2020.

[26] Постановление Арбитражного суда Московского округа от 24.01.2022 № Ф05-24541/2021 по делу № А40-252913/2020.

[27] Постановление Девятого арбитражного апелляционного суда от 21.02.2022 № 09АП-85974/2021 по делу № А40-82802/2021. На момент написания настоящего исследования дело было принято к производству Арбитражным судом Московского округа.

[28] Постановление Девятого арбитражного апелляционного суда от 09.12.2019 № 09АП-69367/2019 по делу № А40-134566/2019.

[29] Постановление Арбитражного суда Московского округа от 19.11.2019 № Ф05-19950/2019 по делу № А40-72718/2019 (оставлено в силе определением Верховного Суда Российской Федерации № 305-ЭС19-22311 от 12.12.2019; решение Арбитражного суда г. Москвы от 18.03.2022 по делу № А40-226783/21-84-1738; решение Арбитражного суда г. Москвы от 03.02.2022 по делу № А40-226774/21-130-1576.

КСОЮ[30], а также судов других округов[31] сформировалась однозначная позиция о том, что ООО «Яндекс.Такси» является владельцем агрегатора. Аналогичным образом у судов не возникает сомнений относительно статуса владельца агрегатора у владельцев сервиса заказа такси «Максим»[32].

При этом, так как при анализе функционала всех упомянутых сервисов заказа такси автором настоящего исследования различий не выявлено, можно сделать вывод, что суды:

- или испытывают сложности при оценке функционала агрегатора с точки зрения критериев, установленных абз. 13 преамбулы Закона о защите прав потребителей;
- или, что видится более опасным, несмотря на три года, прошедших со дня вступления в силу новелл о владельце агрегатора, до сих пор по-разному понимают и применяют указанные критерии.

В первом случае, как представляется, проблема кроется в излишне формальном подходе судов к оцениванию принципов функционирования того или иного агрегатора: суды зачастую ограничиваются изучением пользовательских соглашений и информации на сайте, не проверяя заявленную в них функциональность[33].

Так, например, несмотря на то что согласно лицензионному соглашению об использовании мобильного приложения «Ситимобил» и сервиса «Ситимобил» денежные средства не списываются с привязанной банковской карты пользователя до момента окончания оказания услуги по перевозке[34], в действительности денежные средства списываются с карты сразу после заказа еще до подачи машины[35]. Однако ни в одном из вышерассмотренных судебных дел о признании или непризнании ООО «Сити-Мобил» владельцем агрегатора указанное обстоятельство не учитывалось.

Следствием отсутствия единообразия в судебной практике является невозможность прогнозировать вероятность признания судом конкретного лица владельцем агрегатора и возникающее недоумение у участников рынка. Так, представители ООО «Яндекс.Такси» в рамках различных арбитражных дел неоднократно ссылались на то, что владелец сервиса заказа такси “Gett”, принципы работы которого идентичны принципам работы ООО «Яндекс.Такси», не был признан владельцем агрегатора, однако соответствующий довод поддержки в судах не находит[36]

---

30 Определение Второго кассационного суда общей юрисдикции от 06.04.2021 по делу № 88-6702/2021. См. также определение Второго кассационного суда общей юрисдикции от 27.01.2022 по делу № 88-1537/2022.

31 Постановление Арбитражного суда Северо-Кавказского округа от 21.01.2020 по делу № А53-15922/2019; постановление Тринадцатого арбитражного апелляционного суда от 26.02.2020 г. по делу № А56-111312/2019; определение Шестого кассационного суда общей юрисдикции от 01.02.2022 по делу № 88-1988/2022, 2-882/2021.

32 Постановление Арбитражного суда Центрального округа от 10.01.2022 № Ф10-6145/2021 по делу № А68-1603/2021; постановление Арбитражного суда Дальневосточного округа от 22.09.2021 № Ф03-4427/2021 по делу № А73-16600/2020; постановление Арбитражного суда Восточно-Сибирского округа от 14.05.2021 № Ф02-1922/2021 по делу № А10-5005/2020.

33 Решение Арбитражного суда г. Москвы от 18.03.2022 по делу № А40-226783/21-84-1738; решение Арбитражного суда г. Москвы от 03.02.2022 по делу № А40-226774/21-130-1576; решение Арбитражного суда г. Москвы от 29.12.2021 по делу № А40-226772/21-148-1268.

34 П. 6.1.4 лицензионного соглашения с пользователем. См.: Ситимобил. (2022, 17 августа). *Лицензионное соглашение с конечным пользователем мобильного приложения «Ситимобил»*. https://city-mobil.ru/oferta

35 Проверено эмпирическим путем. При этом даже в случае отмены заказа денежные средства иногда возвращаются на карту не сразу, а в течение нескольких дней.

36 Решение Арбитражного суда г. Москвы от 18.03.2022 по делу № А40-226783/21-84-1738; решение Арбитражного суда г. Москвы от 03.02.2022 по делу № А40-226774/21-130-1576.

(что в то же время, по мнению автора, является справедливым, так как в действительности ООО «ГетТакси Рус» следует рассматривать именно как владельца агрегатора).

Таким образом, несмотря на вполне конкретные признаки владельца агрегатора, сформулированные в Законе о защите прав потребителей, одни и те же суды могут выносить противоположные решения относительно наличия правового статуса владельца агрегатора у одного и того же юридического лица (или не применять соответствующие нормы в тех делах, где их применение является очевидным[37]).

В результате за пределами Закона о защите прав потребителей и его специальных норм об ответственности владельцев агрегаторов, остаются субъекты, являющиеся владельцами (операторами) платформ, но не соответствующие хотя бы одному из критериев, установленных абз. 13 преамбулы Закона о защите прав потребителей, причем зачастую лишь номинально.

Однако ключевым в области обеспечения баланса интересов потребителей и других участников цифрового рынка должно видится даже не столько единообразие судебной практики в части признания владельцев (операторов) платформ владельцами агрегаторов, сколько необходимость принципиального изменения подхода к определению пределов их ответственности перед потребителями.

Пределы ответственности владельцев агрегаторов перед потребителями по праву РФ

Ответственность владельцев агрегаторов, установленная Законом о защите прав потребителей. Действующее законодательство предусматривает довольно ограниченную ответственность субъектов, являющихся владельцами агрегаторов.

Владелец агрегатора может быть привлечен к гражданско-правовой ответственности за действия продавца (исполнителя) только в двух случаях, связанных исключительно с предоставлением потребителю недостоверной или неполной информации о товаре (услуге)[38]:

1) если владельцем агрегатора не были соблюдены требования о доведении до сведения потребителя информации о себе и продавце (исполнителе) в порядке п. 1.2 ст. 9 Закона о защите прав потребителей[39];

2) если владелец агрегатора изменяет предоставленную ему информацию о товаре (услуге), предоставленную продавцом (исполнителем) и содержащуюся в предложении о заключении договора с потребителем[40].

Первое основание обусловлено положениями п. 1.2 ст. 9 Закона о защите прав потребителей, который обязывает владельцев агрегаторов довести до сведения потребителей информацию о себе и продавце (исполнителе): наименование, место нахождения, режим работы и пр., а также об имеющихся изменениях в указанной информации. Соответствующая информация должна быть доведена до сведения потребителей путем ее размещения на сайте агрегатора или его странице, в том числе в виде ссылки на сайт продавца (исполнителя)[41]. Отсутствие такой информации будет являться нарушением[42].

---

[37] См., например, определение Третьего кассационного суда общей юрисдикции от 11.08.2021 по делу № 88-10378/2021, 2-2760/2020, в котором суд, рассматривая требования потребителя к ООО «Яндекс.Такси», не сослался на нормы Закона о защите прав потребителей о владельце агрегатора в принципе.

[38] П. 2.1 ст. 12 Закона о защите прав потребителей.

[39] Абз. 1 п. 2.1 ст. 12 Закона о защите прав потребителей.

[40] Абз. 3 п. 2.1 ст. 12 Закона о защите прав потребителей.

[41] Абз. 1 п. 2.1 ст. 12 Закона о защите прав потребителей.

[42] Решение Арбитражного суда Кемеровской области от 18.09.2019 по делу № А27-11661/2019.

Как указал Арбитражный суд Московского округа, законодательством не установлен конкретный способ, место, продолжительность, размер шрифта или иные условия доведения до потребителя информации о владельце агрегатора и продавце (исполнителе). Следовательно, владелец агрегатора вправе самостоятельно определить способ доведения соответствующей информации до потребителей, который позволит им беспрепятственно воспринять указанную информацию[43].

Судебной практикой были выработаны следующие критерии оценивания соответствия информационных ресурсов, принадлежащих владельцу агрегатора, указанным требованиям:

- информация должна доводиться до сведения потребителя в наглядной и доступной форме, а также учитывать технические особенности определенных носителей[44], при этом под доступностью понимается отсутствие необходимости совершения каких-либо специальных действий (например, перехода по ссылке)[45];
- у потребителя не должно возникать сомнения, что услуга будет оказана не агрегатором[46].

Так, суд определил как нарушение Закона о защите прав потребителей действия владельца агрегатора, который указал информацию об исполнителе на своем официальном сайте, но при этом не указал ее непосредственно в самом мобильном приложении, которое используют потребители[47].

В свою очередь, если информация об исполнителе доступна в мобильном приложении владельца агрегатора, как это, например, сделано в приложении «Яндекс.Такси», требования п. 1.2 ст. 9 Закона о защите прав потребителей будут признаны соблюденными[48]. Примечательно, что наличие соглашений с исполнителями, возлагающих обязанность по доведению необходимых сведений до потребителя на исполнителей, справедливо не признается судами соблюдением указанных требований[49].

В свою очередь, второе основание по своему правовому смыслу является наиболее близким с принципом “safe harbour” (в пер. с англ. — принцип «тихой гавани»), установленным в российском и американском законодательстве в отношении информационных посредников, который заключается в исключении ответственности посредника за материалы, нарушающие авторские права, если он не осуществляет их изменение[50]. Судебные споры по этому основанию сводятся к доказыванию действий владельца агрегатора по изменению информации о товаре (услуге), предоставленной продавцом (исполнителем). При недоказанности факта изменения владельцем агрегатора сведений, предоставленных ему продавцом и содержащихся в предложении о заключении договора купли-продажи, суды отказывают потребителям в иске[51].

---

43 Постановление Арбитражного суда Московского округа от 25.05.2020 № Ф05-6680/2020 по делу № А40-73679/19-153-440.

44 П. 44 постановления Пленума Верховного Суда РФ от 28.06.2012 № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей».

45 Определение Шестого кассационного суда общей юрисдикции от 01.12.2020 по делу № 88-22477/2020.

46 Там же.

47 Постановление Девятого арбитражного апелляционного суда от 20.05.2021 № 09АП-19630/2021 по делу № А40-234424/2020.

48 Постановление Арбитражного суда Московского округа от 19.11.2019 № Ф05-19950/2019 по делу № А40-72718/2019.

49 Постановление Арбитражного суда Восточно-Сибирского округа от 14.05.2021 № Ф02-1922/2021 по делу № А10-5005/2020.

50 См.: ст. 1253.1 ГК РФ; Закон об авторском праве в цифровую эпоху США (Digital Millennium Copyright Act, Pub. L. No. 105-304 (1998), https://www.govinfo.gov/app/details/PLAW-105publ304).

51 Апелляционное определение Тверского районного суда города Москвы от 22.09.2021 по делу № 2-135/2021, 11-139/2021.

Резюмируя, следует согласиться с выводом А.И. Бычкова, который отметил, что, согласно действующему законодательству РФ, «главная задача агрегатора заключается в корректном и своевременном раскрытии информации о себе, продавцах/исполнителях и предлагаемых ими товарах и услугах, а также ее обновлении в течение одного рабочего дня с момента ее получения или изменения», в связи с чем ответственность владельца агрегатора действующим регулированием ограничивается только теми убытками, «которые были причинены потребителю нарушением его права на получение полной и достоверной информации по вине агрегатора» (Bychkov, 2019; Markelova, 2021). Следует отметить, что именно это изначально и было целью авторов законопроекта, в пояснительной записке к которому обращается внимание прежде всего на «несоблюдение такими субъектами прав потребителей на информацию о продавце (изготовителе, исполнителе), реализуемых товарах и предлагаемых услугах»[52].

Из буквального толкования рассмотренных положений закона следует, что если владелец (оператор) цифровой платформы соответствует признакам владельца агрегатора, установленным Законом о защите прав потребителей, то он в любом случае не будет нести ответственность за действия продавцов (исполнителей).

Завершая рассмотрение ответственности владельцев агрегаторов согласно действующей редакции Закона о защите прав потребителей, необходимо отметить, что с вступлением в силу изменений, предусмотренных Федеральным законом от 01.05.2022 № 135-ФЗ «О внесении изменения в статью 16 Закона Российской Федерации «О защите прав потребителей», с 1 сентября 2022 г. вышеописанные основания их ответственности дополнятся еще одним: владельцы агрегаторов теперь будут отвечать перед потребителями и за убытки, причиненные им в результате включения в договор недопустимых условий. Новеллы упомянутого закона предусматривают закрытый перечень недопустимых условий договора, к которым отнесены в том числе условия, предоставляющие владельцу агрегатора право на односторонний отказ или одностороннее изменение условий обязательств перед пользователями, условия, содержащие основания досрочного расторжения договора по требованию владельца агрегатора, условия, ограничивающие или исключающие его ответственность и пр.[53]

Как разъясняет Роспотребнадзор, «предусмотренные законом изменения особо значимы в нынешних условиях, когда потребитель становится более уязвимым перед недобросовестными экономическими агентами и в связи с этим нуждается в дополнительной защите»[54]. В свою очередь, прямое указание в нормах Федерального закона от 01.05.2022 № 135-ФЗ на владельцев агрегаторов свидетельствует о внимании законодателя к деятельности указанных субъектов и их отношениям с потребителями и может рассматриваться как одно из проявлений тенденции расширения пределов ответственности владельцев агрегаторов, необходимость которого обосновывается в настоящем исследовании.

Ответственность владельцев агрегаторов, установленная п. 18 постановления Пленума Верховного Суда РФ от 26.06.2018 № 26. Примечательно, что еще до закрепления в Законе

---

[52] Пояснительная записка к проекту федерального закона «О внесении изменений в Закон Российской Федерации “О защите прав потребителей”» (законопроект № 126869-7). https://sozd.duma.gov.ru/download/14A92C2B-2B52-44B6-9145-4CA51DB8BB66

[53] См.: ст. 1 Федерального закона от 01.05.2022 № 135-ФЗ «О внесении изменения в статью 16 Закона Российской Федерации “О защите прав потребителей”, Собрание законодательства Российской Федерации 2022, № 18, ст. 3021.

[54] Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека. (2022, май). О внесении изменений в закон «О защите прав потребителей». https://www.rospotrebnadzor.ru/about/info/news/news_details.php?ELEMENT_ID=21422

о защите прав потребителей статуса владельцев агрегаторов, возможность привлечения таких субъектов к гражданско-правовой ответственности также обуславливалась исключительно степенью информирования потребителя.

Такая правовая позиция содержится в п. 18 постановления Пленума Верховного Суда РФ от 26.06.2018 № 26 «О некоторых вопросах применения законодательства о договоре перевозки автомобильным транспортом грузов, пассажиров и багажа и о договоре транспортной экспедиции», в котором сформулированы следующие условия ответственности цифрового посредника перед пассажиром за вред, причиненный в процессе перевозки:

- заключение договора перевозки от своего имени, либо
- если из обстоятельств заключения договора у добросовестного гражданина-потребителя могло сложиться мнение, что договор перевозки заключается непосредственно с этим лицом, а фактический перевозчик является его работником либо третьим лицом, привлеченным к исполнению обязательств по перевозке.

Как верно отмечает Е.Б. Подузова, выработанные Пленумом Верховного Суда РФ условия такой ответственности основываются на «добросовестности сторон и субъективном восприятии потребителя» (Poduzova, 2021), то есть фактически сводятся к обязанности надлежащим образом проинформировать потребителя, у кого он действительно приобретает товар (услугу). Аналогичным образом понимают указанные положения и другие ученые (Markelova, 2021; Kuznetsova, 2019), а также в большинстве своем и сами суды, которые отказывают потребителям в удовлетворении исковых требований в случае, если владелец агрегатора обеспечил потребителя всей необходимой информацией[55], или, наоборот, удовлетворяют их, если у потребителя могло сложиться представление, что его контрагентом является именно владелец агрегатора[56].

Таким образом, по своему правовому смыслу позиция Пленума Верховного Суда РФ не вступает в противоречие с нормами Закона о защите прав потребителей, начавшими действовать уже после принятия указанного постановления. Пределы ответственности владельцев агрегаторов, установленные Законом о защите прав потребителей, стали скорее следствием начавшей свое формирование судебной практики, нежели положили начало принципиально новому подходу.

В этой связи видится нелогичным, что в отдельных делах суды продолжают ссылаться исключительно на п. 18 постановления Пленума Верховного Суда РФ от 26.06.2018 № 26, не применяя при этом нормы Закона о защите прав потребителей о владельцах агрегаторов[57].

Несмотря на сходство правового смысла упомянутых положений постановления Пленума Верховного Суда и норм Закона о защите прав потребителей, суды зачастую применяют правовую позицию высшей инстанции как самостоятельное основание ответственности владельцев агрегаторов, существующее автономно от Закона о защите прав потребителей. Аналогичным образом указанные положения рассматриваются и в отдельных научных работах (Krasnova, 2022), однако такой подход видится не совсем верным по причине того, что при условии соблюдения

[55] См., например: определение Третьего кассационного суда общей юрисдикции от 11.08.2021 по делу № 88-10378/2021, 2-2760/2020.

[56] См. определение Седьмого кассационного суда общей юрисдикции от 09.01.2020 № 88-672/2020. См. также определение Шестого кассационного суда общей юрисдикции от 01.12.2020 по делу № 88-22477/2020.

[57] См., например: определение Третьего кассационного суда общей юрисдикции от 11.08.2021 по делу № 88-10378/2021, 2-2760/2020; определение Шестого кассационного суда общей юрисдикции от 06.04.2020 по делу № 88-7055/2020; определение Седьмого кассационного суда общей юрисдикции от 23.01.2020 № 88-972/2020 по делу № 2-2042/2019; определение Седьмого кассационного суда общей юрисдикции от 09.01.2020 № 88-672/2020.

владельцем агрегатора требований ч. 1.2–1.3 ст. 9 Закона о защите прав потребителей о надлежащем информировании потребителя у него в принципе не может «сложиться мнение, что договор заключается непосредственно с владельцем агрегатора»[58]. Ссылка на иное, очевидно, свидетельствовала бы о недобросовестности, а точнее — о неосмотрительно потребителя.

В результате в российской правовой системе формируется два параллельных «стрима» судебной практики: одни решения основываются на ч. 1.2–1.3 ст. 9 и ч. 2.1 ст. 12 Закона о защите прав потребителей, а другие — на положениях п. 18 постановления Пленума Верховного Суда РФ от 26.06.2018 № 26. Тогда как на самом деле правильнее было бы использовать указанные положения во взаимосвязи друг с другом.

Ввиду относительной новизны положений Закона о защите прав потребителей о владельцах агрегаторов, положения постановления Пленума Верховного Суда РФ от 26.06.2018 № 26 могли бы использоваться в качестве разъяснения того, в каких случаях информация о роли владельца агрегатора в отношениях между исполнителем и потребителем является доведенной до последнего надлежащим образом. Так, в одном из дел возложение ответственности на владельца агрегатора такси "Uber" обосновывается судом тем, что предоставленный потребителю автомобиль «имел окраску, схожую по стилю с интерфейсом соответствующего мобильного приложения»[59]. Соответствующие выводы наряду с положениями п. 18 постановления Пленума Верховного Суда РФ от 26.06.2018 № 26 могли быть использованы участниками рынка при толковании положения ч. 1.2–1.3 ст. 9 Закона о защите прав потребителей, однако в указанном деле, как и во многих других, суд на эти нормы не ссылался, что делает применимость таких выводов к нормам о владельце агрегатора для непрофессиональных участников гражданского оборота не такой очевидной.

В качестве примера использования упомянутых норм Закона о защите прав потребителей во взаимосвязи с разъяснениями Пленума Верховного Суда РФ можно привести определение Восьмого кассационного суда общей юрисдикции от 08.02.2022 № 88-3094/2022. Представляется, что именно в такой связке они и должны использоваться судами в мотивировочной части судебных актов.

Обращая внимание на проблемы судебной практики, также следует отметить, что проблема, которая существует как в отношении признания одного и того же лица владельцем агрегаторов (см. раздел 1.2 настоящего исследования), существует также и в отношении признания достаточным информирования потребителя согласно п. 18 упомянутого постановления Пленума. Так, Мосгорсуд в одном из дел в марте 2021 г. признал, что в результате совершения заказа в приложении «Яндекс.Такси» у потребителя не возникает договорных отношений перевозки с владельцем сервиса ввиду того, что потребитель должным образом проинформирован об этом в приложении[60], а в другом деле, рассмотренном летом того же года, наоборот, указал, что у потребителя сложилось мнение о том, что договор перевозки заключается им непосредственно с ООО «Яндекс.Такси», в связи с чем удовлетворил требования к ООО «Яндекс.Такси»[61]. Это еще раз подтверждает отсутствие единого подхода в определении владельцев агрегаторов и их обязанностей в судебной практике.

---

[58] П. 18 постановления Пленума Верховного Суда РФ от 26.06.2018 № 26 «О некоторых вопросах применения законодательства о договоре перевозки автомобильным транспортом грузов, пассажиров и багажа и о договоре транспортной экспедиции».

[59] Определение Четвертого кассационного суда общей юрисдикции от 22.07.2021 по делу № 88-12024/2021.

[60] Апелляционное определение Московского городского суда от 24.03.2021 по делу № 33-12133/2021.

[61] Апелляционное определение Московского городского суда от 12.08.2021 по делу № 33-32624/2021.

Подводя итог, необходимо отметить, что правовая позиция, выработанная Пленумом Верховного Суда РФ в пункте 18 постановлении от 26.06.2018 № 26, должна рассматриваться и применяться во взаимосвязи, а не параллельно или отдельно от норм Закона о защите прав потребителей о владельцах агрегаторов. В частности, со ссылкой на указанной пункт может определяться соблюдение или несоблюдение владельцем агрегатора требований о доведении до сведения потребителей информации о себе и продавце, а именно достаточность объема такой информации (следует ли из нее, что договор заключается с продавцом (исполнителем), а не с владельцем агрегатора) и корректность способа ее доведения до потребителя.

Выводы о пределах ответственности владельцах агрегаторов по праву РФ и необходимости ее расширения. По мнению Роспотребнадзора, заложенная в Законе о защите прав потребителей модель ответственности владельцев агрегаторов обеспечивает дополнительную защиту потребителей[62]. С этим трудно не согласиться, однако «дополнительная» защита далеко не всегда тождественна защите «достаточной».

Вопрос о пределах ответственности владельцев агрегаторов является одним из наиболее спорных в контексте проблемы защиты прав потребителей в цифровой среде, что подтверждается абсолютно противоположной правоприменительной практикой не только в РФ, но и в других странах (Ivanov, 2019; Pleshanova, 2019)[63].

В российской юридической доктрине преобладает мнение о необходимости расширения пределов ответственности владельцев агрегаторов (Krasnova, 2022; Adamenko et al.; Markekova, 2021; Poduzova, 2021; Suvorov, 2019).

Так, по мнению А.К. Губаевой, «новеллы Закона о защите прав потребителей, связанные с ответственностью владельцев агрегатора информации о товарах (услугах), не обеспечили должного уровня защиты прав потребителей» (Gubaeva, 2020). При этом отмечается, что «в старой редакции Закон лучше защищал потребителей, поскольку судам надо было учитывать экономическую цель потребительского договора, сущность отношений участников отношений» (Dolgov, 2021; Poduzova, 2021; Suvorov, 2019; Deryugina, 2018). Сторонники такого подхода видят целесообразным установление субсидиарной ответственности владельцев агрегаторов по сделкам, совершаемым на их платформе (Dolgov, 2021; Poduzova, 2021; Suvorov, 2019; Deryugina, 2018), более того, на определенных условиях с этим были согласны и сами представители крупнейших агрегаторов[64]. В свою очередь, в отдельных работах и вовсе встречаются предложения о солидарной ответственности владельцев агрегаторов и продавцов (исполнителей) (Semyakin, 2020), что, однако, видится чрезмерным.

В то же время некоторые исследователи высказывают опасения относительно тенденции по возложению на владельцев агрегаторов полной или частичной ответственности по опосредуемым ими сделкам является ошибочной и даже опасной (Kuznetsova, 2019). Представляется, что это может быть связано со стремлением не создавать дополнительных барьеров и обременений

[62] Гарант.ру (2021, 30 ноября). *Информация Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека от 26.11.2021 «О правах потребителей в дни распродаж и акции “черная пятница”»*. https://www.garant.ru/products/ipo/prime/doc/403014965/

[63] В указанных научных статьях данная проблема обозначена на примере различных подходов к определению правового статуса агрегатора такси “Uber”.

[64] Скрынникова, А. (2020, 30 сентября). *Агрегаторы такси предложили переложить на них часть расходов за ДТП*. РБК. https://www.rbc.ru/technology_and_media/30/09/2020/5f7336bf9a7947ef128d355d

для участников рынка. Однако в этом контексте нельзя не согласиться с А.А. Маркеловой, которая справедливо замечает, что «право должно отдавать приоритет жизни и здоровью потребителей перед имущественными интересами компаний» (Markelova, 2021).

