

DIGITAL LAW JOURNAL

Vol. 1, No. 4, 2020

ESSAY

- 8 Smart Contracts in the New Era of Contract Law
Alexandros Papantoniou

ARTICLES

- 25 FinTech & New Digital Instruments. Post-Crisis Developments: Russia and Europe
Anna Shashkova, Maria Agranovskaya, David Kitsmarishvili
- 38 The Evolution of Antitrust Regulation in Russia in Digital Era
Ksenia Tarkhova, Vladislav Alifrov, Olga Gorokhova
- 56 Personalized Law and Fundamental Rights
Tembot Misostishkhov
- 74 The Position of the Artificial Intelligence Among the Elements of the Legal Relationship
Anton Vasiliev, Yulia Pechatnova

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 1, No. 4, 2020

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 1, № 4, 2020



Contents

Essay

8 Smart Contracts in the New Era of Contract Law

Alexandros Papantoniou

Articles

25 FinTech & New Digital Instruments. Post-Crisis Developments: Russia and Europe

Anna Shashkova, Maria Agranovskaya, David Kitsmarishvili

38 The Evolution of Antitrust Regulation in Russia in Digital Era

Ksenia Tarkhova, Vladislav Alifirov, Olga Gorokhova

56 Personalized Law and Fundamental Rights

Tembot Misostishkhov

74 The Position of the Artificial Intelligence Among the Elements of the Legal Relationship

Anton Vasiliev, Yulia Pechatnova

Содержание

Эссе

- 8** Смарт-контракты как новая тенденция договорного права
Александрос Папантониу

Статьи

- 25** FinTech и новые цифровые средства. Посткризисное развитие: Россия и Европа
Анна Шашкова, Мария Аграновская, Давид Кицмаришвили
- 38** Эволюция антимонопольного регулирования в России в цифровую эпоху
Ксения Тархова, Владислав Алиферов, Ольга Горохова
- 56** Персонализированное право и фундаментальные права
Тембот Мисостишков
- 74** Место искусственного интеллекта среди элементов состава правоотношения
Антон Васильев, Юлия Печатнова

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 articles 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 12.00.00 and Economic Sciences 08.00.00 according to the HAC nomenclature.

The journal publishes articles in Russian and English.

FOUNDER, PUBLISHER:

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

EDITOR-IN-CHIEF:

Maxim Inozemtsev, Ph.D. in Law, Associate Professor, Department of Private International and Civil Law, Head of Dissertation Council Department of MGIMO-University, inozemtsev@digitallawjournal.org
76, ave. Vernadsky, Moscow, Russia, 119454

EDITORIAL BOARD

Marina Fedotova — Dr. Sci. in Economics, Head of the Department of Corporate Finance and Corporate Governance, Financial University under the Government of the Russian Federation, Moscow, Russia

Nikolaus Forgó — Dr. jur., Head of the Department of Innovation and Digitalisation in Law, University of Vienna, Vienna, Austria

Alice Guerra — Ph.D. in Law and Economics, Associate Professor, Department of Economics, University of Bologna, Bologna, Italy

Max Gutbrod — Dr. jur., Independent Scientist, Former Partner and Managing Partner of Baker McKenzie, Moscow, Russia

Steffen Hindelang — Ph.D. in Law, Department of Law, University of Southern Denmark (University of Siddan), Odense, Denmark

Junzo Iida — Ph.D., Department of Law, Soka University, Tokyo, Japan

Julia Kovalchuk — Dr. Sci. in Economics, Professor of the Department of Energy Service and Energy Supply Management, Moscow Aviation Institute, Moscow, Russia

Natalia Kozlova — Dr. Sci. in Law, Professor, Professor of the Department of Civil Law, Moscow State University Lomonosov, Moscow, Russia

Danijela Lalić — Ph.D. in Technical Sciences, Associate Professor, Faculty of Industrial Engineering and Management, Novi Sad University, Novi Sad, Serbia

Lyudmila Novoselova — Dr. Sci. in Law, Professor, Head of the Department of Intellectual Rights, Kutafin Moscow State Law University (MSAL), Moscow, Russia

Vladimir Osipov — Dr. Sci. in Economics, Ph.D. in Economics, Associate Professor, Professor of the Asset Management Department, Moscow State Institute of International Relations (MGIMO), Moscow, Russia

Francesco Parisi — Ph.D. in Law, Professor, Department of Law, University of Minnesota, Minneapolis, the USA

Vladimir Plotnikov — Dr. Sci. in Economics, Professor, St. Petersburg State University of Economics, St. Petersburg, Russia

Bo Qin — Ph.D., Professor, Head of the Department of urban planning and management, Renmin University of China, Beijing, China

Sergey Ryazantsev — Dr. Sci. in Economics, Corresponding Member of the Russian Academy of Sciences, Russian Academy of Sciences, Moscow, Russia

Elina Sidorenko — Dr. Sci. in Law, Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics, Director of the Center for Digital Economics and Financial Innovations, Moscow State Institute of International Relations (MGIMO), Moscow, Russia

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, digitallawjournal.org , dij@digitallawjournal.org
Published online:	20 Dec. 2020
Copyright:	© Digital Law Journal, 2020
Price:	Free

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 статьи 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 (криптовалюта, 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 экономики 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» 12.00.00 и «Экономические науки» 08.00.00 по номенклатуре ВАК.

В журнале публикуются статьи на русском и английском языках.

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

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

ГЛАВНЫЙ РЕДАКТОР:

Максим Иноземцев, кандидат юридических наук, доцент кафедры международного частного и гражданского права им. С. Н. Лебедева, начальник отдела диссертационных советов МГИМО МИД России, inozemtsev@digitallawjournal.org
119454, Россия, Москва, просп. Вернадского, 76

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Алиса Герра — Ph.D. in Law and Economics, доцент факультета экономики, Болонский университет, Болонья, Италия

Макс Гутброд — Dr. jur., независимый исследователь, бывший управляющий партнер международной юридической фирмы Baker McKenzie, Москва, Россия

Дзюндзо Иида — Ph.D., профессор факультета права, Университет Сока, Токио, Япония

Юлия Ковальчук — доктор экономических наук, профессор, профессор кафедры энергетического сервиса и управления энергоснабжением, Московский авиационный институт, Москва, Россия

Наталья Козлова — доктор юридических наук, профессор, профессор кафедры гражданского права, МГУ имени М.В. Ломоносова, Москва, Россия

Даниела Лалич — Ph.D. in Technical Sciences, доцент факультета промышленной инженерии и менеджмента, Нови-Садский университет, Нови-Сад, Сербия

Людмила Новоселова — доктор юридических наук, профессор, заведующий кафедрой интеллектуальных прав, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Москва, Россия

Владимир Осипов — доктор экономических наук, Ph.D. in Economics, профессор кафедры управления активами, МГИМО МИД России, Москва, Россия

Франческо Паризи — Ph.D. in Law, профессор факультета права, Миннесотский университет, Миннеаполис, США

Владимир Плотников — доктор экономических наук, профессор, профессор кафедры общей экономической теории и истории экономической мысли, Санкт-Петербургский государственный экономический университет, Санкт-Петербург, Россия

Сергей Рязанцев — доктор экономических наук, член-корреспондент РАН, Российская академия наук, Москва, Россия

Элина Сидоренко — доктор юридических наук, доцент, профессор кафедры уголовного права, уголовного процесса и криминалистики, директор Центра цифровой экономики и финансовых инноваций, МГИМО МИД России, Москва, Россия

Марина Федотова — доктор экономических наук, профессор, руководитель департамента корпоративных финансов и корпоративного управления, Финансовый университет при Правительстве Российской Федерации, Москва, Россия

Николаус Форго — Dr. jur., заведующий кафедрой инноваций и цифровизации в праве, Венский университет, Вена, Австрия

Штеффен Хинделанг — Ph.D. in Law, факультет права, Университет Южной Дании (Сидданский университет), Оденсе, Дания

Бо Цинь — Ph.D., профессор, заведующий кафедрой городского планирования и управления, Университет Жэньминь, Пекин, Китай

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:	20.12.2020
Копирайт:	© Цифровое право, 2020
Цена:	Свободная



ESSAYS

SMART CONTRACTS IN THE NEW ERA OF CONTRACT LAW

Alexandros A. Papantoniou

Papantoniou & Papantoniou LLC
41, Themistokli Dervi, Nicosia, Cyprus, 1066

Abstract

This essay examines whether smart contract innovation is capable of displacing the orthodox adherence to traditional contracts. This examination is underpinned by an analysis of the legality of smart contracts, through which it is exemplified that smart contracts ought to be considered legally binding instruments. The essay proceeds to explore the superiority of smart contracting on a technical and theoretical basis. The advantages generated through smart contract automaticity and enforceability present a concrete basis for undermining reliance on traditional contracts. Blockchain Technology also enhances the benefits of smart contracts by acting as a smart contract enabler through guaranteed performance and enforceability. Nevertheless, such novel technologies inevitably suffer from several shortcomings. This essay considers examples which illustrate the inflexibility of smart contracting. Apart from being susceptible to hacking and code exploitation, smart contracting is unable to deal with ambiguities and potential modifications. Overall, this suggests that the advantages of smart contract practice are currently confined to some specified limited scenarios. Smart contracts perform a different function to traditional contracting by merely guaranteeing technical enforceability as opposed to legal enforceability. This essay thus concludes that, for the time being, it is best to regard smart contracting as a supplement to traditional contracts rather than an outright displacement.

Keywords

smart contracts, blockchain, coding, artificial intelligence, automated legal instruments, decentralised autonomous organisations

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

London School of Economics and Political Sciences; Papantoniou & Papantoniou LLC.

For citation

Papantoniou, A. (2020). Smart contracts in the new era of contract law. *Digital Law Journal*, 1(4), 8–24. <https://doi.org/10.38044/2686-9136-2020-1-4-8-24>

Submitted: 16 Sep. 2020, accepted: 15 Nov. 2020, published: 20 Dec. 2020

СМАРТ-КОНТРАКТЫ КАК НОВАЯ ТЕНДЕНЦИЯ ДОГОВОРНОГО ПРАВА

А.А. Папантониу

Papantoniou & Papantoniou LLC
1066, Кипр, Никосия, Темистокли Дерви, 41

Аннотация

В эссе рассматриваются смарт-контракты как одно из оснований возникновения обязательств наряду с классическими договорами. Автоматическое исполнение с использованием технологии блокчейн как особенность конструкции является явным преимуществом по сравнению с традиционными договорными механизмами. В то же время такие новые технологии неизбежно имеют ряд недостатков. В эссе рассматриваются примеры, иллюстрирующие отсутствие гибкости смарт-контрактов. Кроме того, они подвержены взлому и эксплуатации кода и не могут справиться с двусмысленностями и потенциальными модификациями. Автор приходит к выводу о том, что в настоящее время новая популярная конструкция все же не может вытеснить классические договорные формы, а находит свое применение лишь в ограниченных сферах.

Ключевые слова

смарт-контракты, блокчейн, код, искусственный интеллект, автоматизированные правовые инструменты, децентрализованные автономные организации

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Лондонская школа экономики и политических наук; Papantoniou & Papantoniou LLC.

Для цитирования

Папантониу, А. (2020). Смарт-контракты как новая тенденция договорного права. *Цифровое право*, 1(4), 8–24. <https://doi.org/10.38044/2686-9136-2020-1-4-8-24>

Поступила: 16.09.2020, принята в печать: 15.11.2020, опубликована: 20.12.2020

The changes will never be as fast as some may predict, but changes there will be, and they will surely disrupt the way we are used to working.¹

Smart contracts are the tech topic du jour, having the ability to disrupt the practice of traditional contracting. Szabo envisioned smart contracts as a means to “combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols.”² More than twenty years later, Szabo’s vision remains the foundation for an array of literature, although no agreement has yet been reached on a coherent and consistent meaning to smart contracts which accurately reflects their current and potential functionality. This is mainly due to the advent of the blockchain network which transformed smart contracts into what they are today.³ Nevertheless, most academics and practitioners would agree that “a smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control.”⁴ This definition accurately encapsulates the essence of smart contracts, whilst being careful not to suggest anything beyond their existing capabilities.