По результатам изучения доктринальных подходов и правоприменительной практики хотелось бы отметить следующее. Закрепленная в Законе о защите прав потребителей конструкция ограниченности пределов (оснований) ответственности владельцев агрегаторов видится несправедливой и нарушающей баланс интересов не только потребителей и бизнеса, но и онлайн- и офлайн-ретейлеров. Согласно маркетинговым исследованиям, рост рынка e-commerce в 2021 г. составил более 90 % по количеству заказов (1,6 млрд) и более 45 % в денежном эквиваленте (3,9 трлн руб.)[65]. Несмотря на то что в сравнении с офлайн-торговлей рынок e-commerce в РФ пока не столь развит, очевидно, что в ближайшем будущем ситуация изменится. Учитывая значительно возросшую роль цифровых платформ в экономике в целом и на потребительском рынке в частности, существующий иммунитет их владельцев от ответственности за действия продавцов и исполнителей, де-факто являющихся их бизнес-партнерами, не соответствует существу экономических отношений между указанными субъектами и не отвечает общественным интересам.

Видится очевидным, что пределы ответственности владельца агрегатора не должны ограничиваться одним лишь предоставлением потребителю всей необходимой информации. Владелец агрегатора в определенных случаях должен отвечать за своих бизнес-партнеров, оказывающих потребителям услуги или продающим им товары.

Интересно, что в отдельных научных публикациях расширение пределов ответственности указанных субъектов предлагается обеспечить по модели деликтной ответственности.

Данный подход, обосновываемый А.А. Маркеловой, основывается на признании владельцев агрегаторов фактическими исполнителями и применении к ним ст. 1095 ГК РФ об ответственности за вред, причиненный жизни и здоровью потребителя, а также ст. 1068 ГК РФ об ответственности юридического лица за действия привлеченных им лиц — ввиду наличия фактического контроля владельца агрегатора за продавцами (исполнителями) (Markelova, 2021). Однако в отличие от западных правопорядков, где отождествление «платформенной занятости» с трудовыми отношениями уже получило широкое распространение в правоприменительной практике[66], в нашей стране соответствующие подходы пока еще только обсуждаются. Кроме того, существующая в РФ модель ответственности владельцев агрегаторов, рассмотренная в разделах 1.3.2–1.3.3 настоящего исследования, основывается именно на договорной, а не деликтной ответственности таких субъектов. В связи с этим расширение договорной ответственности владельцев агрегаторов, как представляется, потребует значительно меньших преобразований, нежели распространение на них норм о деликтной ответственности, что отнюдь не делает предложенную теорию менее новаторской и заслуживающей внимания.

В свою очередь, при определении новых пределов ответственности владельцев агрегаторов и формировании ее правовой основы видится целесообразным использовать опыт других стран, в том числе опыт США, который будет рассмотрен далее.

---

[65] Мельникова, Ю. (2022, 10 января). *E-commerce показала колоссальный рост.* ComNews. https://www.comnews.ru/content/218162/2022-01-10/2022-w02/e-commerce-pokazala-kolossalnyy-rost

[66] Синявская, О.В., Бирюкова, С.С., Аптекарь, А.П., Горват, Е.С., Грищенко, Н.Б., Гудкова, Т.Б., & Карева, Д.Е. (2021). Платформенная занятость: определение и регулирование. https://ncmu.hse.ru/data/2021/05/26/1438190156/Доклад_Платформенная_занятость_002.pdf

Ответственность владельцев агрегаторов по праву США

В отличие от РФ, где права и гарантии потребителей закреплены на уровне федерального законодательства, в США соответствующее регулирование осуществляется преимущественно на уровне штатов. Однако, несмотря на отсутствие единого источника права, который бы регулировал ответственность владельцев агрегаторов на всей территории США, в судебной практике различных штатов с 2020 г. стал формироваться подход, свидетельствующий о постепенном расширении пределов ответственности таких субъектов.

Первым таким прецедентом, получившим широкое обсуждение в профессиональном сообществе, стало дело Bolger v. Amazon.com[67]. В рамках данного дела потребитель потребовал от Amazon компенсации за серьезные ожоги, полученные в результате возгорания аккумулятора ноутбука, приобретенного у стороннего продавца на платформе.

В 2016 г. суд первой инстанции постановил, что Amazon не может нести ответственность за качество товаров, предлагаемых продавцами. Однако в 2020 г. Апелляционный суд Калифорнии отменил решение суда первой инстанции. Суд применил к Amazon нормы о «строгой ответственности» продавца, обосновав это тем, что компания «встала между продавцом и покупателем в цепочке распространения продукта и в действительности имела возможность влиять на продавцов товаров, размещаемых на ее платформе». Как указал суд, «какой бы термин ни использовался для описания роли компании Amazon, будь то розничный продавец, дистрибьютор или просто посредник, именно он сыграл решающую роль в доведении продукта до потребителя».

По мнению Апелляционного суда Калифорнии, применение к Amazon норм об ответственности продавца обеспечивает максимальную защиту потребителей и в то же время не является для компании излишне обременительным, поскольку владельцы платформ, как указал суд, «могут компенсировать издержки на такие компенсации со своих деловых партнеров». При этом судом также было учтено, что «бизнес-модель Amazon побуждала потребителей напрямую взаимодействовать с его веб-сайтом, а не с веб-сайтом сторонних продавцов, так как при выборе товара он перемещался в «корзину» веб-сайта Amazon, при этом возвраты и обмены товаров также контролировались Amazon». В свою очередь, доводы представителей Amazon о том, что компания является лишь информационным посредником, судом были отклонены.

Данное дело легло в основу последующих решений не только в Калифорнии, но и в других штатах. Так, тот же Апелляционный суд Калифорнии, сославшись на дело Bolger v. Amazon.com, в 2021 г. удовлетворил аналогичные требования потребителя к Amazon в рамках дела Loomis v. Amazon.com[68]. Суд отметил, что Amazon оказал продавцу услугу по размещению его товаров на сайте и их доставке до потребителя, а значит также сыграл важную роль в сделке по продаже товара, что является основанием для применения к Amazon доктрины «строгой ответственности». Примечательно, что, отвечая на доводы Amazon об отсутствии возможности влиять на процесс производства товара и самого продавца, суд обратил внимание, что Amazon ранее публично заявлял о существующей на платформе политике обеспечения безопасности распространяемой продукции, что свидетельствует о том, что такая возможность все же имеется. Таким образом, как резюмировал суд, «применение строгой

[67] Bolger v. Amazon.com, LLC, 53 Cal. App. 5th 481 (Cal. C.A., 2020). https://law.justia.com/cases/california/court-of-appeal/2020/d075738.html

[68] Loomis v. Amazon.com, LLC, 63 Cal.App.5th 466 (Cal. C.A., 2021) https://law.justia.com/cases/california/court-of-appeal/2021/b297995.html

ответственности в этом случае может побудить Amazon расширить свои требования по соблюдению безопасности на большее количество товаров и тем самым способствовать достижению цели безопасности товаров».

Выводы, сделанные судами в приведенных делах, основываются на применении к владельцам агрегаторов норм деликтной ответственности (норм «строгой ответственности»).

Один из основоположников теории строгой ответственности юридических лиц, G. C. Keating, указывает, что в основе ответственности юридического лица лежат два положения (Keating, 2001):

- любая деятельность должна учитывать характерные для нее издержки, которые могут возникнуть из несчастных случаев;
- ответственность юридического лица заключается в том, что такие издержки должны быть распределены между его участниками: затраты на выплату компенсаций за причиненный вред должны быть разделены между теми, кто получает прибыль от деятельности, в результате которой такой вред был причинен, и не должны быть бременем пострадавшей стороны.

По мнению ученого, расходы, связанные со случайным причинением вреда, характерного для той или иной деятельности, должны нести те, кто получает выгоду от этой деятельности, независимо от наличия их вины, что соответствует основным принципам деликтной ответственности как в США, так и в РФ.

Несмотря на то что указанная теория была выработана G. C. Keating более двух десятилетий назад применительно к ответственности предприятий за производственные травмы, она находит отражение и в современных научных работах, посвященных ответственности владельцев агрегаторов (Kreiczer-Levy, 2021). Так, K. Cunningham-Pameter утверждает, что возможность владельцев платформ контролировать исполнение и результаты договоров, заключаемых при их посредничестве (например, установление шкалы оплаты для своих партнеров Amazon), свидетельствует о наличии «абсолютной власти над условиями и методами труда» привлекаемых лиц, а значит — свидетельствует о деликтоспособности владельцев таких ресурсов (Cunningham-Pameter, 2016; Cunningham-Pameter, 2019).

Применение к владельцам агрегаторов норм об ответственности продавцов получило широкое распространение и в судебной практике других штатов. В деле State Farm Fire & Cas Co. v. Amazon.com Верховный суд Нью-Йорка пришел к выводу, что Amazon осуществлял достаточный контроль над термостатом, который предположительно вызвал пожар в доме, чтобы считаться «продавцом», поскольку согласно пользовательским документам у Amazon есть право отказать в регистрации продукта, обрабатывать возвраты клиентов и подготавливать продукты к отгрузке, получая при этом часть прибыли и отправляя продукт в фирменной упаковке Amazon[69]. К аналогичным выводам по спору между теми же сторонами ранее пришел суд штата Висконсин[70], а также суды других штатов[71].

---

[69] State Farm Fire & Casualty Co. v. Amazon.com Services Inc., N.Y. slip op. 20326 (Sup. Ct. Dec. 8, 2020) https://law.justia.com/cases/new-york/other-courts/2020/2020-ny-slip-op-20326.html

[70] State Farm Fire and Casualty Company v. Amazon.com, Inc., No. 3:2018cv00261 — Document 45 (W.D. Wis., 2019). https://law.justia.com/cases/federal/district-courts/wisconsin/wiwdc/3:2018cv00261/41608/45/

[71] См., например, Papataros v. Amazon.com, Inc., Civ. No. 17-9836 (KM) (MAH) (D.N.J., 2019) https://www.govinfo.gov/app/details/USCOURTS-njd-2_17-cv-09836/summary

Отдельного внимания заслуживают условия распространения на владельца агрегатора режима правовой ответственности продавца, сформулированные судом в 2019 г. в деле Oberdorf v. Amazon.com[72] (тест «Обердорфа»):

- является ли владелец агрегатора единственным участником цепочки распространения товара, доступным потребителю для возмещения ущерба?
- служит ли наложение строгой ответственности стимулом к обеспечению безопасности для владельца агрегатора?
- находится ли владелец агрегатора в лучшем положении, чем потребитель, для предотвращения распространения дефектного продукта (например, в данном деле Amazon был признан находящимся в таком положении, так как он осуществляет существенный контроль над сторонними поставщиками и имеет полную возможность удалять небезопасные продукты со своего сайта)?
- может ли владелец агрегатора перераспределить издержки на выплаты компенсаций потребителям на самих поставщиков (например, Amazon действительно включает положения о возмещении убытков в свои договоры с поставщиками и корректирует комиссионные сборы, взимаемые со сторонних поставщиков)?

Суд указал, что положительный ответ на все четыре вопроса свидетельствует о том, что владелец агрегатора может быть привлечен к ответственности по аналогии с нормами о продавце товара. При этом такое решение было обусловлено не тем, что Amazon является владельцем сайта, а именно его непосредственным участием в процессе продаж, в связи с чем нормы об иммунитете владельца платформы, предусмотренные разделом 230 CDA[73], в данном случае применены не были (Busch, 2019).

Обосновывая ответственность владельцев агрегаторов, ученые, как и суды в вышеописанных делах, отмечают, что в отличие от реальных продавцов товаров на онлайн-платформах, которые в подавляющем большинстве являются представителями малого бизнеса, такие компании, как Amazon, в действительности значительно больше влияют на совершаемые сделки и могут и должны контролировать продавцов на своих ресурсах (Janger & Twerski, 2020). При этом встречаются отдельные гипотезы, которые основываются на том, что владелец агрегаторов может рассматриваться не только по аналогии с продавцом, но также и как лицо, которое должно гарантировать качество и соответствие товара, приобретаемого потребителем на его платформе (Janger & Twerski, 2020).

Получающее все большую поддержку в американской судебной практике привлечение владельцев агрегаторов к гражданско-правовой ответственности видится справедливым, однако небезупречным с точки зрения ее правового основания. Это связано с тем, что так как привлечение владельца агрегатора к ответственности обеспечивается путем применения к нему норм о продавце, окончательная ответственность напрямую зависит от того, насколько широко конкретный суд понимает термин «продавец».

Так, Верховный суд Техаса, анализируя законодательство штата в рамках дела Amazon.com v. McMillan[74], постановил, что термин «продавец» не распространяется на Amazon в контексте товаров, продаваемых сторонними продавцами, даже несмотря на то что компания контролировала процесс транзакции и доставку продукта. Аналогичным образом интерпретируют местное

[72] Oberdorf v. Amazon.com, Inc., No. 18-1041 (3d Cir, 2019). https://law.justia.com/cases/federal/appellate-courts/ca3/18-1041/18-1041-2019-07-03.html

[73] Communications Decency Act, §230, 47 U.S.C. §§ 223–230 (1996).

[74] Amazon.com, Inc. v. McMillan, 625 S.W.3d 101 (Tex. 2021). https://law.justia.com/cases/texas/supreme-court/2021/20-0979.html

законодательство суды штатов Иллинойс в деле Great Northern Insurance Company v. Amazon.com[75] и Огайо — в деле Stiner v. Amazon.com[76].

Более того, как отмечают отдельные ученые, несмотря на появление таких прецедентов, как Oberdorf v. Amazon.com и Bolger v. Amazon.com, на 2022 г. было удовлетворено лишь около 20 % потребительских исков против Amazon (García-Micó, 2022).

В этой связи заслуживает внимания исследование S. Kreiczer-Levy "The Duties of Online Marketplaces", в котором предлагается вместо использования уже существующих правовых конструкций дополнить американское законодательство специальными нормами об обязанностях и ответственности операторов платформ в случаях, «когда они создают представление о том, что платформа обеспечивает безопасность сделок», то есть фактически создают у потребителя впечатление о контроле платформы за сделкой и качеством приобретаемого товара. При этом такая ответственность, по мнению автора, должна наступать только когда продавец «недоступен для возмещения ущерба», то есть должна быть субсидиарной (Kreiczer-Levy, 2021).

Изложенное демонстрирует очевидную потребность американского правоприменителя в закреплении оснований ответственности владельцев агрегаторов на уровне законодательства. Так, ответственность владельцев агрегаторов предусмотрена в проекте закона о защите прав потребителей штата Калифорния[77], который предусматривает, что владельцы агрегаторов должны нести ответственность за все убытки, причиненные некачественными продуктами, размещенными на их площадке, в том же объеме, что и сам продавец. Однако участники рынка выступили против его принятия, так как, по их мнению, такие изменения задушат их бизнес[78]. В другом законопроекте, также разработанном в Калифорнии, предлагается установить ответственность за качество товаров участников рынка электронной торговли, которые: (a) сообщают о предложениях о продаже и (b) упрощают оплату между сторонним продавцом и покупателем, даже если интернет-магазин самостоятельно не вступает во владение товаром[79].

Принимая во внимание вполне понятное недовольство бизнеса, нельзя не согласиться с председателем Комиссии по безопасности потребительских товаров США, который еще летом 2021 г. призывал общественность и государство принять решение о том, «как более эффективно регулировать деятельность платформ и как лучше всего защитить потребителей, которые полагаются на них»[80].

Как отмечают американские исследователи, «судебные решения не могут в полной мере учесть неадекватные средства правовой защиты, которые имеют потребители в случае причинения вреда продуктами, купленными на онлайн-рынках у сторонних продавцов, а устаревшие

[75] Great N. Ins. Co. v. Amazon.com, Inc. 19 C 684 (N.D. Ill. Aug. 20, 2019). https://law.justia.com/cases/federal/district-courts/illinois/ilndce/1:2019cv00684/360978/32/

[76] Stiner v. Amazon.com, Inc., 162 Ohio St. 3d 128, slip op. 2020-Ohio-4632, 164 N.E.3d 394 https://law.justia.com/cases/ohio/supreme-court-of-ohio/2020/2019-0488.html

[77] California Product liability: electronic retail marketplaces Bill. (Cal. Assemb. 3262, 2019-2020 Reg. Sess. (Cal. 2020). https://openstates.org/ca/bills/20192020/AB3262/)

[78] Khambatta, D., Paroha, K. & Waldren, H. (2021, September 22). *Product liability risks for online marketplaces — an international comparison of litigation profiles.* Kennedys. URL: https://kennedyslaw.com/thought-leadership/article/product-liability-risks-for-online-marketplaces-an-international-comparison-of-litigation-profiles/

[79] California Product liability: products purchased online Bill (Cal. Assemb. 1182, 2021–2022 Reg. Sess. (Cal. 2021). https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=202120220AB1182

[80] U.S. Consumer Product Safety Commission (2021, July 14). *CPSC Sues Amazon to Force Recall of Hazardous Products Sold on Amazon.com*. https://www.cpsc.gov/Newsroom/News-Releases/2021/CPSC-Sues-Amazon-to-Force-Recall-of-Hazardous-Products-Sold-on-Amazon-com

законы штатов об ответственности за качество продукции могут ограничивать возможность привлечения к ответственности онлайн-рынков» (Bikoff, 2021). Отмечается, что «государства не могут защитить потребителей с помощью законов об ответственности за качество продукции, которые были написаны много лет назад и не учитывают особенности рынка электронной коммерции» (Bikoff, 2021).

Опыт США показывает, что несмотря на глубокий анализ экономической сущности платформ и их посреднической роли, который проводится судами при рассмотрении потребительских исков, а также по смыслу правильную тенденцию привлекать владельцев агрегаторов к ответственности по аналогии с продавцами (исполнителями), без закрепления оснований и пределов такой ответственности на уровне законодательства именно в отношении владельцев агрегатов в полной мере обеспечить защиту прав потребителей и достичь единообразия в правоприменении будет невозможно.

В отличие от РФ, где ответственность владельцев агрегаторов в законодательстве и судебной практике квалифицируется как договорная, в США прослеживается формирование двух параллельных оснований ответственности таких субъектов:

- применение судами к владельцам агрегаторов доктрины строгой ответственности из деликтного права США;
- законодательные инициативы в отдельных штатах, предусматривающие закрепление условий ответственности владельцев агрегаторов за действия продавцов (исполнителей) в законах о защите прав потребителей.

И все же, пока в РФ иммунитет владельцев агрегаторов от требований потребителей, не связанных с их ненадлежащим информированием, остается незыблемым, в США уже начинает формироваться устойчивая тенденция расширения пределов ответственности владельцев агрегаторов. Представляется, что американский опыт, в том числе выводы, сделанные судами при рассмотрении некоторых дел, могут быть использованы при реформировании законодательства о защите прав потребителей и в нашей стране.

Заключение

Стремительное развитие рынка электронной коммерции и появление цифровых посредников в отношениях продавец-потребитель стало вызовом не только для российского законодателя и судебной системы, но и для органов государственной власти во всем мире, в частности в США.

Следствием этого является отсутствие единообразия в судебной практике как РФ, так и США: и российские, и американские суды, очевидно, испытывают сложности при оценке функционала агрегатора, его роли и возможности влиять на продавцов и исполнителей, а значит и нести ответственность за агрегируемые товары и услуги.

Указанное лишний раз подтверждает тезис о том, что российское законодательство в области электронной коммерции, как в принципе и американское, находится пока еще на начальной стадии формирования и развития, что в какой-то степени даже хорошо, так как у законодателя пока еще есть возможность урегулировать одну из ключевых сфер экономики так, чтобы такое регулирование соответствовало технологическим, социальным и политико-правовым вызовам всеобщей цифровизации.

References / Список литературы

1. Adamenko, A. P., Piskunova, N. I., & Tselovalnikova, I. U. (2021). Grazhdansko-pravovaya otvetstvennost vladeltsev agregatorov torgovyh ploschadok pri prodazhe tovarov potrebitelyam [Aggregator owners' civil liability when selling goods to consumers]. *Imuschestvennye otnosheniya v Rossiyskoy Federatsii,* (12), 58–62.
2. Busch, C. (2019). When product liability meets the platform economy: A European perspective on Oberdorf v. Amazon. *Journal of European Consumer and Market Law*, (8), 173–174.
3. Bychkov, A. I. (2019). Agregatory i marketpleisy [Aggregators and marketplaces]. *Ekonomiko-pravovoy bulleten*, (12).
4. Cunningham-Pameter, K. (2019). Gig-dependence: Finding the real independent contractors of platform work. *Northern Illinois University Law Review*, 39(3), 379–427.
5. Cunningham-Pameter, K. (2016). From Amazon to Uber: Defining employment in modern economy. *Boston University Law Review*, 96(5), 1673–1728.
6. Deryugina, T. V. (2018). Pravovaya priroda dogovora, oposreduyuschego vozniknovenie pravootnosheniy s uchastiem agregatora [The legal nature of an agreement mediating origination of legal relationships involving an aggregator]. *Grazhdanskoye pravo*, (6), 3–6.
7. Dolgov, S. G. (2021). Grazhdansko-pravovaya otvetstvennost agregatorov taksi [Civil liability of taxi aggregators]. *Grazhdanskoe pravo*, (1), 3–7.
8. García-Micó, T. (2022). Platform economy and product liability: Old rules for new markets. *IDP: Revista d'Internet*, *Dret i Política*, (34), 1–24.
9. Gubaeva, A. K. (2020). Deliktnoe pravo Rossii: sovremennye visovy i perspectivy razvitiya [Russian tort law: Contemporary challenges and prospects for development]. *Zakon*, (3), 38–48.
10. Ivanov, A. A. (2017). Business-agregatory i pravo [Aggregation business and law]. *Zakon*, (5), 145–156.
11. Ivanov, A. A. (2019). Hronika pikiruyuschego bombardirovschika [Chronicle of a dive bomber]. *Zakon*, (7), 82–91.
12. Janger, E. J., & Twerski, A. D. (2020). Warranty, product liability and transaction structure: The problem of Amazon. *Brooklyn Journal of Corporate, Financial & Commercial Law*, *15*(1), Article 3. https://brooklynworks.brooklaw.edu/bjcfcl/vol15/iss1/3
13. Janger, E. J., & Twerski, A. D. (2020). The heavy hand of Amazon: A seller not a neutral platform. *Brooklyn Journal of Corporate Financial & Commercial Law*, *14*(2), 259–273. https://brooklynworks.brooklaw.edu/bjcfcl/vol14/iss2/3
14. Keating, G.C. (2001). The theory of enterprise liability and common law strict liability. *Vanderbilt Law Review*, *54*(3), Article 20. https://scholarship.law.vanderbilt.edu/vlr/vol54/iss3/20
15. Krasnova, S.A. (2022). Grazhdansko-pravovoy status operatorov online-platform: neopredelennoe nastoyaschee i vozmozhnoe buduschee [Civil legal status of online platform operators: uncertain present and possible future]. *Imuschestvennye otnosheniya v Rossiyskoy Federatsii, 2*(245), 76–86.
16. Kreiczer-Levy, S. (2021). The duties of online marketplaces. *San Diego Law Review*, *58*(2), 269–308. http://id.loc.gov/authorities/names/n79122466.html
17. Kuznetsova, L.V. (2019). Voprosy grazhdansko-pravovoy otvetstvennosti agregatorov elektronnoy kommertsii [Issues of civil liability of e-commerce aggregators]. In M.A. Rozhkova (Ed.) *E-commerce i vzaimosvyazannye oblasti (pravovoe regulirovanie)* [E-commerce and related spheres (legal regulation)] (pp. 39–65). Statut.
18. Lobel, O. (2016). The Law of the Platform. *Minnesota Law Review,* (101), 87–166. https://www.minnesotalawreview.org/wp-content/uploads/2019/07/Lobel.pdf
19. Markelova, A.A. (2021). Civil liability of taxi-aggregation companies: Between contract and tort law. Digital Law Journal, *2*(4), 8–19. https://doi.org/10.38044/2686-9136-2021-2-4-8-19

20. Pleshanova, O.P. (2019). Mnogourovnevaya numeratsiya i botizatsiya vsey strany [Multi-level numeration and nation-wide robotization]. *Zakon*, (6), 112–123.
21. Poduzova, E.B. (2021). Subekty tsifrovykh pravootnosheniy: Tendentsii prava i biznesa [Participants of digital legal relations: Trends in law and business]. *Aktualnye problemy rossiyskogo prava*, *16*(2), 55–60. https://doi.org/10.17803/1994-1471.2021.123.2.055-060
22. Semyakin, M.N. (2020). Grazhdansko-pravovoy dogovor v sfere tsifrovoy ekonomiki [Civil contract in the field of digital economy]. *Rossiyskiy yuridicheskiy journal*, *1*(130), 107–116.
23. Shaidullina, V.K. (2020). Pravovoe regulirovanie funktsionirovaniya tovarnyh agregatorov v seti Internet [Legal regulation of functionality of the trade aggregators online]. *Law and Politics*, (8), 58–66. https://doi.org/10.7256/2454-0706.2020.8.33341
24. Suvorov, E.D. (2019). Nekotorye problemy elektronnoy torgovli: K voprosu ob otvetstvennosti vladeltsev agregatorov pered potrebitelyami [Some problems of e-commerce: On the question of aggregator owners' liability to customers]. *Vestnik ekonomicheskogo pravosudiya Rossiyskoy Federatsii*, (9), 57–67.

Сведения об авторе:

Краулин К. К. — магистрант программы «Цифровое право» факультета права Национального исследовательского университета «Высшая Школа Экономики», Москва, Россия.
kraulin.konstantin@yandex.ru

Information about the author:

Konstantin K. Kraulin — LL.M. Student (LL.M. Program on Digital Law), Faculty of Law, HSE University, Moscow, Russia.
kraulin.konstantin@yandex.ru

https://doi.org/10.38044/2686-9136-2022-3-3-43-57

ARTICLES

ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS: WHAT IS THE EU's APPROACH?

Anna Y. Marchenko*, Mark L. Entin

Moscow State Institute of International Relations (MGIMO-University)
76, ave. Vernadsky, Moscow, Russia, 119454

Abstract

Threats posed to human rights by the rapid development of artificial intelligence (AI) are considered, along with some potential legal mitigations. The active efforts of the EU in the field of AI regulation seem particularly relevant for research considering its approach centred on citizens' rights. Thus, the present study aims to describe the key features of the EU approach to regulating AI in the context of human rights protection, as well as identifying both its achievements and deficiencies, and proposing improvements to existing provisions. The presented analysis of the proposed AI Act pays special attention to provisions that set out to eliminate or mitigate the main risks and dangers of AI. The currently intensive development of AI regulation in the EU (the Presidency Compromise Text presented by the Council of the EU, amendments of the European Committee of the Regions, opinions of interested parties and human rights organisations, etc.) makes this study especially timely due to its highlighting of problematic aspects. The analysis shows that, on closer examination, the proposed law leaves many sensitive and controversial issues unsettled. In the context of AI applications, the proposed solution is considered as an emergency measure in order to rapidly integrate purportedly trustworthy AI into human society. As a result of the analysis, the authors propose potential improvements to the AI Act, including the possibility to update the lists of all types of AI, clarify the concept of transparency and eliminate the self-assessment procedure. It is also necessary to consider the potential reclassification of some AI systems currently defined as presenting limited risk as systems presenting considerable risk or prohibited systems.

Keywords

European Union, European Union law, artificial intelligence, legal regulation of AI, European approach, human rights

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Marchenko, A. Y., & Entin, M. L. (2022). Artificial intelligence and human rights: What is the EU's approach? *Digital Law Journal*, *3*(3), 43–57. https://doi.org/10.38044/2686-9136-2022-3-3-43-57

* Corresponding author

Submitted: 25 May 2022, accepted: 10 Aug. 2022, published: 30 Sep. 2022

СТАТЬИ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРАВА ЧЕЛОВЕКА: ЧТО ПРЕДЛАГАЕТ ЕВРОПЕЙСКИЙ СОЮЗ?

А.Ю. Марченко*, М.Л. Энтин

Московский государственный институт международных отношений (МГИМО-Университет) МИД России
119454, Россия, Москва, просп. Вернадского, 76

Аннотация

Интенсивное развитие технологий обозначает серьезные правовые и этические проблемы, попытки решения которых предприняты в законодательстве ЕС. Статья обращает внимание на сферу прав человека. Рассмотрены риски применения технологий искусственного интеллекта для прав человека, а также возможные варианты их преодоления. Деятельность Европейского союза здесь представляется наиболее интересной с учетом его приверженности подходу к разработке «этичного», «доверенного» ИИ, где во главе угла стоят ценности ЕС и защита прав собственных граждан. Предпосылкой для проведения настоящего исследования является передовой характер подхода ЕС к регулированию ИИ и документов, разработанных Союзом в данной области. На примере предложенного Еврокомиссией Проекта регламента по регулированию ИИ в статье анализируются положения, которые позволяют купировать или снижать данные риски, и предлагаются пути для их улучшения. Ряд предложенных правил при ближайшем рассмотрении оставляет многие чувствительные и спорные вопросы открытыми. В контексте применения технологий ИИ их решение представляется крайне необходимым, с тем чтобы интегрировать безопасный, надежный ИИ в человеческое общество. Особенно интересным данный анализ представляется за счет динамичности развития регулирования — опубликованы компромиссный текст Совета ЕС, поправки Комитета ЕС по регионам, мнения заинтересованных сторон, правозащитных организаций и другие документы, позволяющие подсветить проблемные аспекты. В статье раскрыты особенности подхода ЕС, выявлены основные достижения и пробелы, сформулированы перспективы развития регулирования ИИ.

Ключевые слова

Европейский союз, право Европейского союза, искусственный интеллект, правовое регулирование ИИ, европейский подход, права человека

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Марченко, А. Ю., Энтин, М. Л. (2022). Искусственный интеллект и права человека: что предлагает Европейский союз? *Цифровое право, 3*(3), 43–57. https://doi.org/10.38044/2686-9136-2022-3-3-43-57

* Автор, ответственный за переписку

Поступила: 25.05.2022, принята в печать: 10.08.2022, опубликована: 30.09.2022

Introduction

On April 21, 2021, the European Commission submitted a draft Regulation laying down harmonised rules on artificial intelligence (hereinafter, the AI Act).[1] A year later, this remains the only comprehensive document aimed at regulating almost all aspects of the creation and application of artificial intelligence technologies (hereinafter referred to as AI). The very existence of such a document represents a new stage in the regulation of AI. If adopted, it will be the first large-scale legislative act in the field of AI. Firstly, this will constitute an important example of the unification of rules at the regional level in the field of AI; secondly, due to its extraterritorial nature, it will have an impact on companies located outside the Union, third-country law, as well as the international law.

However, the adoption of this regulation is currently delayed; moreover, the original version submitted by the European Commission has already been supplemented and amended as part of the compromise text submitted by the Council of the EU under the Slovenian presidency on November 29, 2021.[2] The text of the Council of the EU introduces a number of important changes that relate to the subject matter and scope of the Act, the definition of AI systems and other definitions, prohibited uses of AI, rules for high-risk systems, as well as other key aspects that will be discussed later in the present article.

In the near future, the AI Act will undergo even more significant changes, which are to be proposed by the European Parliament (Bertuzzi & Killeen, 2022). Given the dynamic development of the AI industry, as well as disagreements over the most pressing issues, such as prohibited AI applications, certification based on self-assessment, it perhaps unsurprising that approval and adoption of the Act has been delayed. Moreover, it is also relevant to recall that, while the draft General Data Protection Regulation (GDPR) was first published in 2012, the final version was only adopted in 2016.[3] This suggests that the final adoption of the AI Act is likely to take several years.

In the context of the development and widespread use of AI technologies, it is of paramount importance that attention be paid to the sphere of human rights, which is affected directly by AI systems. In this connection, as well as considering the risks and effects of AI technologies on human rights, it is also necessary to identify possible approaches for mitigating them. Thus, in the context of its stated goals and values as one of the main defenders of the rights and freedoms of its own citizens, it is interesting to consider the EU's approach to the regulation of AI.

This is especially relevant given the dynamic regulation environment and changes in the field of AI, which allow us to highlight controversial aspects. So, for instance, concerns expressed by many Russian and foreign experts concerning the excessively restrictive nature of the EU AI Act, upon closer examination, it turns out that many sensitive aspects have remained unresolved. For example, the classification of emotion recognition systems as posing limited risk is controversial; moreover, the list of exceptions envisaged in the ban on the use of biometric identification systems is rather broad.

Among Russian researchers, the problem of regulating the creation and use of AI technologies under the EU law is characterised by a low degree of development. Most of the relevant research

---

1 Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (April 21, 2021).

2 Council of the European Union Presidency Compromise Text on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, (Nov. 29, 2021), https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf

3 Long, W., Blythe, F., Kumar, S., & Long, W. (2022, January 18). EU Council publishes changes to Artificial Intelligence Act Proposal. *Lexology*. https://www.lexology.com/library/detail.aspx?g=717f0c32-2043-4315-ba61-9f181ace3e50

is conducted by European authors. In this connection, the large-scale works of F. Bothmer, T. Bury, N. Petit, A. Renda, R. Rodriguez, A. Siapka, and N. Smuha rate a mention. Among studies devoted to the impact of AI on human rights, the works of B. Lepri, R. Rodriguez, A. Siapka, P. Hacker should also be noted.

The present article is based on an analysis of the latest documents of the European Union in the field of AI, as well as current changes proposed by stakeholders, analytical studies, articles and reviews on the legal regulation of the creation and application of AI technologies in the EU, and the impact of AI on human rights.

The aim of the study is to identify the features, achievements and drawbacks in the EU's approach to AI regulation in the context of human rights protection and proposes approaches for improving the existing provisions.

This aim structures the following tasks:

- consider the problems and risks of human rights violations in the context of the development and implementation of AI technologies;
- analyse the latest documents of the EU, including current amendments and opinions, in the context of their ability to effectively address the above problems;
- track improvements in the original version of the AI Act in accordance with the latest changes;
- formulate the main achievements and drawbacks of the EU's approach to AI regulation and the protection of citizens' rights;
- formulate prospects for the development of legal regulation of AI technologies in the EU.

Results

After examining the main risks of human rights violations in the light of the development and implementation of AI technologies, the present study identifies problematic aspects such as lack of transparency, bias, invasiveness, and discrimination of AI systems. This provides a focus for our analysis of the AI Act and proposed amendments concerning the most controversial aspects.

The AI Act contains provisions aimed at mitigating the risk of human rights violations associated with the development of AI technologies, as well as ensuring the safe and "ethical" implementation of AI.

The AI Act envisages the prohibition of certain AI systems whose use can significantly violate human rights. This includes biometric identification systems used in public places for law enforcement purposes, social scoring systems, and a number of other types. Given that the use of such systems can be invasive and increase discrimination, their proscription seems quite reasonable.

As well as identifying high-risk systems, the AI Act encompasses a substantial number of requirements aimed at regulating the creation and implementation of these systems. For example, it is required to apply a risk management system to control risks throughout the entire life cycle of such an AI system. For this purpose, the AI Act formulates requirements for system transparency and human control.

The AI Act also contains provisions for datasets that must be up-to-date, representative, complete, error-free, and have appropriate statistical characteristics. By reducing the number of biases in datasets, this stipulation is intended to reduce the potential bias of systems and the consequent number of discriminatory decisions.

The Act also stipulates the requirement for high-risk systems to pass conformity assessments; this is designed to ensure that only those systems that meet all the necessary requirements and are safe will be allowed to enter the EU market.

The creation of a specialised supranational body and national supervisory authorities provided for in the Act is intended to facilitate coordination in the field of AI and ensure the implementation of the AI provisions. The AI Act also contains provisions on significant fines imposed in case of violation of the requirements of the Act.

A review of the proposed changes to the AI Act referring to the compromise text of the Council of the EU, the amendments of the EU Committee of the Regions, the joint position of the EDPB and EDPS, reveals several improvements compared to the original version of the AI Act:

- The changes proposed by the Council of the EU regarding the definition of AI systems provide a basis for distinguishing AI technologies from other information technologies. The compromise text does not refer to software as the only form of AI systems.
- Although the risk-based approach, which includes four levels of risk, remains unchanged, there have been clarifications regarding general-purpose AI, to which the AI Act does not apply.
- The prohibited uses of AI have been clarified. The ban on social scoring has also been extended to individuals, while the ban on the use of biometric identification systems in public places now includes the use of systems by and on behalf of law enforcement agencies, which makes it possible to extend the prohibition to include those who cooperate with law enforcement agencies.
- Annex III, which contains eight high-risk AI application areas has been updated. The following sub-items have been added: environmental protection (AI designed to control emissions and pollution) as part of Clause 2, while the AI systems used for calculating insurance premiums, underwriting, and evaluating claims are described in Clause 5 (d). Systems intended for criminal analytics are excluded from the field of law enforcement application of AI (Clause 6 (g)).
- The European Committee of the Regions point out the need for systematic notification of individuals that they interact with the system, as well as the need for such notification in relation to high-risk systems (this is not provided for in the AI Act).
- The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) urge that close attention be paid to emotion recognition systems, which, in their opinion, should be prohibited except in strictly defined cases (in the AI Act such systems are listed among those with limited risk).
- The EDPB and EDPS call for adaptation of the conformity assessment procedure so that preliminary assessment is always conducted by third parties in relation to high-risk systems.
- Noting the obvious improvements in comparison with the original version of the AI Act, we should point out several sensitive aspects that also require close attention:
- The AI Act and proposed amendments do not provide mechanisms for updating prohibited AI applications (Article 5) or systems with limited risk (Article 52). For high-risk AI applications, the ability to update applications is limited to specified areas. Taken together, this implies inflexibility of regulation in terms of an inability to provide a timely response to emerging threats and ensure legislative relevance to the rapidly progressing development of AI. Thus, it becomes necessary to provide for updating mechanisms and appropriate criteria.
- Manipulating and distorting people's behaviour, as well as identifying and exploiting the vulnerabilities of certain categories of citizens, would seem to comprise harmful practices that already violate human rights and thus do not require additional criteria of physical or psychological harm, as indicated in Article 5.
- Among the areas of application of high-risk AI, it is necessary to make provision for the use of AI in the healthcare sector.

- Many questions are raised by the use of AI systems for assessing the risk of an individual committing a crime or repeating it, as well as for predicting a crime or repetition thereof based on profiling or assessment of personal qualities and other characteristics. Since the AI Act considers such systems to be high-risk, it is relevant to classify such systems — or at least certain practices of their application — as prohibited.
- Since the proposed rules for high-risk AI systems are abstract by nature, they require the development of practical instructions in order to ensure their implementation in each specific case.
- It is necessary to clarify the concepts of transparency for Article 13 (high-risk AI) and Article 52 (limited-risk systems) and to include mandatory notification of a person about interaction with the AI system in Article 13.
- The compliance assessment procedure should be adapted to avoid the possibility of self-assessment, at least initially.
- Close attention should be paid to systems with limited risk (listed in Section 52: emotion recognition systems, biometric categorisation systems, deepfakes). It is important to classify some of them as prohibited (e.g., emotion recognition systems) or as high-risk, in order that they come under the appropriate regulation.
- It is important to extend to systems with limited risk the rule regarding a person's right to refuse to interact with the system in favour of a human if this is necessary to protect his or her rights.

Discussion

How AI can violate human rights. General overview

While the benefits of using AI can be significant, opening up the widest prospects for the future humanity, some AI systems and applications nevertheless involve significant risks of violating the fundamental rights of citizens. In terms of human rights, the majority of the problems associated with the use of AI and the integration of technologies into human society boil down to the risks of violating these rights. In this context, we will focus specifically on the present problems and those that may occur in near future without referring to the long-term risks of using AI, which may represent a threat to the existence of human civilisation per se. However, effective rules that allow current risks to be contained can help to prepare the ground for countering long-term threats.

Today all national and international legal documents in the field of AI emphasize the need to protect human rights. For example, in the amendments to the AI Act, the European Committee of the Regions pointed to the protection of citizens' rights as one of the goals of regulation, thus emphasising its connection with the EU Charter of Fundamental Rights.[4]

Problematic aspects may concern both the AI itself and its essence, as well as the features of its application. R. Rodriguez highlights the following problematic aspects of AI: lack of algorithmic transparency; problems associated with bias, injustice and discrimination; difficulties in challenging the decisions of AI systems; adverse impacts on the labour market; problems related to confidentiality of information and data protection (Rodriguez, 2020). These aspects are often interrelated. For instance, a lack of transparency makes it impossible to challenge the relevant decisions of a system (Edwards & Veale, 2017), while bias in datasets can lead to unfair and discriminatory decisions (Hacker, 2018).

[4] Opinion of the European Committee of the Regions on the European approach to artificial intelligence and Artificial Intelligence Act (revised opinion), 2022 O.J. (C 97) 60.

Moreover, all of these problems lead to human rights violations in one way or another. Indeed, if we consider each of the problems inherent in the AI industry such as system bias and discrimination, non-transparency of algorithms, confidentiality, data protection, and responsibility for harm caused by AI systems, it all eventually boils down to the risks of human rights violations. Such risks, which are by no means abstract, are most pronounced in particularly sensitive areas such as justice, health, public safety, employment, where the use of AI algorithms can be detrimental to human rights implying a need for protection. For instance, due to a lack of necessary transparency in AI algorithms, situations can arise where people whose rights are affected by the actions or decisions of the system do not know the reason why they were denied a particular service or why a certain decision was made in relation to them (Desai & Kroll, 2017).

Transparency of AI systems in a narrow sense means the ability to understand and explain the system's decisions. AI systems are characterised by significant complexity; moreover, a deep neural network learns independently to generate "black box effects", meaning that it is impossible to identify and explain each stage of the process in a form that is understandable to humans.[5] As a result of such opacity, the actions and decisions of AI systems often become inexplicable and untraceable, leading to the inability to prove the unfairness of the decisions made by the system, which effectively translates into the inability of citizens to protect their own rights.

Problems of injustice, bias and discrimination also become acute. Although such phenomena can be grouped together (Rodriguez, 2020) due to their significant interrelatedness, bias do not always lead to injustice or discrimination (Ferrer et al., 2021) but can remain an unnoticed deviation from the norm, which does not affect the system's decision in any way.

Typically, algorithmic bias is due to bias in datasets, which originates from the moment of data gathering and can be explained both by incorrect work with datasets and historical biases (Hacker, 2018). In recognising such data bias, algorithms can then identify additional differences to reinforce it resulting in discriminatory decisions (Siapka, 2018). Thus, the bias of algorithms is determined by existing biases in society, as well as by the diverse composition of groups working with data.

To illustrate the above-mentioned problems, we provide an example of one of the most significant EU-wide scandals involving citizens' access to social benefits in the Netherlands.[6] In 2014, with support from the Ministry of Social Affairs and Employment of the Netherlands, some cities started using the Systeem Risico Indicatie (SyRI) system, which is designed to detect fraud in the social security sector. In the process of calculating risks to predict the likelihood of fraud on the part of benefit recipients, this system collects and analyses vast amounts of data. However, people coming from the lower-income brackets of society were disproportionately evaluated, resulting in discrimination. Moreover, potential recipients of benefits did not have the opportunity to learn how the system makes decisions. In 2020, a Dutch court ruled that using the current version of SyRI is illegal due to its violation of the right to privacy in the sense described in the European Convention on Human Rights. The Court pointed out that the system was not transparent, collected too much data, and that the purposes of data collection were not clear and specific enough.[7]

---

5 WIPO. Standing Committee on the Law of Patents. (2019). *Background document on patents and emerging technologies*. https://www.wipo.int/edocs/mdocs/scp/en/scp_30/scp_30_5.pdf

6 AlgorithmWatch, (2020, April 6). *How Dutch activists got an invasive fraud detection algorithm banned*. https://algorithmwatch.org/en/syri-netherlands-algorithm/

7 De Rechtspraak. (2020, February 13). *SyRI legislation in breach of European Convention on Human Rights*. https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-legislation-in-breach-of-European-Convention-on-Human-Rights.aspx

In the case of the Italian food delivery company Deliveroo,[8] a court found that the algorithm used to rank the company's couriers and determine the priority of employees when accessing convenient delivery time slots was discriminatory. In this case, the reasons why a courier did not report that he or she would not be able to go to work were not considered, meaning that a line between absenteeism and absence for valid reasons was not drawn.

Systems that track employees in the workplace are the source of various social issues due to allowing all movements and operations performed by a person, including their location, desktop screen, voice tone and other characteristics, to be recorded and analysed. In particular, various gadgets (for example, Fitbit) are used as part of so-called wellness programs for employees, transmitting data about their health to their employers (Stefano, 2018).

While the use of such vast datasets coupled with analysis tools can increase employee productivity, mitigate health and safety risks, and reduce the likelihood of accidents, such systems are programmed by humans and may not be devoid of human biases. Moreover, given the ability of AI to learn and organise itself, there is a risk that it can reprogram criteria on its own accord in order to achieve set aims, which will result in discrimination. Moreover, even if data is anonymised, the invasive collection process itself violates privacy by overstepping the boundaries of work-related processes.

In the field of labour relations, longer-term risks can also be traced. In future, the widespread use of AI systems is likely to lead to significant changes in the requirements for employees, the creation of new types of jobs, as well as inequalities in the "new" labour market.

The above-mentioned systems can effectively replace human workers currently responsible for personnel management and control. This applies not only to HR specialists, but also to employees in other fields. Over time, AI has the potential to drive humans out of many areas of activity. Thus, M. L. Entin points out that the introduction of AI in the long run does not increase human capabilities, but instead creates an alternative to them in the labour market, leaving humans with nothing to oppose (Entin & Entina, 2021).

Thus, the large-scale capabilities demonstrated by AI entail equally large-scale application risks. Numerous situations have already arisen in which human rights are violated due to the use of artificial intelligence; their number is certain to increase in the future. Therefore, attention must be paid to both current and future risks involved in the use of AI, especially in the field of human rights, as well as to develop an appropriate regulatory framework aimed at minimising such risks.

What does the EU have to offer?

Definition of AI systems. The starting point of any effective regulation is a well-defined conceptual framework. It is not an easy task to define complex, interdisciplinary, and comprehensive technologies such as artificial intelligence without narrowing or expanding the scope of regulation (Samoili et al., 2020). Moreover, the rapidly developing AI industry requires the definition to maintain its relevance even with the further development of technologies and their constant updating (Stahl et al., 2022).

Despite the rather well-developed initial wording, the definition proposed by the European Commission in the AI Act has prompted a considerable number of discussions and already undergone some changes. For instance, in the Council of the EU's compromise text, it is divided into three components. By contrast with the original text, this later version indicates the ability of such systems

[8] Allen, R., & Masters, D. (2021, January 18). *An Italian lesson for Deliveroo: Computer programmes do not always think of everything! AI-Law.* https://ai-lawhub.com/2021/01/18/an-italian-lesson-for-deliveroo-computer-programmes-do-not-always-think-of-everything/

to determine how to achieve a set of human-defined goals by training, drawing logical conclusions or modelling. According to the Council of the EU, this will permit AI technologies to be better distinguished from other information technologies. In addition to this part, the other two essentially repeat the previous version, indicating that the system receives input data (machine or "human") and generates results in the form of content, forecasts, recommendations, or decisions that affect the environment with which the system interacts. In addition, the removal from the definition of a reference to software as the only form of AI systems seems appropriate given that they may take some other form including hardware or something not yet used for such purposes.

In its amendments to the Act, the EU Committee of the Regions mentioned the impossibility of formulating a final definition of AI due to the dynamic development of the AI industry, recommending that the definition should change with the development of AI systems and applications. While committees of the European Parliament are also preparing possible amendments to the existing definition, the indications are that there will be no major changes.[9]

The EU's approach to AI regulation. The AI Act stipulates that the pan-European regulation of reliable AI will provide adequate protection for citizens and at the same time contribute to strengthening the competitiveness and production capacity of Europe in the field of AI.

Changes proposed by the Council of the EU regarding the scope of the AI Act include the exclusion of artificial intelligence systems developed for the sole purpose of conducting scientific research. Existing exclusions from the Act are AIs developed or used for national security purposes and the military.

Despite the various proposed amendments, the broad scope of the Act remains unchanged. Its provisions will also apply to companies located outside the European Union to the extent that results obtained from AI systems belonging to these companies are used in the EU. This provision remains quite controversial for many companies, who do not always know exactly where the results of their systems will be used.

The AI Act has consolidated the EU's commitment to a risk-based approach with four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk. In attempting to balance the need, on the one hand, to encourage further development of innovations, and on the other hand, to protect citizens, such a risk-based approach is aimed at reducing the likelihood or extent of harm through risk assessment and regulation corresponding to the level of risk. Such a risk orientation is intended to avoid overly restrictive regulation.

However, according to representatives of several public organisations for the protection of digital rights, this approach presupposes the preliminary assignment of AI systems to various risk categories without considering that, due to its dependency on the specific context of using AI, the level of risk often cannot be fully determined in advance.[10] Moreover, such an approach is conspicuously convenient in a technical environment where companies assess their own production risks and are unlikely to be motivated to provide adequate protection of human rights.[11]

Moreover, the erroneous classification of some AI systems as low risk (for example, emotion recognition systems are assigned to this level) may lead to a lack of necessary regulation and means for

[9] Bertuzzi, L., & Killeen, M. (2022, March 4). *RT ban, internet struggles, Big Tech takes sides.* Euractiv. https://www.euractiv.com/section/digital/news/digital-brief-rt-ban-internet-struggles-big-tech-takes-sides/

[10] Statewatch. (2021, November 30). *EU: Artificial Intelligence Act must put human rights first.* https://www.statewatch.org/news/2021/november/eu-artificial-intelligence-act-must-put-human-rights-first/

[11] Hidvegi, F., Leufer, D., & Massé, E. (2021, February 17). *The EU should regulate AI on the basis of rights, not risks.* AccessNow. https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

measuring such systems. In particular, in order to facilitate their access to the EU market, companies may deliberately underestimate the level of risk to avoiding complying with the rules.

Nevertheless, the EU is not likely to abandon the risk-based approach. This approach to AI systems was proposed in the White Paper on Artificial Intelligence[12] presented by the Commission in February 2020, in which only two levels of risk were proposed. At that time, the risk categories were studied more thoroughly, which eventually led to a four-tier system. It is now crucially important to clearly define the criteria for assigning systems to a certain level of risk, as well as to provide opportunities for updating for each category in order to ensure regulatory flexibility.

Prohibited uses of AI. Speaking in more detail about each level of risk, we note that within the framework of the compromise text of the Council of the EU, some changes were made to the list of prohibited AI applications (Article 5), along with updates to the areas of application of high-risk AI (Annex III). In addition, the Council of the EU has formulated a separate Article (Article 52a) for general-purpose AI capable of performing generally applicable functions such as image/speech recognition, audio/video generation, image detection, question answering, translation, and others, taking such AI to be beyond the scope of the Act.

Article 5 of the AI Act still lists prohibited uses of AI technologies (systems that distort people's behaviour and thereby harm a person or others; systems that exploit the vulnerabilities of certain groups of people; social scoring systems, remote biometric identification systems applied by law enforcement officers). Additional clarifications have been added to the first two Articles. For example, Article 1 (a) prohibits the use of systems that affect the subconscious mind and thereby distort or change people's behaviour with the aim of significantly changing a person's behaviour in a way that causes or is likely to cause physical or psychological harm to that person or another person.[13] Such formulations seem to imply that a person's behaviour can be significantly distorted without causing harm. Nevertheless, the very fact of distortion, which can take away a person's independence when it comes to decision-making, can already be considered unacceptable.

Noting that private companies such as cloud service providers are now also capable of processing vast amounts of personal data, the EDPB and EDPS insisted in their joint position issued in June 2021 on the complete ban on the use of social assessment and classification systems for individuals.[14] Such a blanket prohibition of social scoring applications demonstrates awareness of the danger such systems pose and can be interpreted as a good sign.