Following this line of thought, this paper will start by analysing the legal status of smart contracts compared to traditional contracts. The view expressed in this work is that smart contracts constitute legally binding and enforceable contracts. This analysis will lead to a critical examination of whether the functionality of traditional contracts has been displaced by the emergence of smart contracts. It will be demonstrated that smart contracts have the potential to challenge the orthodox adherence to traditional contracting. Smart contracts’ automatic execution and self-enforceability offer both a practical and theoretical basis for this challenge. This paper will then explore how the emergence of the blockchain network has affected smart contracting and examine whether this offers the necessary qualities to displace the functionality of traditional contracts. It will be argued that although the blockchain network generates a multitude of advantages, it cannot significantly advance the practice of smart contracting given that it suffers from limitations itself. Subsequently, this paper will turn to consider the range of possible smart contract applications stemming from their versatility as legal instruments. The analysis will show that even though smart contracts show great potential, this has not yet been achieved. Smart contract technology is underdeveloped and the dependence on the code gives rise to systemic risks. Moreover, smart contracts represent an inflexible substitute to traditional contracts, and regarding the outstanding issues of contractual ambiguity, imperfect performance, and contractual modification, in addition, inadequate solutions have been proposed to address them. This discussion will highlight the overarching thesis of this paper: although, in theory, smart contracts appear to be functional legal instruments, they are currently limited in practice. Overall, this work regards smart contracts as currently supplementing traditional contract practice in limited scenarios, rather than displacing traditional functionality.

¹ Sir Vos, G. (2019, November 12). *Future proofing for commercial lawyers in an unpredictable world. Annual combar lecture 2019*. The Commercial Bar Association. www.judiciary.uk/wp-content/uploads/2019/11/COMBAR.lecture2019.final_.pdf

² Szabo, N. (1997). Smart contracts: Formalizing and securing relationships on public networks. *First Monday*, 2(9). Article 1. <https://doi.org/10.5210/fm.v2i9.548>

³ Koulou, R. (2016). Blockchains and online dispute resolution: Smart contracts as an alternative to enforcement. *Scripted. A Journal of Law, Technology & Society*, 13(1), 40–69. <http://doi.org/10.2966/scrip.130116.41>

⁴ Clack, C. D., Bakshi, V. A., & Braine, L. (2016). *Smart contract templates: Foundations, design landscape and research directions*. arXiv. <http://arxiv.org/abs/1608.00771>

The Legal Status of Smart Contracts

For an agreement to constitute an enforceable legally binding contract, common law requires four elements to be present, namely: (i) offer; (ii) acceptance; (iii) consideration and (iv) intentions to create legal relations. The law takes an exceptionally broad approach and will enforce any promise, whatever its form, if the above criteria are met and if there are no vitiating factors such as duress or misrepresentation to taint the agreement.⁵ In practical terms, a contract will be concluded upon the agreement of a future contractual performance, which then generates rights and obligations for all parties.⁶

A lingering question frequently tackled by literature is whether smart contracts carry the same legal validity as traditional contracts. Although this question warranted a definitive and authoritative answer, instead it instigated a never-ending debate amongst academics and practitioners. Some academics have strained every nerve to overestimate the power and authority of smart contracts. For example, Savelyev articulated the radical view that “smart contracts don’t need a legal system to exist: they may operate without any overarching legal framework. De facto, according to Savelyev, they represent a technological alternative to the whole legal system.”⁷ In contrast, practitioners voiced concerns about the legal status of smart contracts since, unlike traditional contracts, the contract is not given force through natural language but rather through computer data and rules.⁸ Although this concern is justifiable, this paper suggests that the prevalent view ought to be that smart contracts have the same legal validity as traditional contracts. This is because “the data-oriented label simply suggests that the parties have decided that some subset of key terms or conditions would benefit from being represented as computer processable data.”⁹ This argument is sensible, since “anything from a verbal agreement to an email conversation can become a contract at law, if the basic elements of a contract can be found.”¹⁰

The prevalent view rests on the premise that the function of a traditional contract is to alter the parties’ rights and obligations. Hence, smart contracts ought to be treated like other contracts, given that they operate themselves as voluntary mechanisms to alter the rights and duties of the parties.¹¹ The legal statement of the UK Jurisdiction Taskforce (hereinafter “UKJT”) reinforces this line of thought. The UKJT reasoned that smart contracts are capable of constituting legally binding contracts provided that the common law requirements for contract formation are satisfied.¹²

⁵ Jones, I. (2019, November 22). *Legal statement on cryptoassets and smart contracts – The breakdown*. Lexology. Collyer Bristow LLP. <https://www.lexology.com/library/detail.aspx?g=002956de-cd49-46ab-9218-f80a1cc92ad3#:~:text=The%20UK%20jurisdiction%20taskforce%20of,are%20enforceable%20by%20the%20courts>

⁶ Cutts, T. (2019). Smart contracts and consumers. *West Virginia Law Review*, 122(2), 389–446. <https://researchrepository.wvu.edu/wvlr/vol122/iss2/4>

⁷ Savelyev, A. (2017). Contract law 2.0: Smart contracts as the beginning of the end of classic contract law. *Information and Communications Technology Law*, 26(2), 116–134. <https://doi.org/10.1080/13600834.2017.1301036>

⁸ Harley, B. (2017, August 01). *Are smart contracts contracts? Talking Tech looks at the concept and realities of smart contract*. Talking Tech. <https://talkingtech.cliffordchance.com/en/emerging-technologies/smart-contracts/are-smart-contracts-contracts.html>

⁹ Surden, H. (2012). Computable contracts. *UC Davis Law Review*, 46(2), 629–700. https://lawreview.law.ucdavis.edu/issues/46/2/Articles/46-2_Surden.pdf

¹⁰ Stark, J. (2016, June 4). *Making sense of blockchain smart contracts*. CoinDesk. www.coindesk.com/making-sense-smart-contracts

¹¹ Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, 67(2), 313–382. <https://scholarship.law.duke.edu/dlj/vol67/iss2/2>

¹² Jones, 2019.

Sir Geoffrey Vos advocated that “a smart contract can be identified, interpreted and enforced using ordinary and well-established [common law] principles.”¹³ Disappointingly, however, the importance of this legal statement has been underestimated in relevant literature on the basis that it does not represent a statement of law. To fully comprehend the importance of the legal statement, it must be acknowledged that the UKJT is made up of highly respected practitioners, government experts, and members of the judiciary. In addition, the statement was heavily relied upon in the recent High Court decision of *AA v. Persons Unknown*.¹⁴ Mr. Justice Bryan acknowledged that the judicial members of UKJT “neither in their judicial capacity were responsible for the drafting of the legal statement, nor have either in their judicial capacities endorsed that legal statement.”¹⁵ Nonetheless, in delivering his judgment, he was greatly influenced by the conclusions of the legal statement. This shows that the statement may not in fact constitute legal authority, but it remains highly persuasive. In sum, in line with the UKJT and various academics, this work concludes that smart contracts are contracts on the basis that they represent “agreements to shift legal rights and responsibilities no less than an agreement between two parties physically exchanging goods for payment over a counter.”¹⁶

The legal validity of smart contracts entails a further layer of complexity which merits consideration: unless smart contracts become internationally recognised, they have the propensity to disturb the application of private international law.¹⁷ International legal systems require different elements for contract formation. A critical distinction, for example, is between civil and common law systems in which the latter requires consideration for a legally binding contract to be formed. Therefore, the validity of a smart contract hinges upon the jurisdiction’s willingness to recognise and enforce it. This represents a major impediment in smart contract practice given that they are placed on the blockchain network which in turn does not acknowledge international borders. Thus, the lack of an internationally co-ordinated effort to recognise the legality of smart contracts may prove to be challenging. It is not possible to predict the outcome of a private international law dispute where one jurisdiction recognises the contract as a valid legal instrument but the other does not. This, however, should not preclude the conclusion that smart contracts ought to constitute legally binding contracts. Therefore, it is prudent to explore the features which may enable smart contracts to displace the functionality of traditional contracts.

Automaticity and Enforceability

The vital characteristics of smart contracts are automaticity and enforceability. The essence of automaticity lies in the contract being performed automatically, without the need of human intervention.¹⁸ This contributes towards a decrease in the marginal cost of contracting and enhances

¹³ Sir Vos, G. (2019, November 18). *The launch of the legal statement on the status of cryptoassets and smart contracts. Annual Combar Lecture 2019*. The Commercial Bar Association. www.judiciary.uk/wp-content/uploads/2019/11/Legal-StatementLaunch.GV_2.pdf

¹⁴ *AA v. Persons Unknown*, 3556 EWHC (2019).

¹⁵ *AA*, 2019.

¹⁶ Werbach & Cornell, 2017.

¹⁷ Janssen, A., & Durovic, M. (2018). The formation of smart contracts and beyond: Shaking the fundamentals of contract law? In L. Di Matteo, M. Cannarsa, & C. Poncibo (Eds.) *Smart contracts and blockchain technology: Role of contract law*. Cambridge University Press. Forthcoming <https://www.researchgate.net/publication/327732779>

¹⁸ Jones, 2019.

the speed with which contractual relationships can be executed.¹⁹ Counterparties are able to enter multiple contracts in minutes, saving on negotiation and organisational costs as well as facilitating everyday commerce. By removing reliance on paper and administrative processes and thus executing the contract in real time, smart contracts prove to be a more efficient and cost-saving method of concluding agreements.²⁰ Hence, it is evident that the efficiencies generated by automatic execution provide great incentives for counterparties to switch to smart contracting.

More importantly, automatic execution represents a key benefit accruing from smart contracting, with it also being “a pre-emptive form of self-help because no recourse to a court is needed for the machine to execute the agreement.”²¹ Taking enforcement out of the hands of the courts is considered particularly important for parties engaging in smart contracting; after all, resolving disputes through litigation has long been criticised as a costly, inefficient, and time-consuming procedure. Indeed, Raskin has argued that “resorting to the court system is a resource intensive process”²² and smart contracting achieves “the lowering of costs through the ensuring of performance without recourse to the courts.”²³ This represents an important incentive for contracting parties to use smart contracts as they will be able to avoid burdensome litigation costs. Arguably, this implies that smart contracts offer the possibility of rendering courts virtually obsolete, since they serve the same function with greater efficiency and customisation.²⁴

Smart contracts also offer law firms the opportunity to allocate resources in a more efficient manner. Heavy manpower is unavoidably required to draft long standardised documents for countless transactions. Rather than dozens of lawyers drafting and reviewing long boilerplate provisions, however, smart contracts offer the advantage of a machine, instead, having to read and verify each term. This would provide the opportunity for lawyers to merely identify non-boilerplate clauses that should be implemented into code and focus their precious time on more intellectually demanding tasks.²⁵ Therefore, smart contracts provide the ability to save on both the resources of counterparties as well as to unlock more efficient allocations of lawyers within law firms.