Significantly, the word "remote" was removed from the ban on the use of biometric identification systems in public places used for law enforcement purposes; instead, the relevant wording now indicates a "real-time". According to the definition, the collection of biometric data, comparison and identification of data in such systems have no significant delay. Moreover, this prohibition now applies to the use of these systems by or on behalf of law enforcement agencies, which makes it possible to extend it to those who cooperate with law enforcement agencies.

Exceptions to this ban remained virtually unchanged: the search for victims of crimes; the prevention of a specific threat to critical infrastructure, life, health, physical safety of individuals or a

[12] *Commission White Paper on Artificial Intelligence: A European approach to excellence and trust,* COM (2020) 65 final (February 19, 2020).

[13] Council of the European Union Presidency Compromise Text on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, (Nov. 29, 2021), https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf

[14] Joint Opinion of the European Data Protection Supervisor and of the European Data Protection Board on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (June 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

terrorist attack; the detection and prosecution of criminals or suspects of criminal offenses that involve a sentence of imprisonment for more than three years. Such exceptions can still be interpreted quite broadly to justify the widespread use of AI by the authorities and law enforcement agencies. The use of such systems involves processing data from a disproportionate number of subjects to identify only a few individuals, which will inevitably result in excessive invasiveness of these practices and violations of the rights of others.

The failure of the Act to address the possibility of updating the list of prohibited AI applications demonstrates the general slowness of the regulation process, reducing its ability to ensure its own relevance with the progressive development and complexity of AI-technologies. Thus, it seems appropriate to provide special mechanisms for updating prohibited AI applications (for instance, in a manner similar to the update mechanism in Annex III) so that the lists can be updated as technology evolves.

High-risk AI systems. Two groups of such systems are identified in the original version of the Act. The first category includes systems that meet two conditions: they are products or are intended to be used as components of product safety that are subject to the applicable Union legislation of Annex II (Directive 2006/42/EC on the safety of machinery and equipment, etc.), and must pass a third-party conformity assessment in order to be placed on the market or put into operation. In the compromise text, the Council of the EU only slightly changed the wording and structure of these provisions, leaving them effectively unchanged.

The second group comprises eight systems used in the areas identified in Annex III:

- biometric systems used without a person's consent (real-time or post identification);
- critical infrastructure and environmental protection;
- education and vocational training;
- employment, employee management and access to self-employment;
- access to private and public services and benefits;
- law enforcement;
- governance migration, asylum, border control;
- administration of justice and democratic processes.

While the Act allows those specific applications of AI systems listed in the Annex can be updated by the Commission, such updates must occur within the specified eight areas.

Thus, as part of Clause 2, environmental protection (AI designed to control emissions and pollution) has been added, while Clause 5 (d) now specifies AI systems used in insurance for calculating insurance premiums, underwriting, and evaluating claims.

As for biometric identification, in general this practice is associated with a substantial risk of invasion of people's privacy and violation of anonymity. While the phrase "without a person's agreement" implies that, in order to use such systems, the person must be informed, the problem of properly informing individuals about such processing has not yet been solved.

Thus, the EDPB and EDPS call for a ban on any use of AI for automatic recognition of human features in public places (faces, gaits, fingerprints, DNA, etc.), as well as systems for biometric categorisation of people. In their joint position, it is also noted that, when it comes to political gatherings and protests, subsequent identification can adversely affect rights and freedoms such as freedom of assembly and association, as well as the fundamental principles of democracy.[15]

[15] Joint Opinion of the European Data Protection Supervisor and of the European Data Protection Board on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (June 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

It is quite problematic to use AI for individual assessments of the risk of committing a crime or the repetition thereof by an individual, as well as for predicting a crime based on profiling or assessment of personal qualities, past behaviour, etc. The use of algorithms to predict future human behaviour in such sensitive areas will inevitably put lower-income brackets of society at risk, leading to discrimination, which in some cases may destroy lives. Therefore, such systems or individual practices of their application, should be classified as prohibited.

The main part of the Act is aimed specifically at regulating high-risk AI. In relation to such systems, suppliers are supposed to provide a risk management system throughout the entire system life cycle, take measures to eliminate or mitigate risks, and conduct post-market monitoring. The Act requires systems to be designed in such a way as to ensure record-keeping during their operation (Article 12), provide transparency of the AI system, ensure availability of information (Article 13). Human control should be conducted throughout the entire life cycle of the system, including the ability to interfere with the system at any time and, if necessary, stop or adjust it (Article 14).

Despite the obvious rationality of the proposed rules, they are rather abstract and require additional practical documents and instructions to ensure compliance in each specific case. The conformity assessment procedure can be based on internal control (self-assessment; Annex VI) or conducted with the participation of a third party (Annex VII). While systems that are subject to EU legislation (Annex II) are also subject to a conformity assessment procedure in accordance with these acts, an AI compliance assessment must be part of this assessment.

With the exception of biometric identification, all of the systems in Annex III are subject to an assessment procedure conducted without the participation of an authorised body. This raises a number of questions. In general, the self-assessment procedure remains controversial due to its potentially insufficiency in terms of protecting human rights.

B. Benifei, the representative of the European Parliament's Internal Market and Consumer Protection Committee (IMCO), referred to the potential failures of such a procedure: "We don't want to detect biases in systems after they've already destroyed families and lives, as has happened in some countries."[16] In their joint position, the EDPB and EDPS also point to the need to adapt the conformity assessment procedure for high-risk systems so that the assessment is always carried out by third parties.

Transparency. While the transparency of AI systems can be difficult to achieve in some cases, it is precisely transparency that can increase citizens' confidence in such systems, as well as provide the ability to control the AI. When this requirement clashes with a trade secret regime, it is important to ensure that the systems are as transparent as possible, at least to the competent supervisory authorities, otherwise we risk finding ourselves in a situation of unexplained actions and decisions that can significantly affect human lives.

Despite the Act containing two Articles on the transparency of AI systems, the uniform wording implies different requirements. Thus, Article 13 (transparency of high-risk systems) deals with the possibility of the interpretation of output data of the system for further use, while Article 52 (transparency of systems with limited risk) refers to the need to inform an individual subject about his or her interaction with the system.[17]

While the Act requires people to be informed when they interact with the AI systems listed in Article 52, it does not contain a similar requirement for high-risk systems that pose an even greater

[16] Bertuzzi, & Killeen, 2022.

[17] Kiseleva, A. (2021, July 29). *Making AI's Transparency Transparent: AI'S: notes on the EU Proposal for the AI Act (2021).* European Law Blog. https://europeanlawblog.eu/2021/07/29/making-ais-transparency-transparent-notes-on-the-eu-proposal-for-the-ai-act/

threat. It remains unclear what information should be specified in such a notification, for example, whether or not information should be included regarding the goals, the logic of the intended actions, or the right to request explanations.

The exception to Article 52 comprises systems used for the detection, prevention, investigation or prosecution of criminal offences. Here again, one cannot fail to note the excessive breadth of the exception. Here it is advisable to distinguish the area of detection and prevention of crimes as requiring greater guarantees for the protection of citizens that take into account the presumption of innocence. It is also possible to cite opinions about the need to completely cancel these exceptions, since the use of such manipulative AI systems without ensuring the required transparency presents a serious threat to fundamental rights.[18]

It should be noted that Article 52 does not contain provisions regarding the possibility of a person to refuse to interact with the system in favour of interacting with a person if this is necessary to protect fundamental rights, as is set out in the Ethics Guidelines for Trustworthy AI prepared by HLEG AI. However, according to the amendments to the Act proposed by the EU Committee on Regions, the scope of opportunities and legal status of individuals interacting with AI systems should not be limited to this interaction.

The EU Committee of the Regions also pointed out the need to systematically notify individuals that they are interacting with the system. The AI Act indicates that individuals should be notified only in cases where this is not obvious from the circumstances and context of use. The Committee also noted: "Natural persons should always be duly informed whenever they encounter AI systems, and this should not be subject to the interpretation of the given situation."[19]

Thus, regardless of whether or not this is obvious from the circumstances of using AI, individuals should always be informed about interactions with AI systems; moreover, this requirement should be extended to high-risk systems that are used in particularly sensitive areas.

Limited-risk systems. Article 52 of the AI Act is aimed at regulating systems with limited risk. These systems, in the opinion of the Commission, do not pose such a significant risk as to be classified as high-risk systems. However, we will try to find out whether these systems are indeed so harmless that they do not require all the complex procedures that are applicable to high-risk AI.

Therefore, the Article specifies the following systems: emotion recognition systems, biometric categorisation systems, deepfakes (systems that generate or manipulate images, audio or video content, real people, objects, places, or other objects or events).

Emotion recognition systems collect and process data and information about a person's mental processes. Examples of such systems can be found in China, where human rights organisations report that Uighurs are undergoing experiments aimed at determining their emotional state.[20] Similar systems can also be used in marketing and social networks aimed at influencing and manipulating people's behaviour in order to mislead them. However, the fact that such systems are not listed as prohibited or high-risk seems rather questionable given the level of risk and questionable use of some of them.

---

[18] Statewatch. (2021, November 30). *EU: Artificial Intelligence Act must put human rights first.* https://www.statewatch.org/news/2021/november/eu-artificial-intelligence-act-must-put-human-rights-first/

[19] Opinion of the European Committee of the Regions on the European approach to artificial intelligence and Artificial Intelligence Act (revised opinion), 2022 O.J. (C 97) 60.

[20] Malgieri, G., & Ienca, M. (2021, July 7). *The EU regulates AI but forgets to protect our mind.* European Law Blog. https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/

Biometric categorisation systems are those aimed at dividing people into categories depending on their ethnicity, gender, political views, sexual orientation etc., based on their biometric data. Deepfakes are fake videos and images created with the intention to discredit or mislead.

According to the Act, it is only possible to provide protection by notifying a person about his or her interaction with the system without providing the opportunity to refuse such interaction. At the same time, the provision concerning the possibility of refusing to interact with the system in favour of interacting with a person is necessary in the context of protecting fundamental rights and ensuring non-discrimination.

Thus, the use of such systems remains insufficiently regulated, except in rare cases when their use causes mental or physical harm or exploits the vulnerabilities of certain groups of people, in which case it will be considered as prohibited.

The need to pay close attention to emotion recognition systems is noted by EDPB and EDPS in their joint statement. Representatives have indicated that the use of emotion recognition systems is highly undesirable and should be prohibited, except for clearly defined applications such as medical applications, where it is necessary to the recognise the emotional state of a patient.[21]

Conclusion

Comprising an all-embracing and ubiquitous technology, artificial intelligence has raised a number of issues that need to be addressed immediately. In order to prepare the ground for overcoming long-term threats, it is of immense importance to quickly and efficiently work out the risks and threats that AI carries.

As one of the leaders in AI regulation, The EU is definitely on the right track, working out comprehensive standards, consulting with all stakeholders in order that the version of the AI Act that is adopted into law takes all relevant factors into account. The post-covid disunity and heterogeneity of the EU member states may be gradually being replaced with a sense of cohesion (Entin & Entina, 2021). Such cohesion of the EU member states is necessary when it comes to regulating the creation and use of AI systems to ensure the protection of its citizens.

The AI Act proposed by the European Commission in April 2021 sets out a number of regulations designed to minimise the threats and risks associated with the rapid development of AI technologies. Once adopted, its provisions will obviously be reflected in both international law and the third-country law; moreover, the Act itself will significantly affect the global artificial intelligence market.

References

1. Desai, D. R., & Kroll, J. A. (2017). Trust but verify: A guide to algorithms and the law. *Harvard Journal of Law & Technology, 31*, 1–64.
2. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for. *Duke Law and Technology Review*, *16*(1), 18–84. https://scholarship.law.duke.edu/dltr/vol16/iss1/2

[21] EDPB Press Release Statement (2021, June 2021). *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination.* https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

3. Entin, M. L., & Entina, E. G. (2021). *V poiskah partnerskih otnoshenij — X: Rossiya i Evropejskij soyuz v 2020 — pervoj polovine 2021 godov* [Looking for partnership — X: Russia and the European Union in 2020 — the first half of 2021]. Zebra E.
4. Ferrer, X., Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: A cross-disciplinary perspective. IEEE Technology and Society Magazine, *40*(2), 72–80. https://doi.org/10.1109/MTS.2021.3056293
5. Hacker, P. (2018). Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU Law. *Common Market Law Review, 55*(4), 1143–1185. https://doi.org/10.54648/cola2018095
6. Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4, Article 100005. https://doi.org/10.1016/j.jrt.2020.100005
7. Samoili, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrev, B. (2020). *AI Watch defining artificial intelligence. Towards an operational definition and taxonomy of artificial intelligence*. Joint Research Centre. https://publications.jrc.ec.europa.eu/repository/handle/JRC118163
8. Siapka, A. (2018). *The ethical and legal challenges of artificial intelligence: The EU response to biased and discriminatory AI*. SSRN. http://dx.doi.org/10.2139/ssrn.3408773
9. Stahl, B., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values. *Computer Law & Security Review, 45*, Article 105661. https://doi.org/10.1016/j.clsr.2022.105661
10. Stefano, V. (2018) *"Negotiating the algorithm": Automation, artificial intelligence and labour protection. Employment*. Working Paper No. 246. International Labour Office, Geneva. https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_policy/documents/publication/wcms_634157.pdf

Information about the authors:

Anna Y. Marchenko* — Ph.D. Student, Department of European Law, MGIMO-University, Moscow, Russia.
anna.yur.marchenko@gmail.com
ORCID: https://orcid.org/0000-0003-1601-7432

Mark L. Entin — Dr. Sci. in Law, Professor, Head of European Law Department, MGIMO-University, Moscow, Russia.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Сведения об авторах:

Марченко А. Ю.* — аспирант кафедры европейского права Московского государственного института международных отношений (МГИМО-Университет) МИД России, Москва, Россия.
anna.yur.marchenko@gmail.com
ORCID: https://orcid.org/0000-0003-1601-7432

Энтин М. Л. — доктор юридических наук, профессор, заведующий кафедрой европейского права Московского государственного института международных отношений (МГИМО-Университет) МИД России, Москва, Россия.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

https://doi.org/10.38044/2686-9136-2022-3-3-58-78

СТАТЬИ

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ЗАКЛЮЧЕНИИ ТОРГОВЫХ ДОГОВОРОВ И ИСПОЛНЕНИИ ОБЯЗАТЕЛЬСТВ ИЗ НИХ[1]

С.Ю. Филиппова

Московский государственный университет имени М.В. Ломоносова
119991, Россия, Москва, Ленинские горы, д. 1

Аннотация

В статье предпринята попытка оценить возможности использования технологий блокчейн и смарт-контракта, больших данных и технологии искусственного интеллекта в классических договорах, опосредующих коммерческий оборот. Кроме того, автор иллюстрирует правовые риски использования информационных технологий и пределы их внедрения в сферу договорного права. Выбранная автором цель предопределила использование формально-юридического метода при анализе действующих норм права. При этом поиск ответов на заданные вопросы невозможно представить без обращения к сравнительно-правовому методу: в статье автор обращается к воззрениям английских и американских ученых при рассмотрении проблем использования технологии искусственного интеллекта в коммерческих договорах.

В результате исследования автор приходит к выводам о том, что (1) смарт-контракты, предназначенные для автоматических трансакций в сети Интернет, не позволяют перемещать реальные товары в реальном мире, поэтому сфера их использования ограничивается только заключением, но не исполнением реализационных договоров; (2) в посреднических договорах, направленных на совершение только юридических действий, смарт-контракт может полностью вытеснить классические договоры и обязательства; (3) при использовании больших данных встает проблема обеспечения права на неприкосновенность частной жизни, поэтому коммерческое использование собранных данных хотя и улучшает сбыт товаров, но ущемляет основные права человека; (4) освоенные возможности по автоматизации отбора контрагентов, определению и изменению условий хранения, по отслеживанию остатков товаров на складе и пр. позволяют говорить о потенциально больших возможностях ИИ в коммерческом обороте.

Ключевые слова

коммерческие договоры, электронная торговля, коммерческое право, Интернет, смарт-контракт, блокчейн, большие данные, искусственный интеллект

[1] При информационной поддержке СПС «Гарант» и СПС «КонсультантПлюс». Законодательство приводится по состоянию на 1 мая 2022 г.

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имело спонсорской поддержки.

Для цитирования Филиппова, С. Ю. (2022). Использование информационных технологий при заключении торговых договоров и исполнении обязательств из них. *Цифровое право, 3*(3), 58–78. https://doi.org/10.38044/2686-9136-2022-3-3-58-78

Поступила: 03.06.2022, принята в печать: 28.08.2022, опубликована: 30.09.2022

ARTICLES

CONCLUSION AND PERFORMANCE OF COMMERCIAL CONTRACTS WITH THE USE OF INFORMATION TECHNOLOGIES

Sofia Y. Filippova

Lomonosov Moscow State University
1, Leninskie Gory, Moscow, Russia, 119991

Abstract

The article attempts to evaluate the possibilities of using blockchain and smart contract technologies, as well as big data and artificial intelligence technologies in traditional commercial contracts. In addition, the author illustrates the legal risks of using information technologies and the limits of their implementation in the field of contract law. The goal chosen by the author predetermined the use of the formal legal method in the analysis of the current legal norms. At the same time, it is impossible to imagine the search for answers to the questions without referring to the comparative legal method: in the article, the author refers to the views of English and American scholars when considering the problems of using artificial intelligence technology in commercial contracts.

As a result of the research, the author comes to the conclusion that firstly smart contracts designed for automatic transactions on the Internet do not allow moving real goods in the real world, therefore the scope of their use is only limited to the conclusion, but not to the execution of contracts of sale. Secondly, a smart contract can completely supplant traditional contracts and obligations in mediation contracts aimed at performing only legal actions. Thirdly, there is a problem of ensuring the right to privacy when using big data, therefore, the commercial use of the collected data, though does improve sales, violates basic human rights. And finally, the mastered capabilities for automating the processes of selecting counterparties, determining and changing storage conditions, tracking the balance of goods in the warehouse, etc., allow author to discuss the potentially great possibilities of using AI in commerce.

Keywords

commercial contracts, electronic commerce, commercial law, Internet, smart contract, blockchain, big data, artificial intelligence

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Filippova, S. Y. (2022). Conclusion and performance of commercial contracts with the use of information technologies. *Digital Law Journal*, *3*(3), 58–78. https://doi.org/10.38044/2686-9136-2022-3-3-58-78

Submitted: 3 Jun. 2022, accepted: 28 Aug. 2022, published: 30 Sep. 2022

Введение

Развитие науки, несомненно, способно улучшить человеческую жизнь. Юриспруденция, являясь одной из старейших и наиболее консервативных научных областей, не всегда может адекватно реагировать на появление новых технологий. Основываясь на базовых идеях, сложившихся еще во времена Римской империи, наука гражданского права не может быстро находить объяснения стремительно изменяющейся реальности. И это, как ни странно, одно из достоинств гражданского права как науки, исследующей частное право, преимущественно основанное на ***внутреннем чувстве права*** людей, весьма ригидном социальном феномене. Юриспруденция основывает свои представления о новых технологиях и их влиянии на социальные отношения, смотря на них через призму базовых ценностей — добра, справедливости, баланса интересов.

В настоящей статье автор выносит на обсуждение юридического сообщества наиболее спорные вопросы, когда остается неясным принципиальное соответствие использования рассматриваемых технологий базовым человеческим ценностям. Автор не ставит задачи обосновать введение запрета на использование технологий в области коммерческих договоров или как-то сдержать развитие науки. Научно-технический прогресс рассматривается автором как константа, использование новейших технологий — это данность, в которой человечеству приходится жить, и задача в том, чтобы *адаптировать классическое правовое регулирование социального взаимодействия с учетом интеграции научных достижений и новых возможностей в классическое правовое регулирование.* Выбранные для настоящей статьи технологии, по мнению автора, затрагивают весьма значимые аспекты *традиционного* устройства российского общества, вопрос о том, где поставить запятую в предложении *«ограничить нельзя разрешить»* применительно к каждой из этих технологий, не имеет однозначного ответа.

В исследовании автор исходит из социологического правопонимания, полагая, что задачей исследования является выявление правового эффекта того или иного регулирования, при котором оценивается воздействие норм права на социальное взаимодействие субъектов, при этом автор критически оценивает возможность получения научного результата с применением только лишь методов догматической юриспруденции, основанных на исследовании позитивного права. Свое понимание юридического метода автор последовательно изложил в ряде научных работ (Filippova, 2013; 2017a; 2017b), настоящая статья является опытом применения инструментального подхода к исследованию использования информационных технологий в коммерческих договорах.

Гипотеза исследования состоит в том, что, основываясь только лишь на идеях получения максимальной прибыли и увеличения сбыта товаров, не может быть построено

правовое регулирование использования информационных технологий, при их регулировании помимо интересов предпринимателей должны учитываться общественные интересы и ценности, использование таких технологий должно быть морально и нравственно приемлемым, для обеспечения такого соответствия право должно использовать «нравственный тест» и отсекать те решения, которые такой тест не проходят. В поиске баланса прибыли и интересов граждан право должно выступать арбитром и внедрять в практику лишь приемлемые решения.

Постановка проблемы

Современный мир немыслим без использования информационных технологий. Каждый коммерсант имеет интернет-сайт, на котором размещает информацию о себе, о предлагаемых товарах, работах и услугах. Девизом современного мира могут служить слова Билла Гейтса: «Если вашего бизнеса нет в Интернете, то вас нет в бизнесе». В экономической литературе отмечают, что интернет-технологии способствуют снижению трансакционных издержек, связанных с поиском информации о товаре и поставщике, клиенте, ведении переговоров, заключением контрактов, мониторингом договорной дисциплины, позволяют повысить производительность труда и, как следствие, обеспечить экономический рост организации[2]. К задачам автоматизации оптовой торговли относят: а) оптимизацию использования площади склада; б) сокращение затрат на хранение товара на складе; в) сокращение времени проведения складских операций; г) сокращение количества ошибочных складских операций; д) повышение точности учета товаров; е) снижение потерь, связанных с ограниченным сроком реализации товаров; ж) уменьшение зависимости от человеческого фактора[3]. Акцент на оптимизацию с помощью информационных технологий складского хозяйства понятен — именно складское хозяйство — узкое место торговли, главный ограничитель ее развития. Это связано с тем, что объемы продаваемых товаров полностью зависят от того, существуют ли условия для обеспечения сохранности товара на его пути от производителя к потребителю. Избыточное наполнение склада товарами одного наименования при отсутствии товаров других наименований создает сложности в обеспечении ассортимента товаров розничного продавца, а значит приводит к снижению прибыли всех звеньев канала сбыта и лиц, содействующих торговле. Оптимизация складского хранения — прямой путь к увеличению продаж. Но, конечно, не единственный. Справедливо отмечают, что «никакие вложения в интернет-технологии сами по себе в изоляции от процессов реинжиниринга не способны обеспечить прибыль торгового предприятия, которая зависит в том числе и от работы с поставщиками и покупателями»[4]. Действительно, заключение коммерческих договоров выполняет множество функций, при всех преимуществах информационных технологий им не удастся наладить сотрудничество между контрагентами, не удастся разработать новый вид товара, новую технологию, расширить ассортимент товаров за счет включения инновационных продуктов. Все то, где речь идет о творчестве, необходимости отступления от норм, шаблонов, личных отношениях — это недоступное для информационных технологий поле — поле деятельности человека.

Простейшие технологии, используемые в деятельности торговой организации, позволяют собирать информацию о качестве товаров, принимать и обрабатывать информацию от покупателей о выявленных недостатках, удобстве пользования, достоинствах и недостатках

[2] Сибирская, Е. В., Старцева, О. А. (2008). *Электронная коммерция: учебное пособие*. Форум.

[3] Гаврилов, Л. П. (2015). *Информационные технологии в коммерции: учебное пособие.* Инфра-М.

[4] Сибирская, Старцева, 2008.

дизайна, на основании которой принимать решения о расширении ассортимента товаров, выводе из ассортимента тех или иных позиций, разрабатывать рекомендации производителю о внесении изменений в конструкцию или дизайн того или иного товара. С помощью использования информационных технологий существенно упрощается планирование ресурсов. Широко используются разнообразные технологии электронного документооборота между поставщиком и покупателями, между производителем товара, складскими организациями, транспортными организациями, экспедиторами. Организуются онлайн-сообщества для общения в режиме реального времени, с использованием ботов организуются ответы на наиболее распространенные вопросы. Сегодня исследование спроса осуществляется посредством автоматизированной оценки поведения потенциальных потребителей в сети Интернет, и место традиционных опросов общественного мнения занимают технологии обработки выражения микроэмоций пользователями технических устройств и их поведения в социальных сетях, остатки товаров на складе отслеживаются автоматически, и на основании текущего состояния складских остатков формируются заявки поставщикам товаров, процесс подачи и согласования заявок занимает мгновения, не требует длительных согласований по отделам снабжения и сбыта организаций, все шире распространяются электронные площадки и посредники, агрегаторы, и иные специальные субъекты, существенно изменяющие сам процесс создания правовых связей между коммерсантами. Все это требует учета специфики происходящих процессов в юридическом сопровождении коммерческого оборота, а значит, дополнительных знаний и умений от юристов, сопровождающих коммерческий оборот товаров. Встает вопрос: что происходит с «традиционным» коммерческим правом в связи со столь широким распространением информационных технологий?

В юридической литературе спектр мнения на этот счет весьма велик, начиная от утверждений о «начале конца договорного права» (Savelyev, 2016), когда новым технологиям приписывается столь глобальное воздействие на процессы формирования воли, что требуется формирование некоего нового права, основанного на иных принципах и положениях, заканчивая тезисом о «свободе права от технологий», вследствие чего максимы и конструкции, разработанные во времена рабовладельческого Рима, рассматриваются как вполне пригодные для обслуживания цифровизации экономики. Как видится, истина где-то посредине. Информационные технологии нельзя игнорировать, поскольку их использование влияет на все процессы хозяйственной деятельности предпринимателя от производства товара до организации сбыта. Вряд ли можно всерьез утверждать, что все эти процессы не влияют на коммерческий оборот товаров. Но, с другой стороны, за каждым товаром мыслится его потребитель, а значит, и его воля. Все коммерческое право, так или иначе, призвано обслуживать потребность человека в товаре, а раз так, исключить человека из права нельзя, а значит, свою сущность социального регулятора право не потеряет и базовые категории права, такие как свобода, воля, действие, не исчезнут в обозримом будущем. Вопрос лишь в форме и способах их выражения на конкретном этапе развития общества.