In addition to providing a less resource-intensive process, smart contract enforceability is able to deliver greater contractual certainty in two interconnected ways. Firstly, smart contracts address the opacity of legal drafting stemming from the inherent ambiguity of natural language. Natural language may be given a multitude of interpretations and thus often represents the subject of a court dispute. However, smart contracts are not capable of understanding and interpreting natural language. As a consequence, smart contracting avoids unnecessary litigation on linguistic interpretations and rather enforces the terms of the agreement.²⁶ Closely associated with this argument is the advantage that, through guaranteeing contractual performance, smart contracts ensure that counterparties are bound to their respective obligations under the agreement. This function is stressed by Werbach and Cornell, who suggest that “smart contracts are like specific performance on steroids and without

¹⁹ Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.2580664>

²⁰ Wright & De Filippi, 2015.

²¹ Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Technology Review*, 1(2), 305–341. <https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO-L-TECH-REV-305-pdf>

²² Raskin, 2017.

²³ Raskin, 2017.

²⁴ Wright & De Filippi, 2015.

²⁵ Wright & De Filippi, 2015.

²⁶ Wright & De Filippi, 2015.

the state's coercive machinery."²⁷ Hence, smart contracts are able to uphold contractual certainty by incorporating legal provisions (wet code) into code (dry code), ensuring that counterparties abide by their duties and obligations under the contract.²⁸ In turn, guaranteed contractual performance will incentive individuals to opt for smart contracting. Contracting parties are assured that the terms of the contract will not be subject to judicial scrutiny, avoiding the risk of a term being stricken down or misinterpreted by the courts. Undoubtedly, this would solve "a longstanding puzzle and problem of e-commerce: courts' longstanding refusal to enforce contract terms proffered by consumers. If courts will not protect consumers, robots will."²⁹

The Harm Principle

On a more theoretical level, automatic execution and enforceability fuel the "subordination of state authority to individual autonomy."³⁰ This view reveals a connection between the much-celebrated harm principle and smart contracting. The harm principle as articulated by Mill mandates that "the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others."³¹ In this sense, the harm principle is inextricably linked with principles of party autonomy and freedom of contract. Arguably, the harm principle finds itself in tension with contract law if the latter is understood as an enforcement of promises; court intervention to interpret contracts and enforce contractual promises is not initiated to prevent harm to others. Indeed, Bix pointed out that some prominent commentators believe that "contract law may involve the state in inappropriately enforcing morality in circumstances where there is no concern about third-party harms."³² In reinforcing this argument, Smith summarised the objection as being "illegitimate for the state to enforce promises qua promises, and thus the state must be doing something other than enforcing promises when it enforces contracts."³³ Unlike traditional contracts, however, smart contracts prevent external interference. They are able to use technology to enforce party autonomy in a more effective manner whilst also maintaining consistency with the harm principle. Consequently, the functionality of smart contracts, both on a practical and theoretical level, has the propensity to disrupt the strict adherence to traditional contracting. To unravel the magnitude of this disruption, one must also consider smart contracts as placed on the blockchain network.

The Blockchain Network: Facilitator or Fallacy?

It has been demonstrated that the attractiveness of smart contracts lies in their automatic execution of tasks and guaranteed contractual performance through eliminating the human element *ex post*. Counterparties enjoy the fruits of contractual certainty through the assurance that the contract will be automatically performed. These gains in efficiency, however, have to be balanced against their lack of agency. Indeed, performance certainty comes at the expense of interpretation uncertainty. This is because an "independent third party must interpret the contract in accord with the

²⁷ Werbach & Cornell, 2017.

²⁸ Wright & De Filippi, 2015.

²⁹ Fairfield, J. (2014). Smart contracts, bitcoin bots, and consumer protection. *Washington and Lee Law Review Online*, 71(2), Article 3. <https://scholarlycommons.law.wlu.edu/wluir-online/vol71/iss2/3>

³⁰ Raskin, 2017.

³¹ Mill, J. S. (1859). *On Liberty*. John W. Parker & Son.

³² Bix, B. H. (2012). Theories of contract law and enforcing promissory morality: Comments on Charles Fried. *Suffolk Law Review*, 45, 719–734. https://scholarship.law.umn.edu/faculty_articles/204

³³ Smith, S. A. (2004). *Contract theory*. Oxford University Press.

intentions of the parties.”³⁴ In the absence of a court to interpret the terms of a smart contract, a solution is presented by blockchain technology. Blockchain is a decentralised ledger used to record transactions verified by members of a peer-to-peer network. Blockchain, therefore, offers a kind of independent agency.³⁵ In essence, the terms and any issues relating to contractual performance will be fed to the blockchain, and if verified by the nodes, the contract will be deemed as having been performed.

The advent of blockchain technology provided the means for transforming Szabo’s vision of smart contracts into something more than a mere curiosity.³⁶ Indeed, “it is only in blockchain networks that there is truly no ex post review of contractual duties after contract formation.”³⁷ This is because blockchain crowdsources the transaction, thus eliminating the threat of counterparty control and the option to frustrate performance.³⁸ One cannot deny that “humans, especially bankers and judges, are seen as fallible and not trustworthy.”³⁹ This consensus gentium is fuelled by the possibility of unconscious bias by the judiciary when resolving disputes and the drive of financial institutions to maximise profit. On the other hand, technology is “objective, infallible and trustworthy.”⁴⁰ The computer merely executes a code, acting without the influence of opinions, emotions, or unintentional biases. Consequently, counterparties may find themselves switching to smart contracting, especially if they are wary of counterparty or external interference with the performance of the contract. The “trustless” blockchain network addresses these concerns “because it creates and confirms a certain state of affairs and replaces the need to trust third parties with the ability to trust the technology itself.”⁴¹

This line of argument demonstrates that “blockchain technology renders the execution of smart contracts truly unstoppable, which means that, in the absence of built-in circuit breakers, all human discretion is excised from the execution and enforcement of contractual duties.”⁴² Nevertheless, one may reasonably question whether this direction is desirable: for example, should legal interpretations be crowdsourced rather than rely on expert judges? Blockchain has proven to be a critical facilitator of the increased reliance on smart contracts, mainly due to the decentralised advantages it offers. Nevertheless, it is an open secret amongst individuals in the industry that blockchain is not as independent as it may seem. In fact, data demonstrates that five large corporations control the majority of the mining process through their mining pools and generate billions in revenue.⁴³ A network cannot be truly decentralised if the majority of the process is conducted by a handful of corporations. The centralisation of the mining process and control over the blockchain network by these corporations may act as a disincentive for counterparties to opt for smart contracting. As a corollary, this also destabilises the balance between the efficiency gains generated by smart contracting and their lack of agency. Even though smart contracts eliminate external interference, by placing the

³⁴ Raskin, 2017.

³⁵ Stark, 2016.

³⁶ Werbach & Cornell, 2017.

³⁷ Paech, P. (2017). The governance of blockchain financial networks. *The Modern Law Review*, 80(6), 1073–1110.

<https://doi.org/10.1111/1468-2230.12303>

³⁸ Cutts, 2019.

³⁹ Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 9(2), 269–300. <https://doi.org/10.1080/17579961.2017.1378468>

⁴⁰ Mik, 2017.

⁴¹ Mik, 2017.

⁴² Paech, 2017.

⁴³ CINDX. (2018, September 1). *Top-5 largest bitcoin mining firms in the world*. <https://medium.com/@cindx/top-5-largest-bitcoin-mining-firms-in-the-world-bb98a1537aad>

blockchain network in the hands of large corporations it can no longer be said that they truly lack agency. Rather, they fall prey to the control of these businesses. This inevitably hinders the displacement of the functionality of traditional contracts.

On the other hand, this may in fact address one major impediment to the widespread adoption of smart contracts. It has been argued that the blockchain network may not be equipped to cope with the potential scalability of smart contracts.⁴⁴ Similarly, Vos predicted smart contracts, when they eventually achieve wider adoption, will become essential in the financial services industry, thus urging the legal community to be prepared.⁴⁵ If there is a surge in the usage of smart contracts, it is not certain whether blockchain has the capacity to facilitate and verify every transaction. Yet, if control of the network rests with several industry giants, they may be able to coordinate and cope with the increased demand. Equally, legal practitioners must prepare and coordinate their efforts to ensure that they can respond to an influx of smart contract litigation. As a result, even though blockchain may not be as decentralised as it was envisaged to be, this could nevertheless facilitate the successful expansion of smart contracts rather than obstruct it. That successful expansion, however, is also contingent upon the blockchain network being safe itself.

The blockchain network portrays itself as an impenetrable environment to conduct transactions. Nonetheless, the Mt. Gox bitcoin exchange hack has demonstrated otherwise. In 2014, following a malicious hack, almost 850 000 bitcoins owned by customers and 100 000 owned by the exchange itself were raided by hackers. Inevitably, the exchange subsequently filed for bankruptcy.⁴⁶ Customers lost all their bitcoin investments along with their trust in the blockchain network. This indicates that contracting parties will be sceptical before choosing to engage in smart contracting. Consequently, it could also be argued that this undermines the scale of efficiency gains against the lack of agency. The blockchain network generates efficiencies for smart contracting parties as long as it remains safe and reliable. Nevertheless, such events prove that the network may be significantly exposed. If all smart contracting gains risk being diverted to malicious hackers, then there is no advantage generated by engaging in smart contracting at all.

The argument in favour of crowdsourcing legal interpretations is therefore already premised on unstable foundations. Blockchain offers a controversial decentralised network that may not be as impenetrable as developers suggest. Sklaroff contributes further to this debate, reasoning that “by shifting dispute resolution to an online system that relies on an ever-changing, unpredictable, unaccountable, and opaque group of decisionmakers, decentralised adjudication cannot generate contract public goods like performance standards, which emerge through the stable application of interpretation rules by courts.”⁴⁷ When delivering judgments, the judiciary shapes the law and provides certainty and clarity to counterparties to determine whether a course of action or inaction would be permissible under a contract. However, by crowdsourcing legal interpretations, the law is deprived of essential guidance and authority that would otherwise emerge from judicial decisions.

⁴⁴ Peters, G. W., & Panayi, E. (2015). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of money. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.2692487>

⁴⁵ Sir Vos, G. (2019, May 14). *Lawtech, smart contracts and artificial intelligence*. Bundesministerium der Justiz und für Verbraucherschutz [Ministry of Justice]. www.judiciary.uk/wp-content/uploads/2019/05/CHC-speech-LawTech-Smart-Contracts-and-Artificial-Intelligence.pdf

⁴⁶ Norry, A. (2020, March 31). *The history of the Mt Gox Hack: Bitcoin's biggest heist*. Blockonomi. <https://blockonomi.com/mt-gox-hack>

⁴⁷ Sklaroff, J. (2017). Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*. 166(1), 263–303.

Closely linked to this argument is the notion that smart contracts merely provide technical contractual enforceability rather than legal enforceability. The judiciary ensures legal enforceability through awarding damages for non-performance to the complainant or legally ordering a performance in cases in which the complainant claims payment of a sum due.⁴⁸ In contrast, smart contracts fail to make this critical distinction. Smart contracts simply recognise that the execution of a contract entails contractual performance; they fail to contemplate for the possibility of legal enforceability through awarding damages. Therefore, by equating enforceability with perfect contractual performance, smart contracts deny counterparties damages that would have been traditionally awarded for non-performance. Overall, this supports the conclusion that the efficiency gains arising out of smart contracts may not be as fruitful when balanced against the lack of a centralised judicial authority to supervise, interpret, and enforce them.

The Potential Versatility of Smart Contracts

This work has demonstrated that smart contract practice is, at the very least, controversial. Nevertheless, this does not negate its effectiveness in a variety of transactions. The versatility of smart contracts as legal instruments suggests that they can be successfully relied upon in many circumstances. In acknowledging this potential, Mik remarked that “what started as a niche phenomenon in such areas as financial derivatives and prediction markets, is now poised to challenge the entire legal landscape and ‘revolutionise’ commerce.”⁴⁹ For example, Vos submitted that “[smart contracts] use in shipping, aviation, energy, telecoms and pharmaceuticals is predictable, because they can provide immutable data, providing huge advantages in terms of certainty and reducing the factual scope of everyday disputes.”⁵⁰ It is evident, therefore, that the potential application of smart contracts is vast.

More specifically, smart contracts could prove to be an invaluable tool in financial market transactions such as share transfers or derivatives contracts. Stark accurately submits that “articulating these contracts in code could allow financial markets to become more automated and simplify many process-intensive systems related to trading and servicing of financial instruments.”⁵¹ In such circumstances the efficiency gains arising from smart contracts trump the lack of agency. This due to the fact that financial transactions are widely used on a standardised basis by sophisticated counterparties and therefore the need for adjudication is minimal.

In addition, through guaranteed contractual performance, counterparty and settlement risks, which are deep-rooted in these contracts, are reduced or even eliminated.⁵² For example, it has been reported that the World Bank authorised CBA to issue a blockchain-based bond; that bond will be governed by smart contracts which will underlie and facilitate the bond transactions.⁵³ Paech observed that a smart contract underpinning a blockchain-based bond “automatically executes interest payments on the payment date, and the amount to be paid is determined on the basis of data retrieved from a predefined, reliable Internet source.”⁵⁴ This will incentivise greater activity in the

⁴⁸ Mik, 2017.

⁴⁹ Mik, 2017.

⁵⁰ Sir Vos, 2019.

⁵¹ Stark, 2016.

⁵² Paech, 2017.

⁵³ Global Banking & Finance Review. (2018, August 23). *Smart contracts and a future of financial operations*. www.globalbankingandfinance.com/smart-contracts-and-a-future-of-financial-operations

⁵⁴ Paech, 2017.

financial industry by reducing the risk of counterparties failing to make timely interest payments. Accordingly, through guaranteed performance and real-time execution, the CBA initiative may prove to be a catalyst in transforming the financial markets industry.

Similarly, smart contracts may also reduce dependence on financial market infrastructures such as CCPs and minimise the risk of default, thereby improving the financial services industry.⁵⁵ For example, in a transaction concerning security collateral held in a blockchain network, the smart contract could automatically transfer the securities to the creditor if the debtor has not paid on time.⁵⁶ Overall, this suggests that the benefits offered by the application of smart contracts in the financial industry are substantial. The lack of agency does not seem to impact the financial sector negatively; rather, the efficiencies generated promote the expansion of financial markets and contribute to the overall development of the economy.

Smart contracts can also be used to execute corporate governance rules, reinforcing the argument of versatility. Decentralised Autonomous Organisations (hereinafter “DAO”) use smart technology to execute corporate governance rules. Slock.it, a German blockchain startup, developed the open source coding framework for the DAO and ultimate control was granted to the shareholders on a blockchain. Slock.it envisioned “build[ing] a humanless venture capital firm that would allow the investors to make all the decisions through smart contracts. There would be no leaders, no authorities.”⁵⁷ This vision was founded on the idea that centralised and hierarchical organisations are inherently inefficient. This is because they lack flexibility to evolve, burdened with unnecessary administrative processes and often suffering from corruption.⁵⁸ Therefore, the thrust of DAOs lies in the belief that by granting directorial power to DAO owners, the ability of directors to misdirect and waste investors’ funds is eliminated. Indeed, the DAO contributed towards the removal of managerial costs⁵⁹ and provided a completely transparent process since everything was run by the code. The desirability of smart contracts in this context rests with their aim “to provide full transparency of the transaction and to grant a high degree of privacy contemporaneously.”⁶⁰ Consequently, they establish DAOs as autonomous and self-sufficient corporate governance tools, requiring users to place trust to the underlying code rather than the organisation itself.⁶¹ Overall, the DAO contributes to the conclusion that smart contracts are versatile legal instruments, offering valuable advantages that traditional contracts are simply not equipped to provide.

Errors in Smart Contract Code: The DAO Experience

Nevertheless, that is only part of the story. Soon after the DAO raised more than \$150 million, an individual discovered a loophole in the code and diverted almost \$70 million worth of ether.⁶² Raskin

⁵⁵ Lord Hodge. (2019). *The potential and perils of financial technology: Can the law adapt to cope?* The First Edinburgh FinTech Law Lecture. University of Edinburgh. www.supremecourt.uk/docs/speech-190314.pdf

⁵⁶ Paech, 2017.

⁵⁷ Kar, I., & Wong, J. I. (2016, July 18). *Everything you need to know about the Ethereum “hard fork”*. Quartz. <https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork>

⁵⁸ Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, 6(1), 45–62. http://dx.doi.org/10.22495/jgr_v6_i1_p5

⁵⁹ Raskin, 2017.

⁶⁰ Janssen & Durovic, 2018.

⁶¹ Wright & De Filippi, 2015.

⁶² Madeira, A. (2019, March 12). *The DAO, the hack, the soft fork and the hard fork*. CryptoCompare. www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork

observed that “the hacker did not hack” the code in a malicious way, but rather used the terms of the existing smart contracts to accomplish something others later found objectionable, i.e. the diversion of their money.⁶³ This demonstrates that smart contracts also suffer from material shortcomings. A mere error or vulnerability in the code may bring about systemic consequences. This is due to the fact that a single error harms every transaction conducted on that code, not only the isolated transaction. The DAO saga, therefore, represents a lacuna in smart contracting which merits greater consideration.

The aftermath of the DAO hack found developers divided. The funds could have been returned through a “hard-fork” which in essence forced developers to create a new smart contract with different rules to reimburse the stolen funds. The division was between proponents of fairness and justice who wanted to see the funds reverted back, versus the “code is king” purists who favoured adherence to the smart contracts’ programming. Eventually, the developers intervened using a “hard-fork” which, in turn, completely undermined the objective of DAO as a decentralised and immutable platform.⁶⁴ The DAO developers may have embarked on a “slippery slope” given that by intervening once they opened up the possibility of more interventions. Similarly, the supposed decentralised nature of the network gets undermined further when one considers the fact that, although DAO was an open source network, Slock.it had a considerable influence in its development.⁶⁵ This fuels the argument that the idea of a decentralised blockchain and the removal of the human element *ex post* is not an accurate representation of these technologies. It is therefore prudent to wonder that “if contracts held to be inviolable can effectively be overturned by a collective decision to run new software, what guarantee do financial institutions have that their transactions and funds are secure?”⁶⁶ The answer is none. This gets at the heart of the functionality of smart contracts. If financial institutions base all their transactions on these technologies, a decision to run new software would generate uncertainty and affect the value of these transactions, causing global systemic effects in financial markets.

It is evident that the systemic risks exposed by the DAO hack raise several concerns about the functionality of smart contracts. More broadly, the hack reveals that the foundational characteristics which make smart contracts attractive ought to be questioned. Unlike traditional contracts where parties may resort to courts to resolve disputes, the automaticity embedded in smart contracts means that the contract will be performed irreversibly, even though the code is prone to errors or exploitation. As a result, since “the possibility of computer errors affecting the manner in which the smart contract operates cannot be eliminated, it is impossible to claim that self-enforcement guarantees perfect performance.”⁶⁷ Inevitably, the outcome will not be one contemplated by the contracting parties, but the contract will be deemed as being performed to their detriment. This represents merely one, albeit fundamental, aspect of the inflexible nature of smart contracts.

The Inflexible Nature of Smart Contracting

It must be acknowledged that smart contract codes lack certain necessary human qualities that might prevent contracting parties from relying on smart contracts. Murray observed that smart contracts “attempt to remove the human elements of contextualization and perhaps even compassion

⁶³ Raskin, 2017.

⁶⁴ Kar & Wong, 2016.

⁶⁵ Janssen & Durovic, 2018.

⁶⁶ Kar & Wong, 2016.

⁶⁷ Mik, 2017.

or the concept of ‘justice’ as opposed to simply interpretation and enforcement from the process.”⁶⁸ Machines cannot develop a sense of empathy, fairness, or justice; with such qualities absent, parties may be reluctant to engage in smart contracting. The force of law lies in the power of the judiciary to apply flexible rules whilst also considering the surrounding circumstances such as the position and relationship of the contracting parties. In contrast, machines are ill-equipped to conduct such an assessment since they are “rigid, deterministic and insulated from their commercial context.”⁶⁹ Equally, machine learning has not reached the stage of understanding and enforcing natural language and is still limited to executing code. This limitation provided the foundation for Clack et al to doubt whether smart contracts are able to address the scenario of parties having a different understanding of the agreed terms.⁷⁰ By failing to grasp the meaning of a contractual term and strictly execute the code, the actual output of the smart contract may not be desirable, since it “may differ from the intentions of the parties.”⁷¹ This inadequacy is highlighted further when considering the situation of the smart contract code not being written by the parties themselves. In fact, Mik argued that the person writing the code may fail to correctly input the parties’ intentions and the parties, not being computer programmers, will not be able to verify the code themselves.⁷² As a result, machines will give effect to a smart contract even though the outcome is not desirable. Courts, on the other hand, through knowledge and experience, are able to assess the intention of the parties to a particular contract unlike machines. This inevitably supports the notion that smart contracts are inflexible self-enforcing instruments, whereas traditional contracts are more flexible.⁷³

It logically follows that opting for smart contracting requires “trade-offs between precision and certainty on one hand and ambiguity and flexibility on the other.”⁷⁴ This trade-off, however, is arguably made redundant if one unpacks further the inflexibility of smart contracting. Mik correctly recognised that “the elimination of human judgment and the automation of choice can easily evolve into a situation where the contracting parties effectively lose the ability to choose whether and how to exercise their rights.”⁷⁵ Smart contracting parties may, thus, find themselves bound to a contractual agreement that does not generate the rights that they intended to gain. If contracting parties take into account these concerns in their decision to opt for smart contracts, then it is likely that they will revert back to traditional contracts. Overall, this fuels the conclusion that the functionality of traditional methods has not been displaced by the emergence of smart contracts.

Ambiguity and Contractual Modification

The inflexible nature of smart contracts is underlined by two additional factors. Courts are unable to affect smart contract performance and the contracts themselves are not susceptible to modifications.⁷⁶ Commercial parties often conclude contracts on ambiguous terms because the cost of

⁶⁸ Murray, A. (2019). *Information technology law* (4th ed.). Oxford University Press.

⁶⁹ Mik, 2017.

⁷⁰ Clack, C. D., Bakshi V. A., & Braine L. (2016). *Smart contract templates: Foundations, design landscape and research directions*. arXiv. <http://arxiv.org/abs/1608.00771>

⁷¹ Raskin, 2017.

⁷² Mik, 2017.

⁷³ Janssen & Durovic, 2018.

⁷⁴ Mik, 2017.

⁷⁵ Mik, 2017.

⁷⁶ O’Shields, R. (2012). Smart contracts: Legal agreements for the blockchain. *North Carolina Banking Institute*, 21(1), 177-191. <https://scholarship.law.unc.edu/ncbi/vol21/iss1/11>

negotiating is too high or the contract itself is regarded as a mere formality and thus they decide not to agree on everything.⁷⁷ This poses an issue for smart contracting parties, since “humans are very good at working with ambiguity [whereas] machines are not.”⁷⁸ If there is an ambiguity in the code, it is hard to see how a smart contract can be executed. Courts in most jurisdictions recognise and give effect to imperfect contractual performance, yet a computer programme is unable to do so, since this possibility was not contemplated and recorded by the parties.⁷⁹ Consequently, this indicates that “smart contracts are not smart enough to adjust as events unfold”⁸⁰ given that they would be unable to cope with vague contract terms.