Среди множества весьма несложных и уже хорошо освоенных технологий, таких как электронная почта, электронные таблицы, электронная подпись как средство индивидуализации, существуют технологи следующего уровня, действительно существенно влияющих на архитектуру продаж товаров. Согласно п. 36 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 09.05.2017 № 203, основными направлениями развития российских информационных и коммуникационных технологий являются: а) конвергенция сетей связи и создание сетей связи нового поколения;

б) обработка больших объемов данных; в) искусственный интеллект; г) доверенные технологии электронной идентификации и аутентификации, в том числе в кредитно-финансовой сфере; д) облачные и туманные вычисления; е) интернет вещей и индустриальный интернет; ж) робототехника и биотехнологии; з) радиотехника и электронная компонентная база; и) информационная безопасность. Некоторые из этих технологий, такие как биотехнологии, радиотехника, пока слабо используются в области коммерческого оборота, но некоторые из них внедряются в него весьма активно. Наибольшее число вопросов вызывает использование доверенных технологий электронной идентификации и аутентификации, в частности технологии блокчейн, Big Data (обработка больших объемов данных), искусственного интеллекта. Рассмотрим, что же это за технологии, и выявим, как именно они используются в коммерческих договорах.

Использование технологии блокчейн в коммерческих договорах

Начнем рассмотрение современного коммерческого оборота с применения технологии «блокчейн». Технологическая составляющая блокчейн подробно описана в литературе (например, Churilov, 2021), для юриста технические подробности значения не имеют, достаточно понимать основные практические результаты, обеспечиваемые ее использованием. Как отмечают в литературе, блокчейн представляет собой децентрализованную распределенную базу данных («учетную книгу»), содержащую информацию о трансакциях, совершенных в отношении определенного актива, которые подтверждены с помощью технологии криптографического преобразования. Преимуществами блокчейна рассматривают: 1) децентрализацию хранения информации, с помощью которой минимизируются риски ее утраты в результате повреждения одного или даже нескольких устройств, входящих в систему хранения и обработки информации; 2) высокую степень безопасности (защиты от взлома) за счет использования средств шифрования при проведении каждой трансакции и распределения данных среди множества устройств; 3) стабильность внесенной информации, обозначающую невозможность (существенная техническая сложность) изменения данных блокчейна после совершения трансакции; 4) скорость совершения трансакции, которая обеспечивается за счет автоматизированного обмена данными; 5) прозрачность, состоящую в том, что действия в системе блокчейна документируются и доступны для ознакомления всем участникам системы (Savelyev, 2017; Sannikova, 2019; Churilov, 2021). Возможно функционирование публичного и частного блокчейна, где публичный блокчейн не предполагает ограничений по доступу в систему, все обладают равными правами, отсутствует администратор или оператор системы с наличием особых прав. Частный блокчейн — это закрытая информационная система, доступ к которой регламентируется определенным лицом (администратором), распределяющим среди участников права по доступу и внесению изменений в отношении данных блокчейна.

На системе блокчейн функционирует технология «смарт-контракта», которая представляет собой самоисполняющийся договор, где информационная система без участия человека выявляет соответствие реальной ситуации определенным условиями и при совпадении условий с заданными параметрами проводит трансакцию, то есть списывает со счета участников договора определенные виртуальные отображения объектов (цифровые права), по поводу которых заключен данный договор. Существует множество блокчейн-систем, на которых функционируют смарт-контракты, например известны системы Etherium, BlockStream. В строгом смысле слова смарт-контракт — это не вполне договор в том смысле, что это не вербально выраженное соглашение сторон, а компьютерный код. В литературе справедливо замечают,

что сложные тексты условий договоров не всегда могут быть переведены в математический алгоритм и прописаны в программе (Uvarov & Uvarov, 2020).

Как отмечал Ник Сзабо, смарт-контракт — это компьютерный протокол, самостоятельно исполняющий сделки, а также контролирующий их исполнение, при реализации которого нарушение договора становится экономически неоправданным (Szabo, 1997). Иначе говоря, потенциальная возможность нарушения договорного обязательства в принципе остается возможной, однако становится чрезмерно сложной и дорогой, причем тем сложнее и дороже, чем больше устройств объединены в блокчейн, и для публичных блокчейнов и частных блокчейнов, объединивших сотни тысяч устройств, такая вероятность становится близкой к нулю. Отметим, что самим термином «смарт-контракт» обозначают не только гражданско-правовой договор, являющийся основанием возникновения обязательства, но вообще любое автоматическое приобретение и (или) осуществление определенных субъективных прав, причем не только в имущественной сфере, но и при взаимодействии с государственными органами. Например, рассматривается выдача с помощью смарт-контрактов в системе блокчейн гражданских паспортов, водительских удостоверений, медицинских справок, документов об образовании. В гражданско-правовой сфере с помощью смарт-контрактов предлагают выдавать банковские гарантии, заключать и исполнять договоры имущественного страхования, размещать государственные облигационные займы и пр. Такая широкая сфера использования этой технологии и приводит к некоторому смешению технологической и правовой составляющей происходящего. Между тем это вряд ли оправданно. Представляется, что если на технологии блокчейн в автоматизированном режиме происходит взаимодействие гражданина или юридического лица с государством, проводится действие по государственной регистрации, выдача справки или иного документа, то правовая природа и последствия данного взаимодействия должны определяться исходя из установленных для административного акта, если же речь идет о самоисполняющемся обязательстве, то его гражданско-правовой характер требует применения к нему правил о сделках, договорах, обязательствах. Ни в том ни в другом ***случае нельзя говорить об отсутствии воли субъектов, ее замене компьютерной программой***. В подобных случаях речь идет о действии под отлагательным условием, при наступлении которого возникает правовой эффект выраженной лицом воли.

По схеме смарт-контракта осуществляется взаимодействие между авиакомпанией S7 Airlines и компанией по продаже билетов S7 Ticket (Zaynutdinova, 2020). Однако отметим, что продажа билетов является лишь одним элементом в системе организации перевозки пассажира, тогда как само исполнение обязательства перевозки в любом случае осуществляется не в системе блокчейн, ***а путем фактических действий, совершаемых авиаперевозчиком*** по перемещению в пространстве пассажира из места отправления в место назначения а воздушном судне, отвечающем требованиям безопасности, при этом должны соблюдаться сроки перевозки, обеспечиваться определенный уровень сервиса и пр. На этом примере хорошо видно, *что смарт-контракт не может заменить весь технологический процесс, а только небольшую часть* (на данную технологию переводится лишь заключение и исполнение посреднического договора).

Приведенный пример с использованием смарт-контракта в пассажирской перевозке хорошо демонстрирует одну из ключевых проблем ***использования смарт-контрактов в коммерческой деятельности***. Технология смарт-контракта предполагает предоставление по обязательству из такого договора ***цифровых прав***, правовая природа которых в настоящее время исходя из буквального толкования ст. 128 ГК РФ определена как ***имущественные права***, тогда

как для торгового оборота основным объектом и основным видом товаров являются ***вещи*** (определенные родовыми признаками, имеющие потребительскую и меновую стоимость) (Puginskiy, 2013)[5]. И это неслучайно. Именно вещи предназначены для удовлетворения базовых человеческих потребностей (в питании, одежде и пр.), поэтому при любом развитии цифровой и виртуальной реальности, продвижении информационных технологий, для обеспечения потребности людей в еде, одежде, мебели, бытовой технике, и пр. нужно будет производить реальные вещи, а значит — продавать, хранить, перевозить, доставлять, ремонтировать эти вещи, и все это будет происходит в реальном, а не виртуальном мире, где могут «жить» лишь виртуальные отображения этих реальных вещей. Можно согласиться с тем, что отдельные «классические» объекты могут трансформироваться и адаптироваться для использования в смарт-контрактах, в частности речь идет о денежных средствах. Как справедливо замечает А.Ю. Чурилов (Churilov, 2021), нет препятствий для использования смарт-контрактов при аккредитивной форме расчетов, когда смарт-контракт будет направлять информацию в банк-исполнитель, который в дальнейшем осуществит перевод денежных средств. Действительно, встречное предоставление в виде оплаты товаров денежными средствами для использования в смарт-контракте вполне можно организовать с помощью системы договорных инструментов (вышеупомянутая аккредитивная форма расчетов, расчеты по инкассо, использование эскроу-агентов и пр.). С помощью смарт-контрактов возможна оптимизация процесса подачи заявок, отгрузочных разнарядок по заключенному договору поставки с открытым условием, когда такие заявки будут подаваться и согласовываться в автоматическом режиме, например при совпадении условия «наличие товара на складе» с условием «количество заказанного товара», при этом самоисполняющимся такой договор может стать лишь в одном элементе — в части оплаты (предоставления встречного предоставления в виде денежных средств, криптовалюты, иных цифровых прав). Однако поскольку передача товара требует совершения фактических действий в реальном мире, то существует риск ненадлежащего исполнения такого обязательства, например предоставления некачественного товара, ненадлежащей упаковки, затаривания и пр. Это значит, что при заключении и исполнении реализационных договоров технология смарт-контракта может использоваться ограниченно, поскольку она не позволяет обеспечить совершение фактических действий по передаче вещей в реальном мире. На технологии могут быть организованы заключение договора, подача заявок, принятие заявок, оплата товаров.

Технология смарт-контракта может использоваться для заключения и исполнения ***посреднических договоров***, не предполагающих совершения фактических действий, например договоров поручения или комиссии, поскольку эти действия могут полностью быть реализованы в виде предоставления имущественных прав, если посреднический договор предполагает совершение как юридических, так и фактических действий, то технология смарт-контракт может лишь частично сопровождать заключение и исполнение таких договоров.

Большая часть ***договоров, содействующих торговле,*** предполагает совершение одной из сторон фактических действий (хранение, перевозка, маркетинговые исследования, обучение персонала), в этой части действует та же логика, что применительно к реализационным и посредническим договорам, то есть использование технологии смарт-контракта не может полностью обеспечить весь цикл обязательства в подобных случаях, а могут использоваться лишь на отдельном его участке, как правило, заключения договора и предоставления встречного

[5] См. напр.: Абросимова, Е. А., Белов, В. А., Пугинский, Б. И. (ред.). (2021). *Коммерческое право: учебник*. Издательство Юрайт.

исполнения. При этом основное исполнение осуществляется путем фактических человеческих действий и контролируется обычными волей и поведением субъектов права.

Использование технологии Big Data в коммерческих договорах

Одна из важнейших информационных технологий, используемых в самых разных сферах, в том числе и в области коммерческих договоров, — это ***технология обработки больших данных***. В литературе большие данные определяют как «динамически изменяющийся массив информации, который представляет собой ценность в силу своих больших объемов и возможности эффективной и быстрой обработки автоматизированными средствами, что, в свою очередь, обеспечивает возможность его использования для аналитики, прогнозирования и автоматизации бизнес-процессов» (Savelyev, 2018). Таким образом, речь идет об информации, но не о любой, а особой. Ее признаки состоят, во-первых, в ее значительном объеме (количественный признак); во-вторых, в назначении этой информации, поскольку таковая может быть использована для прогнозирования (этот признак можно назвать качественным). И третьим признаком является технологическая особенность обработки информации (Savelyev, 2018). В этой связи не будут рассматриваться в качестве больших данных, скажем, каталог библиотечных карточек, который хотя и может включать в себя несколько миллионов записей, не обладает свойством быстрой технологической обработки.

Большие данные представляют собой ***информацию***, однако информация как таковая не является объектом гражданских прав, соответствующая статья была исключена из Гражданского кодекса РФ. Не останавливаясь на правильности данного законодательного решения, отметим, что такое исключение информации из числа объектов гражданских прав является серьезным вызовом в части юридического сопровождения оборота больших данных. Несмотря на то что, согласно ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация может являться объектом публичных, гражданских и иных правовых отношений, она может свободно использоваться любым лицом и передаваться одним лицом другому, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения, ясности о правовом режиме информации нет. По поводу информации могут заключаться договоры о сборе, обработке информации. В статье 783.1 ГК РФ легализован договор об оказании услуг по предоставлению информации. Однако в подобных случаях объектом является не информация как таковая, а услуги по поводу ее сбора и обработки. Когда же речь идет о коммерциализации больших данных, информация предстает уже готовой к использованию. Сбор, обработка и маркировка этой информации уже осуществлена оператором больших данных, на рынке она представлена как готовый продукт, поэтому использование конструкций договора возмездного оказания информационных услуг не вполне соответствует правовой цели сторон и существу их правоотношения. В юридической литературе высказано предположение, что Большие данные сами по себе являются общественным достоянием, в обороте они могут присутствовать только как обработанные и систематизированные для определенных целей (Sannikova & Kharitonova, 2020). В качестве одного из объектов гражданского права, относящегося к группе результатов интеллектуальной деятельности, являются ***базы данных***, на которые признается исключительное право и установлен правовой режим их использования. Согласно ст. 1260 ГК РФ базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов,

судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ). Согласно ст. 1333 ГК РФ, изготовителем базы данных признается лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов. При рассмотрении больших данных в качестве базы данных акцент смещается с содержательной составляющей информации на ее технологическую форму, что в целом соответствует сущности данного феномена и не тормозит оборот больших данных и их коммерческое использование.

Большие данных по источнику формирования можно разделить на: 1) данные, обрабатываемые в специализированных системах организации (данные о сотрудниках, о закупаемой и реализуемой продукции, бухгалтерские данные); 2) данные, созданные пользователями сети Интернет (информация, доступная в социальных сетях, на форумах, тематических веб-сайтах); 3) данные, создаваемые техническими устройствами (лог-файлы, данные геолокационных устройств, показатели датчиков и сенсоров и т. д.) (Lapteva, 2019). Коммерческую ценность могут представлять все виды данных, ***но их правовой режим различается.*** Так, сведения, собранные коммерческим банком о своих клиентах и средствах на их счетах, а также покупках, совершаемых клиентами банка и оплачиваемых банковской картой, охраняются ***режимом банковской тайны*** (ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»), информация, предоставленная работодателю работником, имеет правовой ***режим персональных данных***, режим информации, собираемой камерами видеонаблюдения, различается в зависимости от места установки таких камер и может рассматриваться ***как правомерно полученная информация***[6] и как ***сведения, полученные при незаконном вмешательстве в частную жизнь***[7] и пр. В зависимости от правового режима таких данных, различаются основания и порядок их сбора и последующей обработки. Для некоторых видов информации всякая обработка и передача третьим ***лицам не допускается***, для других — это ***возможно с согласия лица***, о котором собирается такая информация, третьи виды информации собираются и ***обрабатываются свободно***. Для коммерческого оборота важно понимать, какая именно информация собрана и систематизирована, поскольку предоставление исключительного права или отчуждение права на базу данных, содержащую информацию, запрещенную к сбору и обработке и образующую режим тайны, является противоправным действием. Соответствующий договор является ничтожным в соответствии с п. 2 ст. 168 ГК РФ, согласно которому сделка, нарушающая требования закона или иного правового акта и при этом посягающая на публичные интересы либо права и охраняемые законом интересы третьих лиц, ничтожна, если иное не установлено законом. В данном случае в зависимости от вида тайны данный договор нарушает либо публичные интересы (если речь о государственной тайне), либо интересы третьих лиц (если разглашается информация о третьих лицах, полученная незаконным путем).

В современных условиях коммерчески значимые большие данные получаются путем обработки данных технических устройств, например смартфонов, фитнес-браслетов пользователей, которые в автоматическом режиме записывают различные данные своих пользователей, затем передают эти данные в обезличенной форме определенному оператору, где обрабатываются с помощью компьютерной технологии, на их основе формируется база данных. Такая база

[6] Апелляционное определение Верховного суда Республики Коми от 04.02.2019 по делу № 33-640/2019; Апелляционное определение Алтайского краевого суда от 11.12.2018 № 33-11159/2018.

[7] Определение Четвертого кассационного суда общей юрисдикции от 16.07.2020 по делу № 88-9915/2020; Определение Шестого кассационного суда общей юрисдикции от 23.12.2020 по делу № 88-25139/2020.

данных имеет коммерческую ценность, поскольку позволяет прогнозировать поведение субъектов. Подобные базы формируются на основе изучения поведения потребителей в сети Интернет. Например, в настоящее время существует возможность с помощью встроенных в технические устройства пользователей камеры фиксировать микроэмоции, зоны экрана, на которых пользователи задерживают взгляд и путем обработки таких данных выявлять, какие именно образы, цвета, формы вызывают позитивные или негативные эмоции пользователей. Существуют технологии отслеживания поведения пользователей в сети Интернет, например предпочтения в социальных сетях, с помощью информационных технологий все подобные сведения могут обрабатываться, и на основе полученных данных формироваться образ потенциального покупателя товаров, с учетом личных качеств которого может строиться технология продажи товара. Согласно п. 14 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 09.05.2017 № 203, главным способом обеспечения эффективности цифровой экономики становится внедрение технологии обработки данных, что позволят уменьшить затраты при производстве товаров и оказании услуг. Там же отмечается, что конкурентным преимуществом на мировом рынке обладают государства, отрасли экономики которых основываются на технологиях анализа больших объемов данных. Такие технологии активно используются в России, но они основаны на зарубежных разработках. В Стратегии отмечается отсутствие отечественных аналогов подобных систем. События весны 2022 года, когда Россия столкнулась с санкциями иностранных государств, которые привели в том числе и к ограничениям в использовании правомерно приобретенных по лицензионным договорам программ для ЭВМ, сбоев в работе технических устройств, вызванных умышленными действиями субъектов из недружественных государств и пр., показали, что подобные ситуации создают существенные риски для отечественной экономики. В Стратегии было указано, что повсеместное внедрение иностранных информационных и коммуникационных технологий, в том числе на объектах критической информационной инфраструктуры, усложняет решение задачи по обеспечению защиты интересов граждан и государства в информационной сфере. Эти опасения нашли подтверждение. С использованием сети Интернет совершаются компьютерные атаки на государственные и частные информационные ресурсы, на объекты критической информационной инфраструктуры. Получается, что использование технологий обработки больших данных должно обеспечивать решение задач не только частного права, коммерсантов, но и безопасность использования таких технологий на государственном уровне, для этого должно внедряться импортозамещение не только на товарном рынке, но и на рынке технологий обработки больших данных.

Большие данные позволяют перевести технологии продажи на новый уровень, что создают новые возможности для коммерсантов и для всего общества. При этом в литературе отмечают, что данные технологии создают новые риски нарушения конституционных прав и свобод граждан. В частности, отмечают риски, связанные с нарушением неприкосновенности частной жизни, риски утраты контроля за использованием собранных данных, влекущей возможности совершения мошеннических действий; обработки неточных или неполных данных, в результате которой может быть причинен вред гражданам; дискриминации, когда на основе обработанных данных может производиться отсев граждан по расовым, политическим, национальным, гендерным или иным дискриминационным критериям (Savelyev, 2018).

Дилемма коммерческой ценности и неприкосновенности частной жизни решается посредством обезличения собранных данных для их обработки и коммерческого использования. Согласно ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

под **обезличиванием персональных данных** понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Требования и методы такого обезличивания утверждены Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Согласно п. 3 этих требований, обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных: полноту, структурированность, релевантность, семантическую целостность, применимость, анонимность. В соответствии с данным документом любое обезличивание должно предполагать обратимость, то есть потенциальную возможность преобразования, обратного обезличивания (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность (п. 5).

Технологии больших данных активно используются в торговле, особенно значима эта информация в договорах на проведение маркетинговых исследований и организации рекламной кампании. Для лиц, выступающих заказчиками в таких договорах и желающих, чтобы в процессе проведения исследований использовались обработанные большие данные для формирования портрета потенциального потребителя товара, важно корректно описывать информацию, которую они желали бы использовать при составлении отчета с учетом рисков, связанных с использованием информации, полученной или обработанной с нарушением законодательства о разных видах тайн или персональных данных. Стоит помнить об установленной ответственности, в том числе за действия третьих лиц, привлеченных к исполнению обязательства по договору. Представляется целесообразным использовать в договорах, связанных с обработкой больших данных заверений об обстоятельствах, даваемых оператором больших данных или иным управомоченным лицом, содержащим указание на соблюдение закона при сборе и обработке информации, в том числе персональных данных, использовании надлежащих средств обезличения информации, а также целесообразно устанавливать обязанность оператора или иного управомоченного на отчуждение базы данных или предоставления прав на нее лица возместить потери в определенной договором сумме при привлечении к ответственности за использование информации ограниченного доступа, нарушение прав третьих лиц, а также неустойку на случай некорректной обработки такой информации, в результате которой полученные выводы оказались недостоверными. Инструменты возмещения потерь (ст. 406.1 ГК РФ) и неустойки являются более предпочтительными, чем возмещение убытков вследствие сложностей в определении размера убытков и причинной связи между противоправным действием оператора и убытками приобретателя больших данных.

Использование технологии искусственного интеллекта в коммерческих договорах

Искусственный интеллект — это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека (п. 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года,

утвержденной Указом Президента РФ от 10.10.2019 № 490). Как видно из этого определения, технология искусственного интеллекта позволяет имитировать человеческие решения. Основной чертой искусственного интеллекта является его способность самостоятельно формировать алгоритм принятия решения и менять его при изменении вводных данных.

В зарубежной литературе искусственный интеллект определяется как «способность системы правильно интерпретировать внешние данные, извлекать знания из этих данных и использовать их для достижения конкретных целей и задач посредством гибкой адаптации» (Kaplan et al., 2018). Как видим, здесь акцент сделан не на имитацию человеческого решения, а лишь на правильность принятых решений и адаптивность самой системы.

Как отмечают в литературе, научное осмысление и разработка категории искусственного интеллекта начались с середины XX века, то есть задолго до появления современных технологий машинного обучения. Считается, что одним из основоположников теории искусственного интеллекта явился Алан Тьюринг, который в 1947 г. в докладе «Интеллектуальные машины» поставил вопрос о том, может ли машина продемонстрировать разумное поведение. Далее, в статье «Вычислительные машины и разум» в 1950 г., он предложил публике тест (впоследствии получивший имя автора), с помощью которого можно было сравнить машинный интеллект с человеческим (Turing, 1950). Иногда зачатки использования технологий искусственного интеллекта обнаруживают и в более давние времена. Предполагают, что идея создания искусственного интеллекта принадлежит Р. Луллию (XIV в.), который предпринял попытку выработать механизм «решения задач на основе классификации понятий» (Korovnikova, 2021).

Расцвет развития исследований в области искусственного интеллекта пришелся на период с конца 1950-х до середины 1970-х годов, на эту технологию возлагались большие надежды по улучшению эффективности производства, неуклонное улучшение производственных мощностей компьютеров создавало иллюзию, что вот еще буквально пара шагов отделяет компьютерные технологии от креативных возможностей, доступных человеку. Эйфория, связанная с компьютерной игрой в шахматы, компьютерными предсказаниями, основанными на анализе информации, приводила в эту сферу новых исследователей, которые прилагали усилия по решению поставленной задачи создания компьютерной программы, способной достоверно имитировать решения, принимаемые человеком. Бум IT-сферы, в частности, основывался на видимости огромных перспектив данной научной исследовательской области. Однако к концу 1970-х и до середины 1980-х годов темп исследований искусственного интеллекта снизился, это было вызвано разочарованием в эффективности исследований, казалось, что проблема носит технический характер и препятствием в развитии технологий является недостаток компьютерных мощностей. Интерес к проблематике возродился в конце 1980-х годов в связи с проектом по созданию «компьютера пятого поколения», инвестиции в который были вложены японским правительством (Begishev & Khisamova, 2018).

Для адекватной работы данной технологии искусственный интеллект нужно изначально «обучить», то есть маркировать определенным образом значительный объем данных, проанализировав эти данные, искусственный интеллект выявит закономерности и далее сможет самостоятельно проверять данные и их классифицировать. Как отмечается в национальной стратегии, для поиска вычислительной системой непредвзятого решения требуется ввести репрезентативный, релевантный и корректно размеченный набор данных (п. 8). Если на этой стадии возникают ошибки, обусловленные человеческим фактором или неправильной выборкой, то в дальнейшем решения, принятые искусственным интеллектом, оказываются нерелевантными ситуации, а порой дискриминационными и аморальными. Поскольку

собственных представлений о добре и зле (этики и морали) у технологии искусственного интеллекта нет, то «вершителем судеб» внезапно оказывается программист и лицо, осуществлявшее маркировку вводимых в программу данных. Этические проблемы использования искусственного интеллекта в настоящее время являются недооцененными, о чем хорошо свидетельствует п. 48 Национальной стратегии, согласно которому, для стимулирования развития и использования технологий искусственного интеллекта необходимы адаптация нормативного регулирования в части, касающейся взаимодействия человека с искусственным интеллектом, и выработка соответствующих этических норм. При этом избыточное регулирование в этой сфере может существенно замедлить темп развития и внедрения технологических решений. Как видно, разработчикам стратегии не вполне ясно, откуда в принципе берутся этические нормы, они полагают, что таковые можно ***разработать***, при этом они полагают, что затягивание этого процесса мешает внедрению технологий в жизнь. Такой подход удручает. Превенция всегда рассматривалась как более предпочтительный способ воздействия, чем ответственность, поэтому вряд ли стоит спешить внедрять технологии при неизвестности того, как именно будут решаться неизбежно возникающие в будущем проблемы.