Furthermore, not only are smart contracts incapable of dealing with contractual ambiguity, but they are also unable to deal with contractual modification. If a traditional contract cannot be performed due to unforeseeable circumstances, non-performance is excused. The contract becomes frustrated in the event of an unanticipated occurrence that renders performance impossible, meaning that neither party incurs liability for non-performance.⁸¹ On the other hand, a smart contract cannot make sense of any contractual modification. The immutability of smart contracts prevents parties from modifying any contractual term and the possibility of any interference with performance is eliminated even in unprecedented circumstances⁸² (for example, how could one pre-empt in a contract the possibility of a respiratory virus dooming the world?). Nevertheless, a traditional contract could be modified or frustrated to take into account such unforeseeable circumstances, whereas a smart contract is not equipped to handle these situations, and thus the parties will have to fall back to traditional dispute resolution.⁸³

In an attempt to address this deficiency, Raskin offered two solutions to this problem: (i) a publicly available jurisdictional database which contracting parties can feed into the programme to remain updated on evolving legal rules; and (ii) ex post policing of the parties by placing the burden on the parties or their agents to update the code.⁸⁴ Even though these solutions seem viable, there have not yet been any attempts to implement them. More importantly, however, the question should be whether it is even desirable to adopt them. Ex post policing of a smart contract is arguably as inefficient as ex post reviews by courts and judges; this is because it would take time, effort and money to constantly review and update the code. Therefore, it is evident that the efficiency justifications for relying on smart contracts gradually start being eroded as soon as the impracticalities of their application are unpacked.

Paech offered a more practical solution to smart contract immutability. This involves a combination of smart and dumb contracts. Dumb contract terms would encompass parts of the agreement that are excluded from the blockchain and thus are modifiable. The rest of the agreement would be recorded on the blockchain and would be immutable.⁸⁵ Accordingly, this solution would allow parties to modify certain parts of the agreement and address the contractual implications of any unforesee-

⁷⁷ Levy, K. E. C. (2017). Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, 3, 1–15. <https://doi.org/10.17351/ests2017.107>

⁷⁸ Murray, 2019.

⁷⁹ Raskin, 2017.

⁸⁰ Werbach & Cornell, 2017.

⁸¹ *Taylor v. Caldwell*, EWHC QB J1 (1863).

⁸² Paech, 2017.

⁸³ Xiao, D. (2016, June 18). *In bits we trust (?)*. Medium. <https://medium.com/@coriacetic/in-bits-we-trust-4e464b418f0b>

⁸⁴ Raskin, 2017.

⁸⁵ Paech, 2017.

able circumstances. On the other hand, one may reasonably submit that this is contrary to the heart and the spirit of smart contracting. Combining dumb and smart contracts would certainly take more time and may also contribute to increased costs. This would also create difficulties in determining what terms should fall within the smart or dumb part of the contract. Thus, this solution will generate inefficiencies which will disincentivise contracting parties from using smart contracts. After all, why would contracting parties opt for a combination of smart and dumb contracts when they could simply rely on a consistent and trustworthy traditional contract? Counterparties certainly prefer a contracting method that is easy, efficient, and cost-effective. Consequently, the solutions proposed to address smart contract modifications do not portray smart contracts as a viable alternative that can displace the functionality of traditional contracting.

Lastly, this argument is augmented if one explores the possibility that smart contracts may in fact generate greater costs than traditional contracts. Widespread adoption hinges upon the theory that smart contracts are efficient, inter alia eliminating drafting and litigation costs. Nonetheless, Sklaroff remarked that smart contracts may turn out to be more expensive and less efficient than traditional contracts. This argument is premised on the fact that smart contracts “must be written in precise, fully defined computer code; they are unmodifiable once executed; and they favour anonymous and one-off transactions.”⁸⁶ In contrast, traditional contracting practice is often straightforward and merely requires the skillset of an elementary lawyer. This supports the conclusion that smart contracts have not displaced adherence to traditional contracts, given that no active steps have been taken to ameliorate the difficulties they present.

Smart Contracts: Sound in Theory, Limited in Practice?

This essay has steadily demonstrated that, although smart contracts seem sound in theory, the complexities embedded in their execution limit their practice. If one examines various types of contractual arrangements and their possible translation to smart contracts, this picture becomes even clearer. For example, the obligation to exercise reasonable care and skill underpins the majority of goods and services contracts; if these are translated to smart contracts, “it may be difficult to reduce them to sequences of steps and to provide objective benchmarks against which they can be evaluated.”⁸⁷ Indeed, it is hard to imagine how a smart contract code can make a factual inquiry to determine whether reasonable care has been exercised and to evaluate what amounts to reasonable care in the circumstances. More generally, not all contractual terms can be deduced to computer code and fed into a machine,⁸⁸ hindering the predictions of widespread adoption put forwards by smart contract proponents. This implies that smart contracts are currently incapable of displacing outright the functionality of traditional contracts.

Furthermore, it could be argued that, even in those transactions that smart contracts ought to have been conducting flawlessly (such as financial instruments), the results have been disappointing. In 2016 Barclays tested a way to trade derivatives using smart contracts and blockchain technology, but despite this endeavour, that has not been implemented successfully⁸⁹; more crucially, had such a method been implemented, what would be the outcome if Barclays would remove itself from

⁸⁶ Sklaroff, J. (2017). Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, 166(1), 263–303.

⁸⁷ Mik, 2017.

⁸⁸ Mik, 2017.

⁸⁹ Allison, I. (2018, April 26). *Barclays, Goldman champion ISDA standard for blockchain derivatives*. CoinDesk. www.coindesk.com/barclays-goldman-champion-isd-standard-blockchain-derivatives

the transaction? Lord Hodge submitted that if financial institutions were to walk away from such transactions, that would have a systemic effect on the commercial world.⁹⁰ His Lordship therefore urged that “if there is to be a contract drafted or adapted by machines, there will have to be significant development to our law of contract which will require careful and imaginative consideration.”⁹¹ Nevertheless, even if such a contract law is adapted accordingly, the technology underlying smart contracts remains underdeveloped. Although a speculative technological advancement may address concerns regarding smart financial instruments, it does not address concerns in other transactions. Until artificial intelligence is developed significantly to be able to understand and enforce contractual terms, the effectiveness of smart contracts remains disappointing. As a result, current efforts to utilise smart contracts in areas such as real estate or intellectual property provide a false sense of hope given that the technology itself must be brought up to speed.

This naturally leads to the last shortcoming. Even in areas in which smart contracts are successfully relied upon and operate efficiently, they may fall short of providing adequate protection to contracting parties. Smart contracts are not set to render the contract void or non-enforceable if one of the contracting parties is, for example, a victim of duress, misrepresentation, or undue influence of its counterparty.⁹² Similarly, there is no evidence to suggest that smart contracting parties are guarded from unfair contract terms which would otherwise be subject to a statutory test of reasonableness.⁹³ In addition, smart contracting provides a limited, possibly non-existent, remedial infrastructure. Cutts correctly submitted that parties have to rely on their counterparties to remedy any wrong, and that is also contingent upon parties knowing the identity of their counterparty, which will not often be the case.⁹⁴ Hence, Cutts concluded that “without the many safeguards implemented by traditional intermediaries, parties are more exposed to harm, and without the remedial mechanisms of intermediation, most parties will be wholly unable to fix that harm.”⁹⁵ This is a realistic conclusion given that there is no incentive for the wrongdoer to remedy the wrong, especially if they have no connection to the counterparty. Overall, by failing to shield counterparties from harm, smart contracts merely represent a useful innovation in limited transactions rather than providing a viable alternative to traditional contracts.

Concluding Remarks

The reality is that smart contracts have not managed to acquire the widespread adoption that many programmers, lawyers, and academics predicted. Rather, “so far smart contracts have mostly been focused on transactions involving financial instruments and investment instruments as these tend to be more easily reducible to code.”⁹⁶ In line with various academics and the UKJT, this essay took the view that smart contracts carry the same legal validity as traditional contracts. Additionally, it has been acknowledged that the automaticity and self-enforcement advantages provided by smart contracts certainly amplify the scope of certain commercial transactions. Through utilising block-

⁹⁰ Lord Hodge, 2019.

⁹¹ Lord Hodge, 2019.

⁹² Wright & De Filippi, 2015.

⁹³ Unfair Contract Terms Act (1977).

⁹⁴ Cutts, T. (2019). Smart contracts and consumers. *West Virginia Law Review*, 122(2), 389–446. <https://researchrepository.wvu.edu/wvtr/vol122/iss2/4>

⁹⁵ Cutts, 2019.

⁹⁶ Murray, 2019.

chain technology, smart contracts have established themselves as prominent legal instruments; however, the inherent limitations of the blockchain network, which undermine both its immutability and decentralisation benefits, preclude smart contracts from achieving their full potential. Although they may have a potentially versatile application, smart contracts have not been so successful as to disrupt society's preference for traditional contracting. Individuals trust the court process and the protections guaranteed by the legal system. Machines, on the other hand, are susceptible to errors, exploitation, and hacking. They are unable to process natural language or provide solutions to code ambiguities and contractual modifications. Importantly, they also fail to protect contracting parties from counterparty wrongdoing. Overall, the underlying technology is relatively underdeveloped to fully function at its envisaged applications of smart contracting. This essay, therefore, supports the view that "smart contracts may or may not transform the world, but they provide real benefits and seem likely to enjoy significant adoption over time ... they will not, however, replace contract law."⁹⁷ This is because smart contracts are currently limited to performing a different function to traditional contracts. The former guarantees technical contractual enforceability, whilst the latter provides legal enforceability by looking backwards to recognise and remedy grievances.⁹⁸ Consequently, it is prudent to conclude that smart contracts currently serve as a supplement to traditional contracting and the road towards displacing traditional contract practice is uphill. Nonetheless, it is never too early to prepare for the upcoming smart contract revolution, and "the real prize will be to persuade the coders to include a simple English law and UK jurisdiction clause in their algorithmic engagements."⁹⁹

Information about the author:

Alexandros A. Papantoniou – LLM (LSE), Advocate, Papantoniou & Papantoniou LLC, Nicosia, Cyprus.
alexandros.papantoniou1@gmail.com

Сведения об авторе:

Папантониу А.А. — магистр права (LSE), адвокат, Papantoniou & Papantoniou LLC, Никосия, Кипр.
alexandros.papantoniou1@gmail.com

⁹⁷ Werbach & Cornell, 2017.

⁹⁸ Janssen & Durovic, 2018.

⁹⁹ Sir Vos, G. (2019, November 12). *Future proofing for commercial lawyers in an unpredictable world*. Annual Combar Lecture 2019. The Commercial Bar Association. www.judiciary.uk/wp-content/uploads/2019/11/COMBAR.lecture2019.final_.pdf

ARTICLES

FINTECH & NEW DIGITAL INSTRUMENTS. POST-CRISIS DEVELOPMENTS: RUSSIA AND EUROPE

Anna V. Shashkova^{1,*}, Maria A. Agranovskaya²,
David E. Kitsmarishvili³

¹Moscow State Institute of International Relations (MGIMO-University)
76, ave. Vernadsky, Moscow, Russia, 119454

²GRAD Legal & Financial Advisory Services
1-33/2, Baumanskaya str., Moscow, Russia, 105005

³Russian Foreign Trade Academy
6A, Vorobiyovskoye Highway, Moscow, Russia, 119285

Abstract

The article examines 2020 post-crisis results and 2021 trends in FinTech regulation development. FinTech, being a relatively new term, has become a completely new industry, which combines rapidly developing technologies and financial products (including digital assets) or services. The year 2020, despite the pandemic and localization (and maybe even more so), seems as significant, if not more so, for market change and further development. The world has changed, and new technologies are vital for successful competition among financial players and even for their survival. Most of the leading international financial centers have focused on regulating FinTech and the use of innovations in classic highly regulated areas. In the article we address the pros and cons of technology regulation and make a comparative analysis of the leading revolutionary trends.