Еще один весьма любопытный документ, регламентирующий основные направления развития технологии искусственного интеллекта, — Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года, которая была утверждена Распоряжением Правительства РФ от 19 августа 2020 г. № 2129-р. Согласно данному документу, целью Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники (далее — Концепция) является определение основных подходов к трансформации системы нормативного регулирования в Российской Федерации для обеспечения возможности создания и применения таких технологий в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства (раздел 1 Концепции). В отличие от предыдущего упомянутого документа — Национальной стратегии, где правовые и этические риски использования технологий искусственного интеллекта явно оценивались как вторичные, менее значимые, чем технические проблемы, в этом документе отмечается, что «развитие технологий искусственного интеллекта ставит серьезные вызовы перед правовой системой Российской Федерации, системой государственного управления и обществом в целом. Они обусловлены определенной степенью автономности действий систем искусственного интеллекта в решении поставленных задач и их неспособностью непосредственно воспринимать этические и правовые нормы, учитывать их при осуществлении каких-либо действий». Как видим, проблематика уже осознана и вопросы поставлены, что можно считать позитивным итогом осмысления использования технологий искусственного интеллекта и обсуждения на разных дискуссионных площадках. В Концепции отмечается, что для развития технологий искусственного интеллекта и робототехники необходимо создание регуляторной среды, комфортной для безопасного развития и внедрения указанных технологий, основанной на балансе интересов человека, общества, государства, компаний — разработчиков систем искусственного интеллекта и робототехники, а также потребителей их товаров, работ, услуг. При этом, как справедливо констатируют разработчики Концепции, «представления об этом балансе существенно разнятся».

В Концепции заявляется ряд принципов использования технологии искусственного интеллекта, однако каждый из них вызывает ряд вопросов.

В частности, в Концепции в качестве первого принципа заявлено стимулирование развития технологий искусственного интеллекта и робототехники регуляторными средствами

в качестве основного вектора развития регулирования. Представляется, что исходя из заявленных в преамбуле сложностей, указание на приоритетность стимулирования развития технологии ИИ, несмотря на нерешенность этических проблем, выглядит несколько противоречиво и нереалистично. Аналогичные возражения касаются и второго названного в Концепции принципа, состоящего в том, что регуляторное воздействие, основанное на риск-ориентированном, междисциплинарном подходе предусматривает принятие ограничительных норм в случае, если применение технологий искусственного интеллекта и робототехники несет объективно высокий риск причинения вреда участникам общественных отношений, правам человека и интересам общества и государства. Иначе говоря, заявляется преимущественно дозволительное регулирование использование технологий искусственного интеллекта при отсутствии четких указаний на сферы, требующие императивных ограничений. Эта идея продолжается и в следующем принципе, названном в Концепции, состоящем в расширении применения инструментов сорегулирования и саморегулирования, формирование кодексов (сводов) этических правил разработки, внедрения и применения технологий искусственного интеллекта и робототехники. Следующий заявленный принцип вызывает недоумение в той части, что вряд ли необходимо было в принципе его фиксировать в нормативном правовом акте. Согласно Концепции установлен человеко-ориентированный подход, предусматривающий, что конечной целью развития технологий искусственного интеллекта и робототехники, направляемого посредством регуляторного воздействия, является обеспечение защиты гарантированных российским и международным законодательством прав и свобод человека и повышение благосостояния и качества жизни граждан. С одной стороны, как уже неоднократно отмечалось, все технологии предназначены служить именно человеку, это обстоятельство можно вынести за скобки и не указывать в каждом нормативном правовом акте, с другой стороны, возложение защиты прав и свобод человека исключительно на технологии искусственного интеллекта вряд ли оправданно.

Следующее положение, несмотря на отнесение его в Концепции к числу принципов, вряд ли является таковым по своей онтологической природе. Согласно Концепции предусмотрена оценка воздействия технологий и систем искусственного интеллекта и робототехники на все сферы жизни человека, общества и государства, основанная на научно выверенных исследованиях с подключением широкого круга ученых. Это положение имеет природу не основополагающего начала регулирования, а одну из регулятивных норм, направленных на установление правил использования технологии и устанавливающих обязательную оценку последствий использования.

Согласно Концепции, при использовании технологий искусственного интеллекта должен обеспечиваться баланс интересов разработчиков, потребителей и иных лиц в сфере искусственного интеллекта и робототехники, однако как именно искать этот баланс и как определять «сбалансированность» таких интересов, остается неясным. Согласно Концепции, должны быть определены границы ответственности различных субъектов, участвующих в отношениях по использованию этой технологии за возможные негативные последствия. Можно заметить, что подобные границы должны быть установлены вообще во всех сферах правового регулирования, однако поиск адекватных границ — пока лишь одна из актуальных будущих задач.

Весьма актуальным на современном этапе с учетом серьезного геополитического кризиса является реализация установленного Концепцией технологического суверенитета, предусматривающего обеспечение необходимого уровня независимости Российской Федерации в области искусственного интеллекта и робототехники с учетом государственной политики

в сфере развития информационных технологий и импортозамещения. После 2014 года, показавшего несостоятельность надежд на повсеместное надежное международное сотрудничество в различных сферах, был взят курс на импортозамещение в разных сферах, особенно в значимых, события 2022 года показали значимость задач обеспечения такого суверенитета, поэтому установление данного принципа в Концепции оказалось весьма прозорливым решением, хотя о его полной реализации пока говорить не приходится.

Концепция в качестве одного из принципов устанавливает поддержку конкуренции, обеспечение равных для всех, включая предприятия малого и среднего бизнеса, возможностей для применения экспериментальных правовых режимов и мер государственной поддержки, а также для доступа к необходимым в целях разработки систем искусственного интеллекта и робототехники данным из государственных и муниципальных информационных систем.

Остальные названные в Концепции принципы тесно связаны с уже названными и развивают их, это относится к принципу, устанавливающему оценку при разработке нормативных правовых актов и иных документов в сфере искусственного интеллекта и робототехники социально-экономических последствий и рисков в условиях постоянного развития технологий, учет как положительного, так и отрицательного международного опыта регулирования; обязательность обоснованной оценки рисков причинения при применении искусственного интеллекта и робототехники вреда жизни и здоровью человека, реализации угроз обороне страны и безопасности государства и принятие мер, направленных на минимизацию таких рисков и угроз.

Отдельно стоит отметить названные в Концепции базовые этические нормы использования технологии искусственного интеллекта. Так, Концепция устанавливает приоритет благополучия и безопасности человека, защиты его основополагающих прав и свобод (цель обеспечения благополучия и безопасности человека должна преобладать над иными целями разработки и применения систем искусственного интеллекта и робототехники). Возникает вопрос о том, как выбрать приоритетный интерес при их столкновении? Весьма ярко это вопрос иллюстрирует проведенное в сети Интернет исследование. На одном из интернет-сайтов пользователям предложено выбрать вариант поведения в различных ситуациях управления гипотетическим автомобилем, когда дорожная ситуация предполагает неизбежный выбор, кем именно придется пожертвовать водителю — собой, пассажиром, пешеходом, водителем и пассажирами встречного транспортного средства, если он выбирает жертвовать пешеходами, то кем именно. Кому отдать предпочтение, сохранив жизнь? Данный ресурс заявлен как имеющий целью формирование правильного ответа на вопрос выбора для «обучения» программы беспилотного транспортного средства, управляемого искусственным интеллектом. Представляется, что данный выбор основан на этических и нравственных приоритетах, весьма серьезно различающихся по популяции и вряд ли «среднее арифметическое» в ответах популяции действительно станет самым этически безупречным вариантом. Каким стандартом морали и нравственности должен руководствоваться искусственный интеллект, если помнить о том, что мораль, представления о добре, нравственном — часть внутреннего чувства человека, впитанного им с молоком матери через колыбельные песни и народный дух, воплощенный в них. Представляется, что программа искусственного интеллекта не может иметь чувства добра и справедливости, а только расчет выгоды.

Представляется, что это этическое противоречие в настоящее время гораздо более серьезно, чем сложности с правосубъектностью клона человека.

В процессе собственного исследования автор настоящей работы проводил опрос о том, допустимо ли использование технологии искусственного интеллекта до решения этических проблем, связанных с его неспособностью формировать решение на основе представлений

о добре и справедливости. По мнению ¾ опрошенных, использование технологии искусственного интеллекта требует предварительного решения этических проблем. С другой стороны, 1/8 опрошенных полагает, что технологический прогресс нельзя остановить, а поэтому следует использовать технологии искусственного интеллекта, не дожидаясь ответа на все этические вопросы. Остальные опрошенные затруднились ответить на вопрос.

Весьма тесно связан с предыдущим этическим императивом следующий принцип, названный в Концепции и состоящий в ***запрете на причинение вреда человеку по инициативе систем искусственного интеллекта*** и робототехники (по общему правилу следует ограничивать разработку, оборот и применение систем искусственного интеллекта и робототехники, способных по своей инициативе целенаправленно причинять вред человеку). Главный вопрос, который возникает в процессе реализации этого принципа, это вопрос о том, что такое «вред». Ведь классическое понимание вреда как неблагоприятных изменений в имущественной или неимущественной сфере потерпевшего[8], таким образом, любое умаление имущественной или неимущественной сферы лица является вредом. Однако существуют ситуации обоснованного умаления имущественной сферы лица, например, если причинение повреждения позволяет предотвратить больший вред. Так, если у товара истекает срок годности, то продажа такого товара по цене ниже себестоимости будет оправданным действием. Для человека доступным выбором является причинение вреда в состоянии необходимой обороны или крайней необходимости, в том числе речь может идти о причинении вреда здоровью, если это позволяет предотвратить более тяжелое увечье или смерть. Причинение вреда имуществу для предотвращения вреда жизни и здоровью вообще является разумным выбором. Значит ли это, что технологии искусственного интеллекта априори не могут жертвовать меньшим ради спасения более ценного? Если так, то использование таких технологий заведомо не соответствует базовому условию о способности принимать решения, сходные с решениями человека.

Получается, что для использования технологии искусственного интеллекта кто-то должен оценить по некой шкале разные блага, «объяснив» системе, чем можно жертвовать, в чем нет, и когда именно причинение вреда является разумным выбором. Вопрос о том, как это можно сделать и где найти шкалу сравнения ценностей? То, что человек решает интуитивно, не всегда возможно описать в виде алгоритма. Одним из отличий человека от машины является его способность к творчеству, это базовое отличие человека дает ему возможность, во-первых, создавать нормы, во-вторых, принимать решение о неактуальности существующей нормы и принимать решение об их нарушении или отмене. Все это недоступно машине. В отсутствие способности к творчеству, созданию и нарушению правил искусственный интеллект не может являться альтернативой человеческому мышлению.

Много внимания уделяется в документах идее обеспечения подконтрольности технологии искусственного интеллекта человеку. Однако о недостижимости в полной мере данной цели знают и сами разработчики, которые замечают, что подконтрольность возможна лишь «с учетом требуемой степени автономности систем искусственного интеллекта и робототехники и иных обстоятельств». По всей видимости, нужно более реалистично оценивать данную технологию и ее принципиальную непрозрачность, что вкупе с сомнительными этическими стандартами программиста-разработчика делает использование технологии искусственного интеллекта на сегодняшний день весьма сомнительным.

Очень много вопросов вызывает следующий этический принцип, отраженный в Концепции, согласно которому проектируемая технология искусственного интеллекта должна

[8] См.: Болтанова, Е. С., Кратенко, М. В. (2022). *Деликтное право: учебное пособие*. Юстицинформ.

соответствовать закону, в том числе требованиям безопасности (применение систем искусственного интеллекта не должно заведомо для разработчика приводить к нарушению правовых норм). Как ранее было отмечено, способность к созданию и нарушению норм, вытекающая из способности человека к творчеству, составляет основу человеческого мышления, без них искусственный интеллект нельзя считать подобным человеческому. Ограничивая возможность нарушать, с одной стороны, разработчики стремятся обеспечить охрану прав и законных интересов людей, но с другой — лишают технологию искусственного интеллекта принципиальной возможности формировать решения, сходные с решениями человека. В том же принципе вызывает вопросы также указание на «заведомость» для разработчика — кажется, здесь смешиваются принципы функционирования искусственного интеллекта и стандарт ответственности разработчика за причиненные искусственным интеллектом вред. Дополнительные вопросы вызывает и то, что этот стандарт исходя из буквального толкования приведенного положения понижен до вины в форме умысла, а также то, что далее из документа не усматривается, каковы последствия нарушения разработчиком данного этического принципа.

Последним в перечне этическим принципов, отраженных в Концепции, стоит запрет противоправной манипуляции поведением человека. Остается неясным, о чем идет речь в данном случае. Например, любая технология контекстной рекламы предполагает анализ поведения пользователей сети Интернет и формирование предложений исходя из проявленных интересов лица. Можно ли назвать такую рекламу манипулированием поведением или нет?

Технологии искусственного интеллекта существенно упрощают задачи приемки товаров, поскольку в отличие от человека, машина может быстро и точно провести сплошную проверку товара по количеству, качеству и ассортименту, выявить и зафиксировать отступления от условий договора (заданных параметров). Технологии искусственного интеллекта уже внедрены в исполнение обязанностей хранителя по складскому хранению, позволяя отслеживать состояние товара (поклажи) и менять условия хранения (температуру, влажность и пр.) в зависимости от состояния товара на складе. Существенно изменилась технология заключения и исполнения договоров страхования с внедрением технологий искусственного интеллекта, поскольку с одновременным использованием технологии Больших данных искусственный интеллект может точнее оценить вероятность наступления страхового случая и оценить ущерб, если страховой случай наступил.

В литературе встречаются радикальные подходы, согласно которым искусственный интеллект должен признаваться субъектом права, наделяться правами и обязанностями, признаваться законом «электронным лицом». Предполагается создание специальных государственных публичных реестров электронных лиц, где должны указываться объем правоспособности и пределы ответственности таких лиц в зависимости от функционала (Kartskhiya, 2019). Представляется, что это — тупиковый путь. В настоящее время уже существует искусственно созданный субъект права — юридическое лицо. Эта конструкция вполне пригодна для ее использования в самых разных областях, она уже состоит в наделении правосубъектностью некоего искусственного образования, основанного на имущественном или личном объединении, общем труде и пр. Нет никакой необходимости конструировать дополнительных субъектов права, вполне можно достичь указанных целей путем адаптации существующих организационно-правовых форм к использованию технологий искусственного интеллекта.

При современном уровне развития технологии искусственного интеллекта это не более чем техническое решение, позволяющее оптимизировать рутинные процессы и тем самым снижающее трансакционные издержки, риски ненадлежащего исполнения обязательств, риски

порчи товара и пр. Поскольку сама эта технология в значительной степени непрозрачна, самообучаемость — одновременно «плюс» и «минус» этой технологии, которая вкупе с отсутствием внятных правил решения проблемы этического выбора приводит к потенциальной вредоносности такой технологии и неполной контролируемости человеком, то наиболее адекватным способом минимизации рисков для окружающих является признание использования искусственного интеллекта деятельностью, представляющей повышенную опасность для окружающих. Распространение режима источника повышенной опасности на технологии искусственного интеллекта позволяют обеспечить баланс между возможностью использовать искусственный интеллект в коммерческой деятельности и извлекать из нее преимущества и необходимостью обеспечить права и законные интересы окружающих.

В коммерческих договорах использования технологии искусственного интеллекта позволяет оптимизировать складское хранение путем подбора наиболее оптимальных условий хранения и исключить действие человеческого фактора, а значит и человеческих ошибок. С помощью искусственного интеллекта может осуществляться анализ и заказ товаров исходя из тенденции изменения спроса, зависящего от совокупности как факторов окружающей среды, так и публикаций в СМИ, влияющих на формирование представлений населения о моде и пр. Искусственный интеллект существенно упрощает работу колл-центров, предоставляя ответы на вопросы покупателей, сортируя обращения и делая обратную связь доступнее для покупателей и дешевле для коммерсанта. Внедрение искусственного интеллекта на стадии исполнения обязательства позволяет оптимизировать процесс документирования приемки товаров, в том числе путем сплошной проверки вместо «ручной» выборочной, составления актов и товарных накладных, фиксировать нарушения договора, оформлять приемку на ответственное хранение и направлять претензии поставщикам (по качеству и ассортименту товаров) и покупателям (по оплате), оптимизировать перевозку и страхование товаров и пр. Огромные возможности внедрения технологии искусственного интеллекта в коммерческую деятельность создают иллюзию безграничности этих возможностей, но это не так. Человек – как единственный творец, способный создавать нормы и принимать решение о их нарушении, не может полностью быть заменен искусственным интеллектом. Нелинейные и нестандартные задачи требуют творчества в их решении. Заключение коммерческого договора — весьма сложная деятельность, имеющая коммерческий договор как результат юридического творчества, оформляющий согласованную волю сторон, не может быть полностью передана на откуп искусственного интеллекта. В процессе заключения договора стороны устанавливают социальное взаимодействие, могут проверить добросовестность контрагента в том числе по результатам оценки невербальных сигналов, интуитивно считываемых в процессе общения: склонность к сотрудничеству, порядочность, ответственность, уровень правосознания и пр. Как отмечается в юридической литературе, одной из функций договора является определение и юридическое фиксирование общей цели участников договора. Отмечают, что согласование, формулирование совместной цели и ее юридическое закрепление вносит общий смысл во взаимоотношениях договорных контрагентов, создает единую направленность и упорядоченность их усилий (Puginskiy, 2008). Р.О. Халфина писала об этом: «Соглашение участников договора направлено на достижение определенного результата. Права и обязанности, принимаемые каждой из сторон, как правило, различны, но они взаимно согласованы и в совокупности дают единый результат» (Khalfina, 1975). Какой именно правовой и хозяйственный результат желают получить стороны, определяется человеком, поэтому роль искусственного интеллекта в процессе заключения договора не может полностью вытеснить человека и его волю.

Заключение

Подводя итоги, можно отметить, что информационные технологии отлично вписываются в традиционное коммерческое право и не требуют создания особых отраслей права. Для обеспечения надлежащей защиты прав всех участников коммерческих отношений при использовании информационных технологий достаточно точечных изменений, определяющих правовой режим отдельных технологий и последствий их использования.

Исходя из сущности информационных технологий, полностью коммерческий оборот не может быть переведен в «виртуальную плоскость», это связано с тем, что реальные товары перевозятся по земле транспортными средствами, хранятся на товарных складах при определенном температурном режиме, продаются потребителям для потребления, все эти «реальные» элементы цепочки движения товаров требуют участия живых людей с волей и способностью своей человеческой преобразовательной активностью менять окружающую среду.

Условия допустимости использования информационных технологий предполагают внедрение ограничений, призванных защитить базовые ценности (естественные права человека) от технологического вмешательства. Наибольшие риски возникают для сферы частной жизни, личной и семейной тайны. Несмотря на то что адекватных путей регулирования использования информационных технологий пока не создано, нет оснований для установления запрета на использование таких технологий (как это произошло, например, с технологиями в области клонирования человека). Запрет как метод регулирования фактически выводит явление из правового поля, помещая в серую зону, где угроз и рисков для прав и законных интересов граждан неизмеримо больше. В связи с этим стоило бы провести комплексное социолого-правовое исследование влияния информационных технологий на различные сферы человеческого общежития, в том числе и на область коммерческих договоров.

Список литературы / References

1. Begishev, I. R., & Khisamova, Z. I. (2018). Kriminologicheskiye riski primeneniya iskusstvennogo intellekta [Criminological risks of using artificial intelligence]. *Russian Journal of Criminology*, *12*(6), 767–775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775.
2. Churilov, A. Y. (2021). *Pravovoye regulirovaniye primeneniya tekhnologii blockchain* [Legal regulation of the use of blockchain technology]. Yustitsinform.
3. Filippova, S. Y. (2013). *Instrumental'nyy podkhod v nauke chastnogo prava* [Instrumental approach in the science of private law]. Statute.
4. Filippova, S. Y. (2017a). Funktsii nauki grazhdanskogo prava [Functions of the civil law science]. *Pravovedenie*, *61*(4), 102–136. https://pravovedenie.spbu.ru/article/view/6789
5. Filippova, S. Y. (2017b). *Tsivilisticheskaya nauka Rossii: Stanovleniye, funktsii, metodologiya* [Civil science of Russia: Formation, functions, methodology]. Statute.
6. Kaplan, A. & Haenlein, M. (2018). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004
7. Kartskhiya, A. A. (2019). Tsifrovaya transformatsiya prava [Digital transformation of law]. *Monitoring pravoprimeneniya*, (1), 26–27. https://doi.org/10.21681/2226-0692-2019-1-25-29
8. Khalfina, R. O. (1975). *Pravo i khozraschet* [Law and cost accounting]. Yuridicheskaya Literature.

9. Korovnikova, N. A. (2021). Iskusstvennyy intellekt v obrazovatel'nom prostranstve: Problemy i perspektivy [Artificial intelligence in the educational space: Problems and prospects]. *Sotsial'nyye Novatsii i Sotsial'nyye Nauki*, (2), 98–113. https://doi.org/10.31249/snsn/2021.02.07, 10.31249/snss/2021.02.08
10. Laptev, V. A., & Tarasenko, O. A. (Eds.). (2020). *Tsifrovaya ekonomika: Kontseptual'nyye osnovy pravovogo regulirovaniya biznesa v Rossii* [Digital economy: Conceptual foundations of legal regulation of business in Russia]. Prospekt.
11. Lapteva, A. M. (2019). Pravovoy rezhim tsifrovykh aktivov (na primere Big Data) [Legal regime of the digital assets (on Example Big Data)]. *Zhurnal Rossiyskogo Prava*, (4), 93–104. https://doi.org/10.12737/art_2019_4_8
12. Puginskiy, B. I. (2008). *Teoriya i praktika dogovornogo regulirovaniya* [Theory and practice of contractual regulation]. IKD «Zertsalo M».
13. Puginskiy, B. I. (2013). *Kommercheskoye pravo Rossii* [Commercial law of Russia]. IKD «Zertsalo M».
14. Sannikova, L. V. (2019). Blokcheyn v korporativnom upravlenii: Problemy i perspektivy [Blockchain in corporate governance: Challenges and opportunities]. *Pravo i Ekonomika*, 4(374), 27–36.
15. Sannikova, L. V., & Kharitonova, Y. S. (2020). *Tsifrovyye aktivy: Pravovoy analiz* [Digital assets: Legal analysis]. 4 Print.
16. Savelyev, A. I. (2016). Dogovornoye pravo 2.0: "Umnyye" kontrakty kak nachalo kontsa klassicheskogo dogovornogo prava [Contract law 2.0: Smart contracts as the beginning of the end of classical contract law]. *Vestnik Grazhdanskogo Prava*, *16*(3), 32–60.
17. Savelyev, A. I. (2017). Nekotoryye pravovyye aspekty ispol'zovaniya smart-kontraktov blokcheyn-tekhnologiy po rossiyskomu pravu [Some legal aspects of implementation of Smart contracts and blockchain technologies under Russian law]. *Zakon*, (5), 94–117.
18. Savelyev, A. I. (2018). Napravleniya regulirovaniya bol'shikh dannykh i zashchita neprikosnovennosti chastnoy zhizni v novykh ekonomicheskikh realiyakh [Directions of regulation of Big Data and protection of privacy in the new economic realities]. *Zakon*, (5), 122–144.
19. Szabo, N. (1997). Formalizing and securing relationships on public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548
20. Turing, A. (1950). Computing machinery and intelligence. *Mind, New Series*, *59*(236), 433–460.
21. Uvarov, A. A., & Uvarov, A. A. (2020). Problemy ispol'zovaniya tsifrovykh tekhnologiy pri realizatsii prav i svobod grazhdan [Problems of the use of digital technologies in enforcement of the citizens rights and freedoms]. *Law and Digital Economy*, *2*(08), 5–11. https://doi.org/10.17803/2618-8198.2020.08.2.005-011
22. Zaynutdinova, E. V. (2020). Smart-kontrakt: Vozniknoveniye i razvitiye v grazhdanskom prave [Smart contract: The origination and development in civil law]. *Predprinimatel'skoye Pravo*, (3), 25–32.

Сведения об авторе:

Филиппова С. Ю. — доктор юридических наук, доцент, доцент кафедры коммерческого права и основ правоведения юридического факультета Московского государственного университета имени М.В. Ломоносова, Москва, Россия.
filippovasy@yandex.ru

Information about the author:

Sofia Y. Filippova — Dr. Sci. in Law, Associate Professor, Department of Commercial and Fundamentals of Jurisprudence, Faculty of Law, Lomonosov Moscow State University, Moscow, Russia.
filippovasy@yandex.ru

https://doi.org/10.38044/2686-9136-2022-3-3-79-96

СТАТЬИ

ЭВОЛЮЦИЯ АНТИМОНОПОЛЬНОГО РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ПЛАТФОРМ

А.А. Арутюнян[1,*], А.Д. Бербенева[2]

[1]Московский государственный университет имени М.В. Ломоносова
119991, Россия, Москва, Ленинские горы, 1

[2]Адвокатское Бюро «Егоров, Пугинский, Афанасьев и партнеры»
125047, Россия, Москва, ул. 1-я Тверская-Ямская, 21

Аннотация

Статья посвящена комплексному анализу развития подходов к антимонопольному регулированию экономической деятельности участников цифровых рынков, так называемых «цифровых платформ». Бизнес-практики цифровых платформ и их соответствие требованиям антимонопольного законодательства к настоящему моменту довольно широко исследованы и регуляторами различных стран, и экспертным сообществом. Однако еще несколько лет назад такой степени погружения в эти вопросы не было ни в науке, ни в практике. Сегодня, когда опыт регулирования цифровых рынков уже накоплен в достаточной степени, в различных правопорядках стали появляться нормативные акты, регламентирующие подходы к оценке рыночного положения цифровых платформ, а также допустимых и недопустимых практик, стали формироваться механизмы контроля, специфичные для цифровых рынков и направленные на предотвращение антимонопольных нарушений. В то же время скорость развития цифровых технологий слишком велика. Это неизбежно будет ставить новые задачи перед регуляторами и наукой: будут появляться новые цифровые услуги, новые бизнес-модели и новые варианты расширения рынков, например посредством развития экосистемных продуктов. В работе представлен анализ основных этапов развития антимонопольного регулирования цифровых рынков: с момента первых дел о нарушении антимонопольного законодательства IT-компаниями до разработки специальных механизмов регулирования и контроля цифровых платформ, а также дана оценка потенциальному развитию самих цифровых рынков и их антимонопольного регулирования как в России, так и за рубежом. Работа содержит обзор нормативных актов и иных регуляторных инициатив в области цифровых рынков в различных регионах мира, а также отсылки к ключевым антимонопольным делам в отношении цифровых компаний, которые повлияли на формирование регуляторных подходов.