The most revolutionary developments have appeared in smaller European countries, which the leaders are forced to follow. Law harmonization has become a natural step forward for Europe to regulate blockchain businesses and to agree on terminology and risk prevention measures for innovation support. The research examines the development and regulation of FinTech in such jurisdictions as Switzerland, Malta, Liechtenstein, Gibraltar and the United States. The approach is interdisciplinary, linking Russian legal norms, applicable rules, and expected results. The main methods used in the research are analysis, comparative-legal, and formal-legal methods.

Keywords

FinTech, post-crisis regulation, financial sector, blockchain, digital assets, Russia, EU, Switzerland

Conflict of interest The authors declare no conflict of interest.

Financial disclosure The study had no sponsorship.

For citation

Shashkova, A. V., Agranovskaya, M. A., & Kitsmarishvili, D. E. (2020). FinTech & new digital instruments. Post-crisis developments: Russia and Europe. *Digital Law Journal*, 1(4), 25–37. <https://doi.org/10.38044/2686-9136-2020-1-4-25-37>

* Corresponding author

Submitted: 12 Sep. 2020, accepted: 02 Oct. 2020, published: 20 Dec. 2020

СТАТЬИ

FINTECH И НОВЫЕ ЦИФРОВЫЕ СРЕДСТВА. ПОСТКРИЗИСНОЕ РАЗВИТИЕ: РОССИЯ И ЕВРОПА

А.В. Шашкова^{1,*}, М.А. Аграновская², Д.Э. Кицмаришвили³

¹Московский государственный институт международных отношений (МГИМО-университет) МИД России
119454, Россия, Москва, просп. Вернадского, 76

²МКА «ГРАД»
105005, Россия, Москва, ул. Бауманская 33/2, стр.1

³Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации
119285, Россия, Москва, Воробьевское шоссе, 6А

Аннотация

В статье исследуются последствия кризиса 2020 года и тенденции развития регулирования FinTech 2021 года. FinTech, являясь относительно новым термином, стал совершенно новой отраслью, которая сочетает в себе быстро развивающиеся технологии и финансовые продукты (в том числе цифровые активы) или услуги. 2020 год, несмотря на пандемию и локализацию (а может быть благодаря пандемии), представляется столь же значительным, если не более значительным, для изменения рынка и его дальнейшего развития. Мир изменился, и новые технологии имеют жизненно важное значение для успешной конкуренции между финансовыми игроками, и даже для их выживания. Большинство ведущих международных финансовых центров сосредоточилось на регулировании FinTech и использовании инноваций в классических высоко регулируемых областях. В статье мы рассматриваем плюсы и минусы регулирования технологий и проводим сравнительный анализ развивающихся тенденций.

Наиболее революционные тенденции проявились в небольших европейских странах, за которыми лидеры вынуждены следовать. Гармонизация законодательства стала для Европы естественным шагом вперед в регулировании блокчейн бизнеса, и согласовании терминологии и мер по предотвращению рисков для поддержки инноваций. В статье рассматривается развитие и регулирование FinTech в таких юрисдикциях, как Швейцария, Мальта, Лихтенштейн, Гибралтар и Соединенные Штаты.

Подход является междисциплинарным, увязывающим российские правовые нормы, применимые правила и ожидаемые результаты. Основными методами, используемыми в исследовании, являются аналитический, сравнительно-правовой и формально-юридический методы.

Ключевые слова

FinTech, посткризисное регулирование, финансовый сектор, блокчейн, цифровые активы, Россия, ЕС, Швейцария

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Шашкова, А. В., Аграновская, М. А., Кицмаришвили, Д. Э. (2020). FinTech и новые цифровые средства. Посткризисное развитие: Россия и Европа. <i>Цифровое право</i> , 1(4), 25–37. https://doi.org/10.38044/2686-9136-2020-1-4-25-37

* Автор, ответственный за переписку

Поступила: 12.09.2020, принята в печать: 02.10.2020, опубликована: 20.12.2020

Introduction

FinTech, being a relatively new term, has become a whole new industry that combines rapidly developing technology (blockchain, artificial intelligence (AI) and machine learning, Internet of things (IoT), big data, etc.) and financial products (including digital assets) or services. Considering this issue in the context of the current situation and post-crisis results analysis, it would be useful to revert to previous experience, specifically the year 2008. Apparently, the crisis then gave rise to new FinTech products and projects, an innovation initiative, and the renewal of banking, insurance, payment systems, lending, and other activities in the financial world (Arner et al., 2016).

2020, despite (or maybe even more due to) the pandemic and lockdown, seems to be as significant – if not even more so – for the market change and further development. The world has changed, and new technologies are vital for successful competition between and even the survival of financial players.

Most leading international financial centers have paid a lot of attention to regulation of FinTech, largely as a special block – blockchain and digital assets, accordingly, and the use of innovation in the classic highly regulated areas. The regulatory update has been welcomed in light of the social and economic impact of the financial crisis. The experiences of reasonable regulators over recent years (2017–2020) support legal improvements in this regards; for example, blockchain related projects in Switzerland or Singapore have resulted in the market revival, new local and foreign investments, and new international collaboration opportunities too.

Analysis of the Current FinTech State. The “Pulse of FinTech” Trends

This year’s crisis has shown the great need for cooperation and the legal grounds for this, as well as a harmonization of standards and procedures in the financial world, alongside other such matters. The European Union Commission has recently announced its goal to complete its work on digital finance, in particular, to introduce a clear definition for cryptocurrency into European law. As the Commission Executive Vice President Valdis Dombrovskis highlighted

this June, a “lack of legal certainty is often cited as the main barrier to developing a sound crypto-asset market in the EU. This is a good chance for Europe to strengthen its international standing and to become a global standard-setter, with European companies leading new technologies for digital finance”¹

The outcome of the 2019 consultation held by the Commission for experts around Europe was a “non-paper”² with clear priorities:

- Definitions for all types of crypto, including stablecoins and security tokens.
- Changes to the markets in Financial Instruments Directive II (“MiFID II” Directive 2014/65/EU)³ to include crypto assets.
- A regime for blockchain-based platforms.

Many important players, such as PayPal or Google, have made their contributions. Bruno Schneider Le-Saout, the President of the Blockchain Federation (Brussels), has named the upcoming legislation as “historic”⁴

Among the pioneers of new local regulatory developments within the EU have been Malta and Liechtenstein, as examples, but the rules then were valid only for a single country territory; now, the whole EU market should be covered. The pandemic outburst has only proven the importance of new efficient cross-border mechanisms, new technology implementation, and common international standards and rules. The regulation of financial markets is probably one of the most difficult to change, especially requiring various considerations of political and economic interests. Some retrospective references to previous post-crisis measures have been used to understand the efficiency of the new measures to be taken. The cross-jurisdictional comparative analysis may demonstrate the most successful regulatory solutions in specific FinTech areas or mechanisms for the general development of the economy, e.g., sandboxes and experimental legal regimes (Allen, 2020). Such work may assist in the unification and harmonization of international approaches and the setting of the best practices and common standards for financial technology regulation that can “open a new era in FinTech” (Arner et al., 2016).

Russia has been comparatively active in FinTech and the digitalization of its economy (though the success in different financial spheres of technology application is not the same). The National Digital Economy Programme⁵ has been introduced, covering the main goals for several years. The crisis has definitely had a serious impact on these plans. The state and regional budgets for new technology projects are being cut and the resources redistributed to healthcare and support of the most affected businesses. Together with that, enhancing and updating the legal framework becomes even more important for the economic recovery and new investments in technology. Such work will

¹ European Commission. (2020, June 23). *Speech by Executive Vice-President Valdis Dombrovskis at the Digital Finance Outreach 2020 closing conference*. https://ec.europa.eu/commission/commissioners/2019-2024/dombrovskis/announcements/speech-executive-vice-president-valdis-dombrovskis-digital-finance-outreach-2020-closing-conference_en

² For more information see: Houben, R., & Snyers, A. (2020). *Crypto-assets. Key developments, regulatory concerns and responses (Study)*. Luxembourg: European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU\(2020\)648779_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf)

³ European Commission. (2014). *Markets in financial instruments directive (MiFID II)*. https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en

⁴ Reynaldo, M. (2020, August 20). *Europe to introduce “historic” legislation for Bitcoin and cryptocurrencies in autumn*. <https://www.crypto-news-flash.com/europe-to-introduce-historic-legislation-for-bitcoin-and-cryptocurrencies-in-autumn/>

⁵ *Natsional'naya programma “Tsfrovaya ekonomika Rossiyskoy Federatsii” [The National Digital Economy Program of the Russian Federation]*. (2019). This includes the current normative regulation of digital industry.

be continued intensively in 2020 and beyond. Three important acts regulating blockchain related matters and new financial assets have been a subject of debate for at least a couple of years, and this year has brought the long-awaited results. The new, and as-yet outstanding, regulation will be discussed further.

The main part of this article addresses in more detail the specific area of financial sector regulation — blockchain based or digital financial assets, crypto currencies, and new investment platforms involving digital assets — and the impact of new regulation on the market development (based on the Russian example).

New FinTech & Blockchain Related Country Regulation: Licensing Regimes

After the financial crisis of 2008, banks were also forced to comply with the Basel III⁶, the Dodd-Frank Act⁷, and other similar requirements, which led to increased costs. Competition with efficient FinTech firms has forced banks to go online, introducing different services to their customers and trying to reduce high operational expenses to cope with payment startups. Slow regulatory changes and huge institutional players with internal procedures and rules are unable to regulate this promptly changing area with a lot of relatively small players. Accordingly, this has been an obstacle for development and raising investment for technology and FinTech startups. From an industry perspective and from a regulatory perspective alike, a change in attitude is needed towards how FinTech should be regulated. From this point of view, the examples of Switzerland, Liechtenstein, Gibraltar, and Malta are remarkably interesting.

Often, new FinTech regulation concerns the use of DLT or new financial assets built on and transferred via blockchain. In this article we are only giving a couple of examples and will be following up with further articles and a more in-depth comparative analysis of all leading jurisdictions (UK or the USA, Singapore, some CIS countries, and more).

Gibraltar

Gibraltar, a British overseas territory, was the first jurisdiction that implemented special FinTech regulatory legislation. By passing the Financial Services (Distributed Ledger Technology or DLT) Regulations 2017⁸, entered into force from 01 January 2018, the Gibraltar Financial Services Commission (GFSC) became the standard-setter body, licensing any person (legal entity), in or from Gibraltar, that uses DLT for storing or transmitting value belonging to others (Lifshits, 2016). There are three classes of DLT licenses in Gibraltar, based on the complexity of the matter — Malta came out later, but has gone further with a more structured approach to legislation (as described below).

The Republic of Malta

The Maltese legal framework governing the FinTech industry consists of three main laws, namely:

⁶ Basel III is a global regulatory framework on bank capital adequacy, liquidity risks, stress testing. (2019, November 19). <https://www.bis.org/bcbs/basel3.htm>

⁷ The Dodd-Frank Act is a complex bill that put strict regulation on the US financial industry and created programs to stop mortgage companies and lenders from taking advantage of consumers. (2010). <https://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm>

⁸ HM Government of Gibraltar. (2020, September 17). *The British Overseas Territory Gibraltar. Distributed ledger technology regulations — 631/2020*. <https://www.gibraltar.gov.gi/press-releases/gibraltar-regulator-refreshes-jurisdictions-distributed-ledger-technology-regulation-6312020-6206>

- The Innovative Technology Arrangements and Services Act (ITAS)⁹;
- The Malta Digital Innovation Authority Act (MDIA)¹⁰;
- The Virtual Financial Assets Act (VFAA).¹¹

It has to be mentioned that the Malta Financial Services Authority plays a significant role in the process of “lawmaking” by issuing its FinTech guidelines.