Ключевые слова

цифровые рынки, цифровые платформы, антимонопольное регулирование, экосистемы

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.

Для цитирования Арутюнян, А. А., Бербенева, А. Д. (2022). Эволюция антимонопольного регулирования цифровых платформ. *Цифровое право, 3*(3), 79–96. https://doi.org/10.38044/2686-9136-2022-3-3-79-96

* Автор, ответственный за переписку

Поступила: 30.04.2022, принята в печать: 22.07.2022, опубликована: 30.09.2022

ARTICLES

THE EVOLUTION OF ANTIMONOPOLY REGULATION OF DIGITAL PLATFORMS

Anna A. Arutyunyan[1,*], Anastasia D. Berbeneva[2]

[1]Lomonosov Moscow State University
1, Leninskie Gory, Moscow, Russia, 119991

[2]Egorov Puginsky Afanasiev & Partners
21, 1st Tverskaya-Yamskaya str., Moscow, Russia, 125047

Abstract

This paper provides comprehensive analysis of the evolution of approaches to antimonopoly regulation of digital market participants, the so-called "digital platforms". So far business practices of digital platforms and their compliance with the antitrust rules have been widely studied by both the watchdogs of various countries and the expert community. However, a few years ago the research into these issues was not that thorough neither in science nor in practice Today, with sufficient experience on regulation of digital markets, legal acts are being drawn up in various jurisdictions that cover approaches to assessing the market position of digital platforms, as well as acceptable and unacceptable practices. Besides, specific control mechanisms are being designed to deter antitrust violations in digital markets. At the same time, digital technologies are evolving too fast. This will inevitably pose new challenges to regulators and science. New digital services, business models and options for expanding markets, for example, by developing ecosystem products, will appear. The paper presents analysis of the main stages in the development of antimonopoly regulation of digital markets: from the first antitrust cases against IT-companies to creation of special regulatory and control mechanisms of digital platforms. Furthermore, potential development of digital markets and their antitrust regulation both in Russia and abroad is considered. The paper offers review of legal acts and regulatory initiatives in the area of digital markets in different regions worldwide and refers to the key antitrust cases that have affected the regulatory approaches.

Keywords

digital markets, digital platforms, antimonopoly regulation, ecosystems

Conflict of interest The authors declare no conflict of interest.

Financial disclosure The study had no sponsorship.

For citation Arutyunyan, A. A., & Berbeneva, A. D. (2022). The evolution of antimonopoly regulation of digital platforms. *Digital Law Journal*, *3*(3), 79–96. https://doi.org/10.38044/2686-9136-2022-3-3-79-96

* Corresponding author

Submitted: 30 Apr. 2022, accepted: 22 Jul. 2022, published: 30 Sep. 2022

Введение

Стремительное развитие Интернета и информационных технологий привело к формированию новых общественных отношений и возникновению новых — цифровых — рынков. Основными участниками таких рынков стали так называемые цифровые платформы. Данное понятие является экономическим по своей сути и раскрывает сущностно новую бизнес-модель, которая стала распространяться на разных рынках — платформенную, при которой хозяйствующий субъект, разработчик (и правообладатель), создает онлайн-сервис (сайт, приложение для мобильного устройства и иное подобное программное обеспечение), выступающий в качестве платформы для совершения сделок между продавцами и покупателями товаров (работ, услуг) или осуществления доступа к какому-либо контенту, размещаемому либо самим владельцем платформы, либо пользователями платформы. Данная бизнес-модель в классической версии предполагает посредническую роль платформы, но нередко можно встретить ситуации, когда владелец платформы одновременно становится и ее участником наряду с независимыми участниками платформы.

Легального определения понятия цифровой платформы российским законодательством не предусмотрено, однако в одном из недавних документов ФАС России, а именно в Принципах взаимодействия участников цифровых рынков, утвержденных Протоколом заседания Экспертного совета при ФАС России по развитию конкуренции в области информационных технологий 22 сентября 2021 г., указано, что сами Принципы распространяются на *цифровые платформы, обеспечивающие опосредованное (через платформу) или прямое взаимодействие различных групп пользователей, помимо самой платформы, включая, но не ограничиваясь агрегаторами товаров, работ, услуг, поисковыми системами, сайтами объявлений, рекламными системами, операционными системами, магазинами приложений, социальными сетями.*

Европейский регулятор (Европейская комиссия) в 2015 году в ходе публичных обсуждений антимонопольного регулирования цифровых рынков предложил следующее определение онлайн-платформы: компания, работающая на двусторонних (или многосторонних) рынках, использующая Интернет для обеспечения взаимодействия между двумя или более отдельными, но взаимозависимыми группами пользователей, чтобы создать ценность по крайней мере для одной из групп[1]. Впоследствии в проекте общеевропейского нормативного акта, посвященного регулированию цифровых рынков, — Digital Markets Act[2] — Еврокомиссия определила перечень ключевых платформ (*core platforms*), деятельность которых имеет большое

[1] House of Lords. Select Committee on European Union. (2016, April 20). *Online platforms and the digital single market*. The European Union Committee. https://www.europarl.europa.eu/doceo/document/A-8-2017-0204_EN.html

[2] European Commission. (n.d.). Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). Document 52020PC0842. EUR-Lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

значение для обеспечения конкуренции на цифровых рынках. К их числу Еврокомиссия отнесла провайдеров посреднических онлайн-услуг (например, маркетплейсы, магазины приложений для операционных систем, агрегаторы такси и т. п.); поисковые системы; социальные сети; платформы видеошеринга; коммуникационные сервисы; операционные системы; облачные сервисы и рекламные сервисы, включая рекламные сети и иные посреднические платформы для размещения рекламы, предоставляемые владельцами вышеупомянутых ключевых платформ.

Данная бизнес-модель стала очень востребованной именно на цифровых рынках, т. к. их особенность состоит в создании инновационных технологий, повышающих эффективность взаимодействия участников оборота, а также в создании дополнительной ценности для пользователей. То, на что раньше могли потребоваться значительные временные и финансовые ресурсы, стало доступно «на расстоянии одного клика».

Разумеется, конкуренция в области технологичных рынков не могла остаться вне поля зрения антимонопольных регуляторов. Однако время показало, что реакция регуляторов не всегда была своевременна и эффективна. Специфика сетевых эффектов, существенно влияющих на конкуренцию на цифровых рынках, такова, что, однажды завоевав популярность и став востребованной, та или иная платформа может приобрести такую рыночную власть и устойчивое положение на рынке, что потенциальным конкурентам преодолеть барьеры входа на этот рынок будет непросто даже при очень высоком уровне финансовых и иных вложений.

С учетом указанного представляется интересным проследить и проанализировать этапы развития антимонопольного регулирования цифровых рынков на примере России и иных юрисдикций, в рамках которых были выработаны соответствующие механизмы регулирования, включая США, Европейский союз, реализующий свою наднациональную антимонопольную политику через Еврокомиссию, отдельные европейские государства, национальное регулирование которых оказало влияние в том числе на развитие общеевропейских подходов, а также отдельные страны БРИКС, которые также большое внимание уделяют антимонопольному регулированию в интересующей области.

Этапы развития антимонопольного регулирования цифровых платформ

Первый этап — накопление эмпирического опыта оценки бизнес-практик технологических компаний

Первые значимые шаги в вопросах анализа и оценки практик цифровых компаний на предмет их антиконкурентного характера были предприняты в США. Так, в 1994 году Министерство юстиции США подало первый иск против Microsoft, обвинив компанию, в том числе, в незаконном поддержании монополии на рынке операционных систем путем включения неконкурентных условий в лицензионные соглашения и соглашения с разработчиками программного обеспечения. Это дело так и не было рассмотрено по существу, так как стороны пришли к мировому соглашению[3]. Однако уже в 2000 году по решению Окружного суда США округа Колумбия действия Microsoft по связыванию операционной системы Windows и браузера были признаны нарушением Закона Шермана. Это дело положило начало серии расследований в отношении технологических компаний по поводу довольно распространенной практики связывания (*tying*). Понятная с экономической точки зрения и широко применяемая

[3] *United States v. Microsoft Corp.*, 56 F.3d 1448 (D.C.Cir. 1995).

на традиционных рынках практика связывания стала очень актуальной на цифровых рынках. Связывание как одна из форм злоупотребления доминирующим положением предполагает использование товара, на рынке которого субъект занимает доминирующее положение в качестве локомотива для продвижения других товаров. Такая связка товаров (например, предоставление владельцем операционной системы прав на ее использование производителям аппаратных устройств только при условии предустановки на такие устройства браузера, разработанного владельцем операционной системы) позволяет ускорить экспансию на смежных рынках и обеспечить определенное конкурентное преимущество за счет того товара, на рынке которого уже установлено доминирование. В описываемом деле Microsoft правоприменитель столкнулся именно с этой практикой, которую впоследствии мы увидим еще неоднократно в антимонопольных делах против других компаний. Примечательно, что решением суда по делу Microsoft была предусмотрена довольно редкая, структурная, мера воздействия — разделение Microsoft на две компании с целью разграничения направлений разработки операционной системы и программных продуктов[4]. Однако суд апелляционной инстанции не согласился с некоторыми выводами окружного суда и направил дело на новое рассмотрение[5]. При этом суд справедливо обратил внимание на динамичный характер цифровых рынков, в связи с чем за период с момента, когда компания предположительно совершила первое антиконкурентное действие, и до вынесения решения условия на рынке могли измениться, что значительно затрудняет рассмотрение таких дел[6]. В результате судебное разбирательство завершилось мировым соглашением, по которому Microsoft обязался делиться интерфейсом программирования приложений (API) с третьими лицами, тем самым обеспечив бóльшую совместимость собственных систем с продуктами конкурентов.

Практически одновременно с рассмотрением дела в США деятельность Microsoft стала предметом рассмотрения в Европейской комиссии. Производитель программного и аппаратного обеспечения Sun Microsystems обратился в европейский антимонопольный регулятор с жалобой на отказ Microsoft предоставлять информацию об интерфейсе, необходимую для разработки продукции конкурентов. Решением 2004 года было установлено злоупотребление Microsoft доминирующим положением, что выразилось в намеренном ограничении совместимости Windows с серверами сторонних производителей[7]. Еврокомиссия обязала Microsoft раскрывать конкурентам соответствующую информацию для производства совместимых продуктов, а также устранить связывание Windows Media Player с ОС Windows.

С 2010-х годов под пристальным вниманием европейского регулятора оказался и другой цифровой гигант — Google, на ограничительные практики которого постоянно поступали жалобы как в Еврокомиссию, так и в национальные антимонопольные ведомства государств — членов ЕС. В 2017 году в решении Еврокомиссии по делу Google Shopping было установлено, что Google, используя свое доминирующее положение на рынке поисковых систем, продвигал собственный сервис сравнения цен на товары Google Shopping. Google отображал собственный сервис на первых (то есть более выгодных) строках поисковой выдачи, занижая позиции конкурирующих сервисов, что лишало их возможности конкурировать с Google на равных. Одним из последствий таких действий Google явилось ограничение европейских потребителей

[4] *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30 (D.D.C. 2000).

[5] *United States v. Microsoft Corp.*, 253 F.3d 34 (D.C. Cir. 2001).

[6] *United States v. Microsoft Corp.*, 253 F.3d 34 at 49 (D.C. Cir. 2001).

[7] *Commission decision of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty* (Case COMP/C-3/37.792 Microsoft).

в получении доступа к наиболее подходящим им сервисам сравнения покупок и, соответственно, в возможностях выбора.

В данном деле Европейская комиссия выработала подход к практике, которую можно обозначить как *self-preferencing* (предоставление преимуществ собственным продуктам). Google как доминант на рынке поисковых систем использовал свою платформу поиска для преимущественного продвижения собственного сервиса по сравнению цен за счет применения специальных неорганических (т. е. сгенерированных не в соответствии с общими правилами ранжирования) элементов поисковой выдачи (технология OneBox). Данная практика оказалась также широко распространенной на цифровых рынках и спустя несколько лет была рассмотрена и российским регулятором в рамках дела о «колдунщиках» Яндекса.

В деле Google Shopping Еврокомиссия столкнулась с необходимостью использовать и адаптировать классические антимонопольные инструменты применительно к нарушению на цифровом рынке. В результате решение Еврокомиссии подверглось значительной критике, в том числе потому что вынесенное Google предписание оказалось неэффективным.

Следует отметить, что расследование Еврокомиссии продлилось почти 10 лет с момента обращения первого потерпевшего с жалобой. За время рассмотрения дела многие онлайн-сервисы — конкуренты Google, которые были в числе заявителей жалоб, не выдержав агрессивной конкуренции, были вынуждены покинуть рынок. Но даже и после вынесения решения и выдачи предписания Google ситуация на рынке кардинально не поменялась, т. к. предписанные Google меры по обеспечению конкуренции оказались неэффективными, что подробно рассмотрено в исследовании Томаса Хоппнера[8].

Еврокомиссия обязала Google самостоятельно определить, каким образом необходимо изменить технологии поиска, чтобы обеспечить всем конкурентам равную представленность в поисковой системе. Меры, которые предпринял Google, оказались недостаточными для восстановления конкуренции, поскольку за время реализации соответствующей практики сервисы Google значительно укрепились на рынке. Несмотря на то, что Google формально исполнил предписание, это не привело к повышению трафика конкурентов и, соответственно, эффективному восстановлению конкуренции[9].

Помимо этого дела Еврокомиссией в отношении Google были рассмотрены еще два (дела Google Android и Google Ads). По каждому из них Google был оштрафован на значительные суммы. Например, по делу Google Android[10], связанному со злоупотреблением доминирующим положением на рынке операционных систем, Еврокомиссия наложила на Google беспрецедентный на тот момент штраф в размере 4,34 млрд евро[11]. Однако эффективность таких штрафов вызывает обоснованные сомнения, поскольку они не способны повлиять на состояние конкуренции и для глобальных интернет-компаний хоть и являются значительными, но все же не создают серьезных стимулов для отказа от антиконкурентных действий в будущем (Höppner, 2022).

---

[8] Höppner, T. (2020, November 24). *Google's (non-) compliance with the EU shopping decision*. Competition Policy International. https://www.competitionpolicyinternational.com/googles-non-compliance-with-the-eu-shopping-decision/

[9] Chee, F. Y., & Waldersee, V. (2019, November 7). *EU's Vestager says Google's antitrust proposal not helping shopping rivals.* Reuters. https://www.reuters.com/article/us-eu-alphabet-antitrust-idUSKBN1XH2I8

[10] *Commission decision of 18.7.2018 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (the Treaty) and Article 54 of the EEA Agreement* (Case AT.40099 — Google Android)..

[11] При этом выручка материнской компании Alphabet в 2018 году составила 136,82 млрд долларов. https://abc.xyz/investor/static/pdf/20180204_alphabet_10K.pdf?cache=11336e3

Накопленный в ходе рассмотрения данных дел опыт позволил осознать, что классические антимонопольные инструменты, носящие зачастую ретроспективный, последующий характер (*ex-post*) не являются в полной мере достаточными для своевременного выявления и устранения антимонопольных рисков на цифровых рынках. Более эффективным в условиях быстро меняющихся цифровых реалий является предупредительный, *ex ante* контроль, переход к которому выразился в разработке ранее упомянутого Акта о цифровых рынках. Данный акт содержит ряд превентивных механизмов, среди которых, например, обязанность крупных цифровых компаний воздерживаться от предоставления преимуществ собственным продуктам (*self-preferencing*) — практика, подробно рассмотренная Еврокомиссией в деле Google Shopping.

На уровне государств — членов Европейского союза также имели место громкие антимонопольные расследования в отношении цифровых компаний. Например, в Германии предметом антимонопольного разбирательства являлись правила Facebook, позволявшие компании собирать с разных ресурсов (включая сторонние) большие массивы персональных данных пользователей. Дело вызвало активную дискуссию, в том числе в правовом сообществе (Kerber, Zolna, 2022), и завершилось решением Федерального верховного суда Германии, подтвердившим, что такая практика навязывания сбора данных составляет злоупотребление доминирующим положением[12]. Данное дело внесло значительный вклад как в развитие национального законодательства Германии, так и в разработку Акта о цифровых рынках, в котором был предусмотрен запрет на объединение персональных данных, собираемых на ключевой платформе IT-гигантов, с данными остальных платформ, включая сторонние. Подробнее содержание Акта о цифровых рынках раскрывается в следующем разделе.

В правоприменительной практике США в течение 20 лет после дела Microsoft отсутствовали громкие дела по привлечению цифровых компаний к ответственности за нарушение антимонопольного законодательства. Представляется, что это преимущественно связано со стремлением американских властей поддержать свои национальные технологические компании, в том числе на международных рынках. Такая политика в целом принесла свои результаты и привела к тому, что на глобальном уровне данные компании стали более чем успешны. В то же время совершенно очевидно, что и в самих США эти компании монополизировали соответствующие рынки, поскольку получили значительную свободу действий на начальных этапах развития. В конечном счете это привело к необходимости проведения масштабного расследования в Конгрессе по вопросу об антиконкурентных практиках цифровых гигантов — Alphabet (Google), Amazon, Facebook (Meta)[13] и Apple. Составленный по итогам расследования и четырехчасовых слушаний в Конгрессе США доклад содержал многочисленные примеры недопустимых действий указанных компаний и выводы о необходимости изменения антимонопольного законодательства[14].

Проведенное парламентское расследование стало триггером для многочисленных антимонопольных исков в отношении перечисленных компаний со стороны американских регуляторов. Например, в августе 2021 года Федеральная торговая комиссия США подала повторный (первоначальный иск Комиссии был отклонен судом как недостаточно аргументированный)

---

12 Bundesgerichtshof Beschluss KVR 69/19 vom 23. Juni 2020.

13 Здесь и далее Компания Meta Platforms Inc. признана в России экстремистской организацией и запрещена.

14 Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary. (2020). *Investigation of Competition in Digital Markets.* https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519

иск против Facebook, в котором утверждается, что монопольное положение компании на рынке личных социальных сетей во многом получено за счет неправомерного приобретения Instagram и WhatsApp. В январе 2022 года окружной судья США Джеймс Боасберг отклонил ходатайство Facebook о прекращении дела, тем самым постановив, что рассмотрение спора будет продолжено[15].

Между тем, многие иски к цифровым компаниям отклоняются как недостаточно аргументированные. Так, в марте 2022 года суд округа Колумбия отклонил иск против Amazon, в котором компания обвинялась в нарушении антимонопольного законодательства путем запрета продавать товары на сторонних платформах на более выгодных условиях, нежели на Amazon[16].

Федеральная антимонопольная служба России за последние пять лет также рассмотрела ряд прецедентных цифровых кейсов, среди которых следует отметить решения в отношении Google, HeadHunter, Booking, Apple, «Яндекса» и др. Так, в 2019 году действия ООО «Хэдхантер» по блокировке использования стороннего сервиса по автоматизированному подбору персонала на собственном сайте hh.ru (притом что компания предлагала пользователям собственный сервис с похожим функционалом) были признаны нарушением п. 9 ч. 1 ст. 10 Закона о защите конкуренции[17] (злоупотребление доминирующим положением в виде создания препятствий доступу на товарный рынок)[18].

Правомерность включения оговорки о паритете цен в договоры между Booking.com и отелями была предметом рассмотрения как ФАС России, так и регуляторов ряда европейских стран таких как Франция, Германия, Швеция, Италия. Данная оговорка обязывает отели предлагать на Booking.com номера на таких же или более выгодных условиях, чем на других онлайн- и офлайн-площадках (широкая оговорка о паритете цен) или на собственном веб-сайте отеля (узкая оговорка о паритете цен).

Решением ФАС России от 29 декабря 2020 г.[19] действия компании Booking.com B.V. были признаны нарушением п. 3 ч. 1 ст. 10 Закона о защите конкуренции путем навязывания средствам размещения невыгодных условий взаимодействия с Booking.com в части необходимости обязательного предоставления и соблюдения паритета цен, наличия номеров и условий во всех каналах продаж (распространения) гостиничных услуг. Компании было предписано прекратить требовать соблюдение паритета цен. Впоследствии компания была оштрафована на внушительную сумму (более 1 млрд руб.).

Антиконкурентные практики российского IT-гиганта «Яндекса» также были предметом рассмотрения ФАС России. В 2020 году ряд цифровых сервисов (Avito, Циан, 2ГИС, Туту.ру и пр.) обратились в ФАС России с жалобой на злоупотребление доминирующим положением ООО «Яндекс» на рынке поиска в Интернете путем возможного антиконкурентного продвижения сервисов «Яндекса» (таких как «Яндекс.Маркет», «Яндекс.Недвижимость», «Яндекс. Путешествия») в его поисковой системе. Предметом рассмотрения являлись интерактивные виджеты «Яндекса» — так называемые «колдунщики», которые позволяли визуально выделять сервисы «Яндекса» на странице результатов поиска, тем самым уводя трафик конкурентов и замещая и подменяя реальный выбор пользователя. В результате спор завершился

[15] *FTC v. Facebook, Inc.,* D.D.C. https://www.documentcloud.org/documents/21177063-memorandum-opinion

[16] Binoy, R., & Mallard, W. (Ed.). (2022, March 21). *U.S. court dismisses D.C. antitrust lawsuit against Amazon.* Reuters. https://www.reuters.com/business/retail-consumer/us-court-dismisses-dc-antitrust-lawsuit-against-amazon-2022-03-19/

[17] Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции». Российская газета, № 162, 27.07.2006.

[18] Решение ФАС России №АГ/4087/20 по делу № 11/01/10-9/2019 от 23.01.2020.

[19] Решение ФАС России №АД/115711-ДСП/20 по делу № 11/01/10-41/2019 от 29.12.2020.

подписанием мирового соглашения между «Яндексом», IT-коалицией и ФАС России в январе 2022 года, согласно которому «Яндекс» разработал Политику партнерской интеграции со своей поисковой системой, что должно позволить сервисам конкурентов наравне с сервисами «Яндекса» конкурировать за места на странице результатов поиска.

Примеры подобных дел, которые были рассмотрены ФАС России, можно продолжать. Однако важно то, что российский антимонопольный орган был в числе первых, кто начал активно исследовать цифровые рынки и применять наиболее передовые подходы к регулированию на них.

Следует отметить, что активное правоприменение по аналогичным вопросам за эти годы имело место и в других юрисдикциях, в том числе в Китае, для которого также характерна высокая степень концентрации на цифровых рынках, в Бразилии, Индии, на уровне государств — членов ЕС и т. д.

Например, в ноябре 2021 года китайский регулятор оштрафовал таких крупных цифровых игроков, как Alibaba, Tencent и Baidu на 3,4 млн долларов за непредоставление информации о совершении ряда сделок в 2012–2021 годах[20]. Также в 2021 году было установлено, что на протяжении нескольких лет компания Alibaba злоупотребляла доминирующим положением, что выразилось в установлении условий, согласно которым продавцам, реализующим товары на Alibaba, было запрещено использовать конкурирующие платформы[21].

Анализ этой практики позволяет в какой-то степени выделить основные формы нарушения антимонопольных запретов цифровыми платформами, к которым можно отнести:

- связывание, т. е. использование доминирующей платформы для продвижения товаров на смежных рынках;
- дискриминацию или установление преимущественных условий для собственных сервисов (товаров, работ, услуг) на собственной платформе по сравнению с сервисами конкурентов;
- получение преимуществ за счет эксклюзивного доступа к массиву пользовательских данных;
- создание технологических решений, исключающих совместимость программных решений с разными платформами, упразднение мультихоуминга, т. е. замыкание пользователя на своей платформе;
- ценовой паритет (т. е. запрет на установление продавцами более низких цен на конкурирующих платформах);
- антиконкурентное поглощение компаний.

Второй этап — разработка нормативных правил конкуренции на цифровых рынках

Безусловно, описанные выше практики не исчерпывают все поведенческое многообразие цифровых платформ. Однако в определенный момент накопленный опыт продемонстрировал острую необходимость уточнения законодательства в области защиты конкуренции и нормативного регулирования деятельности платформ, развитие которых приводит к появлению новых и ранее не исследованных видов антиконкурентного поведения.

Более того, стало понятно, что назрела необходимость модернизации антимонопольных подходов при рассмотрении дел о нарушениях на цифровых рынках. Например, одним

[20] Reuters. (2021, November 20). *China fines tech giants for failing to report 43 old deals.* https://www.reuters.com/technology/china-finds-43-anti-trust-law-violations-involving-alibaba-baidu-jdcom-2021-11-20/

[21] Reuters. (2021, November 10). *China fines Alibaba record $2.75 bln for anti-monopoly violations.* https://www.reuters.com/business/retail-consumer/china-regulators-fine-alibaba-275-bln-anti-monopoly-violations-2021-04-10/

из важных элементов антимонопольного регулирования является анализ состояния конкуренции на рынке, без которого фактически невозможно ни одно антимонопольное расследование. Однако ранее сформулированные правила анализа рынка оказались малопригодны для анализа цифровых рынков. Например, традиционный «тест гипотетического монополиста», который оценивает изменение спроса на товар при изменении цены и с помощью которого определяются продуктовые границы рынка, практически неприменим в своем классическом виде к цифровым рынкам, поскольку многие услуги онлайн-платформ предлагаются формально на безвозмездной основе (де-факто потребители «платят» своими данными и вниманием, а монетизация деятельности платформы осуществляется либо по комиссионной модели, либо по рекламной модели). В качестве альтернативы предлагается оценивать изменение спроса на цифровую услугу в случае ухудшения качества предоставляемых услуг (SSNIQ или SSNDQ-тест), но его применение сопряжено с вопросом, как измерять качество цифровых услуг (Gal, Rubinfeld, 2016). Например, в рамках данного теста может оцениваться поведение пользователей в случае изменения производительности платформы или объема собираемых персональных данных. Кроме того, измерение качества услуг может быть весьма субъективным и требовать доступа к большому объему информации (Patakyová, 2020).