Licensing issues are regulated by the VFAA. One of the salient features which determines the applicability of the VFAA is the *type of asset* which the operator would be dealing with. Through the application of the Financial Instrument Test, a DLT asset (i.e. a cryptocurrency) will be classified as either a virtual token, a financial instrument, e-money, or a virtual financial asset. In this regard, it has to be mentioned that the EU Directives and Regulations on markets in financial instruments, e-money, payment services, and anti-money laundering are additionally applicable; this, despite Maltese laws not applying and local licenses not being valid throughout the EU. The same applies, for example, to Gibraltar (not being formally part of the EU).

The provision of the following services in or from within Malta, in relation to a DLT asset which has been determined to be a virtual financial asset in terms of VFAA, requires a license to regulate one of the following services: the reception & transmission of orders; the execution of orders on behalf of other persons; custody or nominee services; portfolio management; dealing on one’s own account; investment advice; placing virtual financial assets; operations of a VFA exchange. In order to provide these services, it is needed to obtain a license. There are four types of “FinTech licenses”: *VFAA Class 1 to 4* (depending on the activity itself).

The Virtual Financial Assets Act establishes the application procedure and the requirements that the service providers shall meet in order to be granted a license, including – but not limited to – organizational requirements, financial requirements, operational requirements and anti-money laundering (AML), combating the financing of terrorism (CFT), and cybersecurity related requirements.¹² The VFAA license will only cover services with respect to virtual financial assets. If a particular asset is classified as a financial instrument, then any service provided in relation thereto would require prior authorization under traditional financial services legislation (including placement).

The Principality of Liechtenstein

Liechtenstein is also amongst the world’s first jurisdictions to pass a specialized “Blockchain Act”¹³ The new Blockchain Act applies to all trustworthy technology service providers (instead of just using the term “blockchain” or “distributed ledger technology”, the term “trustworthy technology or TT” is used). From 01 January 2020 (from the date when this law entered into force) the following services on a professional basis in Liechtenstein must register with the Financial Market Authority of Liechtenstein (FMA): *token issuers; token generators; TT Key Depositaries and TT Token Depositaries*.

Generally, the law clearly defines the end scope of services that should be registered (licensed) by the Liechtenstein’s FMA. In addition to the aforementioned services, other TT services can be

⁹ The Innovative Technology Arrangements and Services Act (ITAS). (2018).

¹⁰ The Malta Digital Innovation Authority Act (MDIA). (2018).

¹¹ The Virtual Financial Assets Act (VFAA). (2018).

¹² Malta Financial Services Authority. (n.d.). *Virtual Financial Assets*. <https://www.mfsa.mt/fintech/virtual-financial-assets/#legislativeRegulatoryFramework>

¹³ Originally, the Token and TT-Service Provider Act (the so-called Blockchain Act) was adopted by the Liechtenstein’s Parliament on October 3, 2019. https://www.regierung.li/media/medienarchiv/950_6_04_11_2019_TVTVG_english.pdf?t=1

mentioned: TT Protectors and Physical Validators; TT Exchange Service Providers; TT Verifying Authorities; and TT Price and Identity Service Providers.¹⁴ The Blockchain Act aims to improve investor protection, combat money laundering, and establish legal certainty in regulating blockchain projects.

The Swiss Confederation

The Swiss legal framework governing the activities of traditional banking (financial) services and FinTech firms consists of federal acts, implementing ordinances, a number of circulars, and guidance from the Financial Market Supervisory Authority (FINMA). More specifically, under the recent amendments to the Banking Act 2019, a new “FinTech license” has entered into force.¹⁵ FinTech related companies came into conflict with the Banking Act, as the acceptance of deposits from the public requires a banking license. Since the Banking Act places high demands regarding the granting of licenses, the banking license is a considerable barrier to market entry for FinTech companies.

The Swiss FinTech model now creates opportunities for all market participants, whether established financial service providers or startup companies. FINMA takes a fundamentally neutral stance towards new business models and technologies, and considers innovation as an important factor for the competitiveness of the Swiss financial market. At the same time, the Swiss standard-setter pays close attention to prudential and conduct supervision.¹⁶ Switzerland’s model is based on several core elements that are briefly described below.

- A FinTech license allows non-banking companies to accept deposits from the public and not conduct any lending business with maturity transformation or interest payments.
- The conditions to be fulfilled for obtaining a FinTech license are lower than for traditional banks¹⁷; deposits may not exceed a value of CHF 100 mln. and may not be reinvested; the minimum capital shall always be 3 % of the total amount of deposits held, but not less than CHF 300 000.
- A legal entity pursuant to Art. 1b of the Banking Act 2019 is subject to supervision by FINMA and must have certain requirements audited by an auditing company.

These requirements allow FinTech firms to successfully set up and compete with classic banks. Indeed, as of 21 April 2020, there is now a registered entity licensed by FINMA pursuant to Art. 1b of the Banking Act 2019¹⁸: Yapeal AG (<https://yapeal.ch/#intro>), the “neobank” registered in Zurich. Yapeal will offer accounts with Swiss IBAN without being tied to an offline bank payment system. With FINMA banking and securities dealer licenses, Sygnum and SEBA (<https://www.seba.swiss/>) banks are other examples of how traditional and innovative banking services can be combined. These “crypto banks” enable professional individuals and companies as well as institutional clients to invest, safely keep, trade, and borrow against digital and traditional assets, all in one space. For Swiss Blockchain companies they provide accounts and custody for fiat and digital assets. In addition, they are trying to issue their own digital currencies (e.g. Sygnum).

In this regard it is interesting how FinTech is regulated in Russia; Accordingly in the following paragraph we will analyze current trends and regulations of FinTech in Russia.

¹⁴ For more details see: Liechtenstein’s FMA. <https://www.fma-li.li/en/fintech-and-tvtg.html>

¹⁵ The Swiss Banking Act. (2019).

¹⁶ Swiss Financial Market Supervisory Authority (FINMA). (n.d.). Reports on key financial market issues. Supervisory reports. <https://www.finma.ch/en/documentation/finma-publications/reports/supervisory-reports/>

¹⁷ The Swiss Banking Act. (2019).

¹⁸ The list of persons licensed by FINMA (FinTech License) can be found on FINMA’s webpage. <https://www.finma.ch/en/search/>

Russian Trends and Regulations

The Russian FinTech market has been growing significantly for the past several years in terms of both the number of deals and the volume of investment.¹⁹ The Central Bank of Russia (CBR) issued “The Main Directions of Financial Technology Development for the Period 2018–2020” (the “Main Directions”) and the road map naming the key technologies. In particular, a blockchain-based platform is envisaged, with the corresponding marketplace having been set up. Various projects have been launched, and several documents enacted accordingly.

The regulation of payment systems has been updated; some examples of this would be Federal Law “On the National Payment System” No. 161-FZ of 27 June 2011 (the “NPS Law”), and Federal Law “On the Central Bank of the Russian Federation” No. 86-FZ of 10 July 2002 (the “CBR Law”), concerning relations between local money transfer operators and international payment services providers, anti-money laundering and some other matters. The localization of foreign services for GDPR reasons remains a hot topic (not all providers may extend their services to Russia properly — e.g. PayPal).

The progress is significant, though the legislation is yet to be updated in order to cope with technological development. The amendments are not always sufficient, and the regulator often takes a conservative approach. Regions are also participating in regulatory development and adopting new acts within the scope of competence. Some regions are very progressive (e.g. Tatarstan, the Moscow Oblast (Region), Kaliningrad), while others are much behind.

Digital Assets, Blockchain

There are three “blockchain” acts regulating this new technology application and use in the financial sector:

- The “*Digital Rights Act*” — Federal Law No. 34-FZ of 18 March 2019 “On Amendments to Parts One, Two and Article 1124 of Part Three of the Civil Code of the Russian Federation” (in force as of 01 October 2019);
- The “*Crowdfunding Act*” — Federal Law No. 259-FZ of 02 August 2019 “On Raising Investments Using Investment Platforms and Amendments to Certain Legislative Acts of the Russian Federation” (in force as of 01 January 2020);
- The “*DFA Act*” — Federal Law of 31.07.2020 Nr.259-FZ “On Digital Financial Assets, Cryptocurrency and Amendment of Separate Legal Acts of the Russian Federation (in force as of 01 January 2021).

Existing legal acts relating to issues such as securities markets (most significantly), banking and payment services, advertisement, consumer rights protection, information security, cyber security, and more still apply, working together with the above specific acts. Russia is surprisingly far behind regarding cryptocurrency and digital asset regulation. The first two acts have finally entered into force, but the main act regulating DFA issue and exchange, the DFA Act, governing digital tokens, cryptocurrencies, the circulation of crypto-assets, and market participant activities enters into force on 01 January 2021.

The legal grounds for the regulation of digital or blockchain based assets have been introduced step by step. The first important acknowledgement of a concept of “digital rights” was introduced in spring 2019 by an amendment of the Civil Code. The New Clause 141.1 “Digital Rights” has been introduced. The digital rights definition acknowledged some rights (rights of claim and other rights named in the law as such), if their content and terms of execution were determined by the rules

¹⁹ Agranovskaya, M. (2020, March 2). *FinTech law and practice in Russia*. In *FinTech 2020. Global practice guide*. Cambers and Partners. <https://practiceguides.chambers.com/practice-guides/fintech-2020/russia>

of an information system subject to characteristics provided for in the legislation. Operations and transactions with digital rights are only possible within the information system.

From that point on, reference was even given to the legal act from which the information system definition should be taken (there is more than one such act). The DFA Act has clarified that the definition of information shall be referred to the Federal Law of 27 July 2006 Nr. 149-FZ “On information, information technology and information protection”, just as the “information system operator”. It has to be noted that the definition of “*information*” is very broad, thus giving rise to a collision of the existing term of “digital currency” (limited in turnover as a mean of payment for goods and services) with bonuses, award miles, and the like.

The regulated area will cover only the DFA issue and exchange, and potential candidates may apply for licenses as of next year (with the Central Bank). No cryptocurrency exchanges, nor traders or depositaries, may be regulated yet. What is more, no payments are allowed for now in crypto for goods and services: this remains one of the most disputed areas of the business and the lawmakers.

There have not been any possibilities to receive a license and become a fully regulated player in the legal field for blockchain related businesses, including cryptocurrency exchanges, depositaries, token issuers, miners, or others, not to mention crypto-banks, crypto-funds, or insurance programs, until the year 2020. Many players have been present at the market (e.g., Huobi) through representative offices or operations involving foreign regulated entities run by Russian beneficiaries.

As regards operators of investment platforms, the CBR has already published Instruction No. 5342-U of 04 December 2019 “On the Way of Record Keeping for the Investment Platforms Operators”²⁰ and Instruction No. 5337-U of 02 December 2019 “On Requirements for the Internal Document(s) for Managing Conflicts of Interest of the Investment Platform Operator”.²¹ The theoretical base is there, but many definitions and explanations are absent.

The DFA Act has been a long-awaited subject of hot discussions. The final variant represents only a partial and incomplete set of solutions; the cryptocurrency market has been left out of its scope for now. This autumn the discussions are continuing, but the only aspect known for now is that crypto will not be allowed freely as a means of payment for goods and services. As has already been mentioned, a proper distinction from the digital miles and bonuses or non-documentary securities is for now absent. Together with that, a huge step forward has been made.