По нашему мнению, при оценке продуктовых границ рынка важно учитывать, что является объектом конкурентных отношений: за какие блага конкурируют разные участники рынка (за количество пользователей, за их рекламодателей, за количество кликов или транзакций, совершенных на платформе, и т. д.). Представляется, что создать унифицированный критерий или показатель для оценки границ рынка в отношении цифровых платформ невозможно и, напротив, было бы даже вредно, поскольку исключило бы гибкий подход к рынкам, которые находятся в состоянии перманентной эволюции, в отличие от традиционных товарных рынков, которые, как правило, значительно более стабильны в плане своих характеристик.

Эти и другие вопросы, связанные с особенностями подходов к цифровым рынкам, возникают повсеместно и регулярно.

Кроме того, специфика цифровых рынков предполагает, что рыночная власть интернет-компаний во многом зависит от сетевых эффектов, накопленных баз пользовательских данных, исключительных прав на результаты интеллектуальной деятельности, обладание которыми иногда рассматривается как «легальная монополия».

В связи с этим в последние годы регуляторы во многих юрисдикциях, помимо непосредственно расследования нарушений на цифровых рынках, стали уделять большое внимание разработке нормативного регулирования, призванного установить специальные правила для цифровых платформ и упростить антимонопольный анализ на цифровых рынках.

Так, например, с середины 2010-х годов Европейская комиссия совместно с иными институтами Европейского союза ведет работу над адаптацией правовой базы к реалиям цифровой экономики. В 2019 году был принят Регламент 2019/1150 о содействии справедливости и прозрачности для бизнес-пользователей услуг онлайн-посредничества[22], направленный на развитие конкурентной и справедливой цифровой бизнес-среды. Регламент возлагает на поисковые системы и онлайн-посредников (магазины приложений, онлайн-сервисы социальных сетей) ряд обязанностей по взаимодействию с бизнес-пользователями, то есть лицами, предлагающими свои товары и услуги через онлайн-посредников. В частности, условия

[22] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150

использования онлайн-посредников должны быть составлены простым и понятным языком, должны быть легко доступны бизнес-пользователям для ознакомления, а также должны закреплять основания для ограничения, приостановления или прекращения предоставления услуг бизнес-пользователям.

Кроме того, Регламент содержит обязанность онлайн-посредников и поисковых систем сделать общедоступным описание основных параметров ранжирования. Актуальность введения данной обязанности наглядно иллюстрирует выше рассмотренный кейс Google Shopping, в котором было установлено, что недобросовестное поведение Google стало во многом возможным в связи с непрозрачной работой алгоритмов ранжирования.

В настоящий момент в Европейском союзе активно разрабатываются два прогрессивных законопроекта — упомянутый выше Акт о цифровых рынках и Акт о цифровых услугах[23]. Акт о цифровых рынках вводит понятие «гейткиперов» (*англ*. gatekeepers, дословно «привратник», «сторож»), то есть компаний, занимающих особое место на цифровых рынках и отвечающих установленным количественным и качественным критериям. «Гейткипером» может быть признан тот участник рынка, который:

а) имеет значительное влияние на внутренний рынок;

б) владеет ключевой платформой, которая обеспечивает важную точку доступа для взаимодействия профессиональных пользователей (бизнес-пользователей) с конечными пользователями;

в) имеет долгосрочное устойчивое положение на рынке, или есть основания полагать, что такое положение будет установлено в ближайшем будущем.

При этом критерий значительного влияния на внутренний рынок оценивается на основании следующих пороговых значений по годовой выручке в Европейской экономической зоне за последние три финансовых года или по средней рыночной капитализации или эквивалентной справедливой рыночной стоимости компании за последний финансовый год. При этом компания должна оказывать услуги не менее чем в трех государствах — членах ЕС.

Ключевой характер платформы (критерий б) определяется по количеству пользователей: ключевая платформа предоставляет услуги не менее чем 45 миллионам активных конечных пользователей в месяц (*monthly active users*) и более чем 10 тысячам активных профессиональных пользователей в год за последний финансовый год.

Устойчивое положение на рынке определяется тем, как долго платформа является ключевой с учетом показателей количества пользователей. Если платформа удовлетворяет критериям ключевой (т. е. имеет соответствующее количество пользователей) в течение последних трех финансовых лет, ее положение оценивается как устойчивое.

На «гейткиперов» в целях обеспечения конкуренции и предотвращения нарушений возлагаются такие дополнительные обязательства, как запрет приоритизации собственных сервисов; запрет объединения пользовательских данных, собранных на разных сервисах «гейткипера»; запрет ограничения возможностей пользователей переключаться на сторонние сервисы; обеспечение большей совместимости конкурирующих продуктов и т. д. При этом проектом Акта о цифровых рынках предусмотрено право Еврокомиссии в исключительных случаях полностью или частично приостанавливать действие конкретного обязательства, если компания обоснует, что соблюдение такого обязательства поставит под угрозу саму экономическую целесообразность ее деятельности, или если его соблюдение не отвечает важнейшим общественным

[23] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN

интересам. Кроме того, Акт вводит обязанность «гейткипера» уведомлять Комиссию о любых планируемых сделках на цифровых рынках, вне зависимости от их размеров.

В свою очередь, Акт о цифровых услугах направлен на борьбу с незаконным и вредоносным контентом, обеспечение безопасности пользователей, транспарентности платформ. В начале июля 2022 года оба данных акта были приняты Европейским парламентом в первом чтении. Затем акты должны быть одобрены Советом ЕС, опубликованы, и ожидается, что осенью 2022 года они вступят в силу.

Похожий на общеевропейский подход избран и в Великобритании, где рассматриваются предложения по введению нового «проконкурентного» режима на цифровых рынках и усилению контроля за сделками экономической концентрации на цифровых рынках. В частности, в апреле 2021 года в рамках Управления по конкуренции и рынкам Великобритании (CMA) был создан специальный орган по осуществлению контроля за крупными цифровыми компаниями — Отдел цифровых рынков (DMU), к компетенции которого будет относиться мониторинг и обеспечение соблюдения нового «проконкурентного» режима. Данный режим предусматривает введение теста стратегического статуса на рынке (*Strategic Market Status*), которому будут отвечать компании, обладающие существенной и укоренившейся рыночной властью по крайней мере в одном виде деятельности, для которого цифровые технологии являются ключевым компонентом[24]. Для оценки стратегического положения интернет-компании предлагается учитывать не только размер и масштаб ее деятельности, но и оценивать, является ли она важной точкой доступа («шлюзом») ко множеству других предприятий, может ли ее деятельность позволить укрепить свою рыночную власть или распространить ее на другие виды деятельности, может ли компания диктовать «правила игры» пользователям экосистемы. В США разрабатывается пакет законопроектов, направленных на снижение рыночной власти BigTech, на ослабление их доминирования, среди которых особое внимание следует уделить:

- Закону об инновациях и выборе в Интернете[25], который запрещает приоритизацию собственных сервисов и другое дискриминационное поведение технологических гигантов.
- Закону о конкуренции и возможностях платформ[26], направленному на сдерживание дальнейшего расширения IT-гигантов путем поглощения конкурентов.
- Закону о прекращении монополизма платформ[27], предусматривающему ограничение интернет-гигантов во владении и управлении сервисами, создающими «конфликт интересов».
- Закону о повышении уровня совместимости и конкуренции путем смены провайдеров или Закону о доступе[28], упрощающему перенос данных с одной платформы на другую посредством повышения требований к совместимости данных.
- Закону об открытых рынках приложений[29], направленному на деконцентрацию дуополии магазинов приложений Apple и Google.

Проекты законов об инновациях и выборе в Интернете и об открытых рынках приложений в январе — феврале 2022 года были одобрены Юридическим комитетом Сената США. При этом

---

[24] Secretary of State for Digital, Culture, Media & Sport, Secretary of State for Business, Energy and Industrial Strategy. (2021). A new pro-competition regime for digital markets. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003913/Digital_Competition_Consultation_v2.pdf

[25] H.R.3816 — American Choice and Innovation Online Act.

[26] H.R.3826 — Platform Competition and Opportunity Act of 2021.

[27] H.R.3825 — Ending Platform Monopolies Act.

[28] H.R.3849 — ACCESS Act of 2021.

[29] S.2710 — Open App Markets Act.

их разработка сопровождается активными дискуссиями и подвергается значительной критике со стороны бизнес-сообщества как подрывающих конфиденциальность и безопасность оказания цифровых услуг, и, соответственно, приводящих к ущемлению прав пользователей[30]. Кроме того, законопроекты отличаются расплывчатыми и широкими формулировками, что может негативно сказаться на качестве предоставляемых услуг и снизить стимулы к инновациям.

Идея возложения дополнительных обязанностей на крупнейшие цифровые платформы поддерживается и другими зарубежными регуляторами. В частности, проект Руководства по обязанностям интернет-платформ, разработанный в 2021 году в Китае, предполагает введение обязательств не использовать непубличные данные (полученные во время использования платформы) без уважительных причин; не связывать использование одного сервиса с другими; исключить приоритизацию собственных сервисов; способствовать совместимости собственного сервиса и сервисов конкурентов[31]. Соответственно, можно сделать вывод, что в целом содержание таких дополнительных обязательств в различных юрисдикциях схоже.

В России работа по корректировке нормативного регулирования также ведется. «Пятый антимонопольный пакет», посвященный преимущественно регулированию цифровых рынков, был разработан еще в 2018 году[32] и на тот момент являлся одним из первых документов в мире, закрепляющим изменение антимонопольных подходов к цифровым рынкам на законодательном уровне. Он предусматривал введение нормативного определения цифровой платформы и сетевых эффектов, новых критериев доминирующего положения на цифровых рынках, ужесточение контроля за сделками экономической концентрации. Однако его рассмотрение затянулось, встретив критику государственных органов и участников рынка. Эта критика была связана с различными причинами, но отдельно стоит отметить, что позиция участников рынка разделилась в том числе в связи с тем, что предлагаемое регулирование распространялось только на транзакционные платформы (на которых совершаются сделки по приобретению товаров, работ, услуг) и не распространялась на платформы социальных сетей, поисковых сервисов. Однако на данный момент разногласия относительно содержания «пятого антимонопольного пакета» удалось преодолеть и законопроект был поддержан Правительством РФ и 7 июля 2022 года внесен в Государственную Думу РФ[33].

Законопроектом предлагается дополнить Закон о защите конкуренции понятием «сетевые эффекты», установить особенности проведения анализа состояния конкуренции на цифровых рынках. Предусматривается введение новой статьи — 10^1, которая закрепляет запрет монополистической деятельности платформами, на которых осуществляются сделки между продавцами и покупателями (например, маркетплейсы, агрегаторы). Такие запреты распространяются на платформы, отвечающие следующим критериям: платформа в силу

---

30 Rodrigo, C. M. (2022, April 12). *Tim Cook cautions against antitrust legislation*. The Hill. https://thehill.com/policy/technology/3265186-tim-cook-cautions-against-antitrust-legislation/

31 Brown, I., & Korff, D. (2021, November 1). *Data protection and digital competition*. https://www.ianbrown.tech/2021/11/01/chinas-new-platform-guidelines/

32 Проект Федерального закона «О внесении изменений в Федеральный закон “О защите конкуренции”» и иные законодательные акты Российской Федерации», 2018. https://regulation.gov.ru/projects#npa=79428

33 Проект Федерального закона № 160280-8 «О внесении изменений в Федеральный закон “О защите конкуренции”», 2022. https://sozd.duma.gov.ru/bill/160280-8

сетевых эффектов имеет возможность оказывать решающее влияние на общие условия обращения товара на цифровом рынке; доля сделок на данной платформе превышает 35 % от общего объема в стоимостном выражении сделок, совершаемых на соответствующем товарном рынке; выручка платформы превышает 2 млрд рублей. Кроме того, условия контроля сделок экономической концентрации дополняются новым основанием — если цена сделки превышает 7 млрд рублей, что также призвано способствовать усилению антимонопольного контроля над цифровыми платформами. Законопроект включен в примерную программу осенней сессии Государственной Думы РФ.

Если принятие «пятого антимонопольного пакета» несколько затянулось, то принятие принципов саморегулирования цифровых рынков не заставило себя ждать. Летом 2021 года Федеральная антимонопольная служба России разработала проект базовых принципов взаимодействия участников цифровых рынков, к которым относятся[34]:

- разумная открытость цифровых платформ;
- нейтральность отношения к различным сторонам рынка (включая конкурентов);
- обеспечение самостоятельности пользователей платформ при взаимодействии с ней;
- недопущение расширительных и двусмысленных формулировок в правилах работы цифровых платформ;
- обеспечение прав пользователей платформы, в том числе путем рассмотрения их обращений и предоставление им полных ответов;
- саморегулирование онлайн-платформ.

В феврале 2022 года ФАС России подписала меморандум с IT-компаниями («Яндекс», «Циан», «Авито») о присоединении к данным принципам[35], что является важным шагом к «мягкому» превентивному управлению антимонопольными рисками на цифровых рынках и подтверждает готовность участников рынка следовать принципам конкуренции.

При этом в антимонопольное законодательство некоторых стран уже введены дополнительные инструменты, направленные на регулирование поведения цифровых компаний. Например, в антимонопольном законе Германии закреплено, что при оценке положения субъекта на многосторонних рынках должны приниматься во внимание сетевые эффекты, использование нескольких услуг одновременно и издержки переключения между ними, экономия от масштаба в связи с сетевыми эффектами, доступ к данным, влияние инноваций на конкуренцию (ст. 3a раздела 18 Закона)[36].

В Китае в настоящий момент рассматриваются поправки в антимонопольный закон, среди которых предлагается закрепить новый вид злоупотребления — необоснованное ограничение деятельности хозяйствующих субъектов посредством данных, алгоритмов, технологий и правил цифровой платформы[37].

---

[34] Федеральная антимонопольная служба России. (2021, август 18). *Экспертный совет при ФАС России озвучил проект базовых принципов взаимодействия участников цифровых рынков.* https://fas.gov.ru/news/31434

[35] Селиванова, А. (2022, февраль 17). *ФАС подписала с IT-компаниями меморандум о принципах работы на цифровых рынках.* Российская газета. https://rg.ru/2022/02/17/fas-podpisala-s-it-kompaniiami-memorandum-o-principah-raboty-na-cifrovyh-rynkah.html

[36] Act against Restraints of Competition. Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245.

[37] Zhou, F., & Cao, V. (2021, November 3). *China publishes latest draft amendments to anti-monopoly law: Highlights and implications.* Linklaters. https://www.linklaters.com/ru-ru/knowledge/publications/alerts-newsletters-and-guides/2021/november/03/china-publishes-latest-draft-amendments-to-anti-monopoly-law-highlights-and-implications

В рамках Евразийского экономического союза также предлагается выработать дополнительные антимонопольные инструменты в отношении онлайн-платформ[38]: определить специальные критерии доминирующего положения на цифровых рынках и виды злоупотреблений таким положением. Кроме того, в праве ЕАЭС планируется определить процедуру и порядок проведения оценки состояния конкуренции на трансграничных и цифровых рынках[39].

Будущее цифровых рынков

Если с предыдущими этапами развития регулирования цифровых рынков все более или менее понятно, то вот будущее цифровой среды пока не определено. В то же время в экономике наметилась отчетливая тенденция, которая очевидно влияет и на правовое регулирование цифровых рынков, и на практику антимонопольного правоприменения. Она выражается в переходе от платформенной модели экономики к экосистемной.

Проблематика цифровых экосистем сегодня находится на острие науки, практики и нормотворческой работы. Одной из ключевых проблем в правовом регулировании цифровых экосистем является проблема недопущения монополизации рынка экосистемами, поскольку такая угроза является вполне реальной и ощутимой.

Следует признать, что на данный момент единого и точного подхода к определению понятия экосистемы еще не выработано. С точки зрения своего технологического содержания под цифровой экосистемой можно понимать цифровую среду, состоящую из онлайн-сервисов и прочих программных продуктов, взаимодополняющих друг друга, построенных по принципу взаимной интеграции и предполагающих предоставление пользователю широкого спектра услуг «из единого окна» без необходимости переключения на других поставщиков таких услуг или ввода дополнительных данных для доступа к тому или иному сервису. С экономической точки зрения цифровую экосистему можно рассматривать как своеобразную бизнес-модель, направленную на расширение перечня реализуемых товаров и услуг для удовлетворения большего числа потребностей клиентов экосистемы[40]. Близкое определение экосистемы предложено и в докладе ЦБ РФ «Регулирование рисков участия банков в экосистемах и вложений в иммобилизованные активы», в котором под экосистемой понимается построенная на основе данных о клиентах совокупность сервисов, в том числе платформенных решений, позволяющих пользователям в рамках единого процесса получать широкий спектр продуктов и услуг[41].

Гораздо сложнее определить экосистему с правовой точки зрения, поскольку организационно экосистема, как правило, выражается в формировании многопрофильного холдинга, объединяющего компании, осуществляющие разные виды деятельности, подчиняющиеся зачастую разным правовым режимам и регуляторным требованиям (например, «Яндекс», в группу

---

38 Евразийская экономическая комиссия. (2021). *Обзор «Конкурентное (антимонопольное) регулирование на цифровых рынках»*. http://www.eurasiancommission.org/ru/act/caa/cpol/konkurentpol/Documents/Обзор.pdf

39 Евразийская экономическая комиссия. (2021, июль 14). *В право ЕАЭС внесут изменения по оценке состояния конкуренции на цифровых рынках.* https://eec.eaeunion.org/news/v-pravo-eaes-vnesut-izmeneniya-po-otsenke-sostoyaniya-konkurentsii-na-tsifrovyh-rynkah-/

40 Похожий подход к определению экосистемы предложен и в Концепции государственного регулирования цифровых платформ и экосистем, разработанной Министерством экономического развития России. https://economy.gov.ru/material/departments/d31/koncepciya_gos_regulirovaniya_cifrovyh_platform_i_ekosistem/

41 Банк России. (2021, июнь). *Регулирование рисков участия банков в экосистемах и вложений в иммобилизованные активы.* https://cbr.ru/Content/Document/File/123688/Consultation_Paper_23062021.pdf

которого входят различные компании, осуществляющие разработку и управление различными сервисами «Яндекса»).

По нашему мнению, как с технической, так и с экономической точек зрения нельзя отождествлять экосистему с простой совокупностью онлайн-сервисов. Разработчик, который выпустил несколько мобильных приложений, дающих доступ к нескольких разным сервисам, или разработчик, который создал одно приложение, объединяющее в себе несколько функций, еще не является владельцем экосистемы. В некотором смысле можно сказать, что экосистема — это понятие не количественное, а качественное, хотя, безусловно, фактор количества тоже должен учитываться.

История развития экосистем указывает, что в основе экосистемы всегда лежит какая-то ключевая платформа, вокруг которой происходит формирование дополнительных сервисов. Например, экосистема Google формировалась вокруг поисковой системы Google, а затем — на основе операционной системы Android, благодаря которой Google удалось стать разработчиком одной из наиболее востребованных в мире экосистем на базе мобильных устройств. В качестве такой ключевой может выступать и платформа для получения финансовых услуг. Именно поэтому создателями экосистем в основном становятся либо крупные интернет-компании, имеющие в своем распоряжении поисковые системы, операционные системы и подобные ключевые платформы, либо крупные финансовые учреждения. Примечателен в этом смысле опыт «Сбера», которому за короткий срок удалось создать действительно значимую экосистему цифровых продуктов под собственным брендом за счет своего ключевого сервиса — банковского — и коллаборации с крупными IT-компаниями, обладающими необходимым технологическим опытом.

Появление экосистем и тяготение крупных игроков рынка к экосистемной модели предполагает, в свою очередь, решение вопроса о том, каким образом должна быть обеспечена конкуренция на рынках, на которых представлены экосистемы, должны ли для экосистем быть предусмотрены специальные ограничения, которые обеспечили бы равную конкурентную среду для экосистем и независимых участников рынка с учетом определенного рыночного преимущества первых перед вторыми.

Так, в частности, важной целью регулирования может стать недопущение искусственного «закрытия» экосистем, при котором сторонние поставщики цифровых услуг не имеют возможности продвигать свои товары и услуги на платформах крупных интернет-компаний. Частично данная цель может быть достигнута за счет закрепления принципа недискриминационного доступа к платформам, управляемым крупными экосистемами, а также повышения прозрачности условий функционирования таких платформ, например за счет раскрытия принципов ранжирования платформ в той степени, в которой это позволит удостовериться в корректности работы алгоритмов платформы.

Рассуждая о дополнительных способах сдерживания антиконкурентного потенциала экосистем, можно назвать несколько возможных механизмов, которые могут быть использованы для этих целей: от наиболее радикальных (например, законодательное ограничение допустимой рыночной доли для отдельных видов платформ) до менее радикальных (например, изменение пороговых значений для согласования сделок на цифровых рынках в целях усиления превентивного контроля над монополизацией рынка). Также полезной мерой могло бы стать внедрение «обеспечительных предварительных мер» по делам о нарушении антимонопольного законодательства на цифровых рынках (например, в виде требования приостановить те или иные практики до вынесения решения), поскольку на таких рынках в течение

срока рассмотрения дела могут произойти стремительные и кардинальные изменения, которые сведут на нет принятые регулятором меры.

Не будучи сторонниками радикальных и жестких регуляторных мер, особенно на цифровых рынках, полагаем в то же время, что потребность расширить контроль за экономической концентрацией на цифровых рынках назрела уже давно. Текущая практика показывает, что многие совершенные ранее сделки, в том числе по приобретению небольших, но перспективных стартапов в среднесрочной перспективе привели к усилению рыночного положения крупных онлайн-платформ за счет объединения функционала и пользовательских данных. При этом в силу существующих регуляторных порогов такие сделки не были предметом рассмотрения антимонопольных органов. Как показало исследование Федеральной торговой комиссии США, за период с начала 2010 по конец 2019 года пять крупнейших цифровых компаний — Alphabet, Amazon, Apple, Facebook и Microsoft — совершили 616 сделок, не подлежащих согласованию с регулятором[42]. В результате многие потенциальные конкуренты были устранены, а позиции лидеров рынка были дополнительно усилены.

Заключение

Таким образом, очевидно, что в настоящий момент на законодательном и правоприменительном уровне необходимо сконцентрировать усилия на создании конкурентной среды в условиях развития цифровых экосистем, на формировании новых подходов к оценке влияния экосистем на рынок. Нельзя игнорировать то обстоятельство, что динамика развития цифровых рынков многократно превышает скорость разработки подходящего регулирования, поэтому более перспективным представляется создание не правил как таковых, а инструментов, с помощью которых можно было бы оперативно и гибко реагировать на те или иные проблемы на рынке. Тем более, учитывая текущий экономический кризис в России, который беспрецедентен по своему характеру и масштабу, в силу чего жесткие меры регулирования могут стать препятствием для восстановления экономики и адаптации бизнеса к новым условиям в тех сферах, где речь не идет о жизненно необходимых благах и высококонцентрированных рынках, а, напротив, есть активная конкуренция, требующая поддержки и развития.

Список литературы / References

1. Gal, M., & Rubinfeld, D. L. (2016). The hidden costs of free goods: Implications for antitrust enforcement. *Antitrust Law Journal*, *80*(3), 521–562.
2. Kerber, W., & Zolna, K. K. (2022). The German Facebook case: The law and economics of the relationship between competition and data protection law. *European Journal of Law and Economics,* Article e09727-8. https://doi.org/10.1007/s10657-022-09727-8
3. Höppner, T. (2022). The European Google shopping competition saga, compliance and the rule of law. *15 Global Competition Litigation Review, 1/2022*, 8–20. http://doi.org/10.2139/ssrn.4029927
4. Patakyová, M. T. (2020). Competition law in digital era–how to define the relevant market? In *Economics & management: How to cope with disrupted times: Proceedings of the 4th international scientific conference EMAN* (pp. 171–177). https://doi.org/10.31410/EMAN.2020.171

[42] Federal Trade Commission. (2021, September 15). *FTC Staff Presents Report on Nearly a Decade of Unreported Acquisitions by the Biggest Technology Companies.* https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-staff-presents-report-nearly-decade-unreported-acquisitions-biggest-technology-companies

Сведения об авторах:

Арутюнян А. А.* — кандидат юридических наук, доцент юридического факультета МГУ имени М.В. Ломоносова; адвокат, советник антимонопольной практики Адвокатского Бюро «Егоров, Пугинский, Афанасьев и партнеры», Москва, Россия.
anna_arutyunyan@epam.ru

Бербенева А. Д. — магистр права, младший юрист антимонопольной практики Адвокатского Бюро «Егоров, Пугинский, Афанасьев и партнеры», Москва, Россия.
anastasia_berbeneva@epam.ru

Information about the authors:

Anna A. Arutyunyan* — Ph.D. in Law, Associate Professor, Faculty of Law, Lomonosov Moscow State University, Attorney, Counsel, Competition Law Practice, Egorov Puginsky Afanasiev & Partners, Moscow, Russia.
anna_arutyunyan@epam.ru

Anastasia D. Berbeneva — LL.M., Junior Associate, Competition Law Practice, Egorov Puginsky Afanasiev & Partners, Moscow, Russia.
anastasia_berbeneva@epam.ru