Digital assets classification: for now, they are classified (on the basis of all acts that have been enacted) as follows: *digital financial assets (DFA)*; *digital currency*; *utility digital rights (UDR)*.

DFA resemble security tokens when compared to more common divisions in Switzerland and other European countries, as well as Singapore. Their distinction from non-documentary securities is mainly based on the *technology first* principle (not dissimilarly to Malta). Existing securities laws apply, where applicable: in particular, the limitations relating to issues to be distributed to qualified investors. The Central Bank has wide discretion to expand the list of DFA that may only be issued to such investor community.

Digital currency definition is ambiguous and too broad, thus resulting in problems with award miles and e-commerce. It is defined as electronic data (digital code or reference) in an information system that are offered or may be accepted as means of payment subject to Rubles or foreign

²⁰ Ukazaniye Banka Rossii N 5342-U “O poryadke vedeniya reyestra operatorov investitsionnykh platform” [Bank of Russia Ordinance No. 5342-U “On the Procedure for Maintaining the Register of Investment Platform Operators”] (2019).

²¹ Ukazaniye Banka Rossii N 5337-U “O trebovaniyakh k vnutrennemu dokumentu (dokumentam) po upravleniyu konfliktami interesov operatora investitsionnoy platformy” [Bank of Russia Ordinance No. 5337-U “On Requirements for an Internal Document (Documents) for Managing Conflicts of Interest of an Investment Platform Operator”] (2019).

currency, should a person be absent liable to each owner of such data, except for an operator and (or) nodes of the system that are only responsible for the compliance of an issue of such data and entry of operations in the system according to its rules.

UDR are listed in Clause 8 of the Crowdfunding Act. They shall be circulating within the investment platform (being an information system per se):

- The right to claim vindication.
- The right to claim IP rights title transfer or the rights to use such.
- The right to claim that services are conveyed or works are done.

They have to arise within the platform as a digital right initially. Despite the similarity, they are not in practice utility tokens in the common understanding.

Currently the *regulated payers* include operators of investment platforms based on DLT (the Crowdfunding Act); information systems issuing digital financial assets (DFA Act); DFA exchange (DFA Act).

From 01 January, 2021, the issue of a new financial instrument in digital form (the DFA) or their exchange shall be made via the regulated operator. The conflict of the DFA Act with certain provisions of the Federal Law on the Securities Market²² and the Federal Law on Joint-Stock Companies²³ as well as with the Criminal and the Criminal Procedural Codes is obvious (Shashkova, 2019). The Act creates a kind of a surrogate as well of the digital securities market, and requires additional clarification work from the Central Bank.

In addition, it should be noted that CBR launched a sandbox in April 2018 in accordance with the Main Directions for piloting and modelling processes for new financial services and technologies in case the regulation needs amendment. The sandbox should encourage new financial services and technologies such as a system of fast payments, a unified system of biometric identification, and a financial supermarket. Together with this, the Central Bank is still taking a very rigid position as regards cryptocurrencies and their use in electronic commerce. No special licenses or permits have yet been introduced to allow mining or cryptocurrency exchange for Rubles, and the pending amendments to the legislation in discussion are not at their most positive at the moment.

An important new act has been passed: “On Experimental Legal Regimes in the Digital Innovation Field in Russia and on Amendments to Certain Legislative Acts of the Russian Federation”²⁴ (ELD Law). This allows legal sandbox-like exceptions for the new digital technology projects. The CBR is also recognized as the regulatory power for financial innovation. The CBR sandbox and the ELR Law procedures differ; it could be noted that the process and deadlines therein seem rather optimistic (e.g. 85 days for an application processing in general).

The Swiss FINMA example of forming the new legitimate field and attracting investments by reviewing projects on a case-by-case basis could be much more successful for Russia than vertically governed and lengthy legislative processes and their subsequent implementation, especially to cope with rapidly changing technology. Unfortunately, the regulator is not very active in Russia compared to those in Switzerland, Liechtenstein, Singapore, Malta, and other countries.

²² Federal Law on the Securities Market of the Russian Federation. (1996). Retrieved from Bank of Russia website: <https://www.cbr.ru/Content/Document/File/36165/39-FZ.pdf>

²³ Federal Law on Joint-Stock Companies of the Russian Federation. (1995). Retrieved from Bank of Russia website: <http://cbr.ru/Content/Document/File/33657/208-FZ.pdf>

²⁴ Federal'nyy zakon N 258-FZ “Ob eksperimental'nykh pravovykh rezhimakh v sfere tsifrovyykh innovatsiy v Rossiyskoy Federatsii” [Federal Law N 258-FZ “On Experimental Legal Regimes in the Field of Digital Innovation in the Russian Federation”] (2020).

Conclusion

The regulatory field had been poor for good crop until the year 2020. The new area of the financial market has been developing in an almost grey area. Court practice, tax authorities, and regulatory acts have often been contradictory. The regulator has not been actively supporting innovative products and businesses with private addresses for clarification of safe ways to work on the existing legislation basis. FINMA in Switzerland (just to mention the Libra related regulation on stablecoins), FMA in Lichtenstein, MAS in Singapore, and some other regulators have been active in creating the new legal regimes on the basis of the existing acts when working at private addresses: “how to do” approach instead of “we warn you and prohibit it”. In Russia this has not been the case, and few projects have gained support so far, even in the sandbox. Together with that, considering the regulatory sandbox activity and the enactment of new legislation and the active support of the business community, 2021 should prove a breakthrough year. Cryptocurrencies as a method of payment, and the use of DFA in payments as well as mining, however, are (so far) out of the legal field.

The DFA Act has not (as many had expected) created a comprehensive database for the classification and qualification of all digital assets nor a clear system of terminology. The definition of cryptocurrencies referred to above herein allows dangerous terminology competition with air miles, e-commerce certificates, or bonuses. Cryptocurrencies are so far legal but discouraged as a means of payment, while digital financial assets issue and crowdfunding have gained popularity as alternative sources of capital. Some terms do not require extra considerations as they are currently used in international practice. However, other new institutes to be implemented raise conflicts with the currently applied domestic workings — this refers to DFA as a term, for example.

The UDR in the Crowdfunding Act should in theory be commonly accepted utility tokens, but in reality the substance of this is different. Payment tokens do not exist as such; hybrid tokens are only allowed as DFA with other elements. DFA is the security token, whilst some UDRs may also be security tokens as they are described in particular regulations, such as (to give some examples) those issued in the aforementioned countries in Europe, just as in Gibraltar or in Singapore. Integration of this terminology within the global market may be a problem, but, at least, the legal grounds are there to start with.

At the same time, other legal developments relating to digitalization in the Russian Federation are said to be among the highest priorities of the State Duma and the Central Bank, together with other competence centers involved (like Skolkovo). Such directions as new financial instruments, information systems, information security, and transparency of process development are continuing further at full speed in Russia. The COVID-19 crisis — as any other crisis — shall exacerbate the named trends with the facilitation of the Russian political will, which has been highlighted in the Presidential Decree No. 204 of 7 May 2018 “On the National Goals and Strategic Tasks of the Russian Federation Development for the Period until 2024”²⁵, and in the National Digital Economy Programme that includes the current Normative Regulation of the Digital Sphere project. The Central Bank has issued the special road map for these, and the major competence centers, universities, and market players are very enthusiastic supporters of this activity, addressing the State Duma and the House of Parliament Chamber with initiatives via expert groups for specific areas. Political will is expected for further developments.

²⁵ Ukaz Prezidenta Rossiyskoy Federatsii № 204 [The President Decree No. 204] (2018).

References:

1. Allen, H. J. (2020). Experimental strategies for regulating FinTech. *Articles in Law Reviews & Other Academic Journals*, (696), 1–30. https://digitalcommons.wcl.american.edu/facsch_lawrev/696
2. Arner, D., Barberis, J., & Buckley, R. (2016). The evolution of FinTech: A new post-crisis paradigm? (Law Research Paper No. 2016–62). Sydney: University of New South Wales. <http://dx.doi.org/10.2139/ssrn.2676553>
3. Lifshits, I. M. (2016). Fenomen standard-setting bodies v mezhdunarodnom finansovom pravoporyadke [The phenomenon of standard-setting bodies in the international financial legal order]. In *Sumus Ubi Sumus. Mezhdunarodnoye pravo XXI veka: Mir i bezopasnost', sotrudnichestvo, prava cheloveka: Liber Amicorum v chest' prof. L. P. Anufriyevoy* [International law of the XXI century: Peace and security, cooperation, human rights: Liber amicorum in honor of prof. L. P. Anufrieva] (pp. 393–400). Moscow: Prospekt.
4. Kudryashova, E. (2019). Finansovaya bezopasnost' v ierarkhii tseley strategicheskogo planirovaniya v Rossiyskoy Federatsii [Financial safety within hierarchy of strategic planning purposes in Russian Federation]. *Pravo. Zhurnal Vysshey Shkoly Ekonomiki*, (2), 124–138. <http://doi.org/10.17323/2072-8166.2019.2.124.138>
5. Shashkova, A. V. (2019). Regulating principles of disclosure of information to shareholders under G20 / OECD principles. In K.S. Soliman, *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 1931–1936). International Business Information Management Association.

The authors' contribution:

Anna V. Shashkova – scientific editing, general formulation of research tasks.

Maria A. Agranovskaya – scientific editing, determination of research methodology.

David E. Kitsmarishvili – analysis of the trends of Russian FinTech market.

Вклад авторов:

Шашкова А.В. – научное редактирование, общая постановка исследовательских задач, определение методологии исследования.

Аграновская М.А. – научное редактирование, определение методологии исследования.

Кицмаришвили Д.Э. – определение направлений регулирования российского рынка FinTech.

Information about the authors:

Anna V. Shashkova – Dr. Sci. in Politics, Ph.D. in Law, Professor of Constitutional Law Chair, Moscow State Institute of International Relations (MGIMO-University), Honorary Consul for St. Vincent and the Grenadines in the Russian Federation, Attorney at Law, Executive MBA Supervisor in MGIMO School of Business and International Proficiency, Moscow, Russia.

a.shashkova@inno.mgimo.ru

Maria A. Agranovskaya – Attorney at Law, Managing Partner at GRAD Legal & Financial Advisory Services, expert in FinTech and international Law, invited lecturer in MGIMO-University, Plekhanov University, HSE, Moscow, Russia.

David E. Kitsmarishvili – Attorney at Law, GRAD Legal & Financial Advisory Services, invited lecturer in Russian Foreign Trade Academy, Moscow, Russia.

Сведения об авторах:

Шашкова А.В. — доктор политических наук, кандидат юридических наук, профессор кафедры конституционного права Московского государственного института международных отношений МГИМО МИД России, Почетный консул Сент-Винсента и Гренадин в Российской Федерации, адвокат, научный руководитель Executive MBA Школы бизнеса и международных компетенций МГИМО, Москва, Россия.

a.shashkova@inno.mgimo.ru

Аграновская М.А. — адвокат, управляющий партнер МКА «ГРАД»; эксперт в сфере FinTech и в области международного права, приглашенный преподаватель в МГИМО-университет, Российском экономическом университете им. Г.В. Плеханова, а также в НИУ «Высшая школа экономики», Москва, Россия.

Кицмаришвили Д.Э. — адвокат МКА «ГРАД», приглашенный преподаватель Всероссийской академии внешней торговли Министерства экономического развития Российской Федерации, Москва, Россия.

СТАТЬИ

ЭВОЛЮЦИЯ АНТИМОНОПОЛЬНОГО РЕГУЛИРОВАНИЯ В РОССИИ В ЦИФРОВУЮ ЭПОХУ

К.В. Тархова, В.И. Алифиров*, О.Н. Горохова

Юридическая фирма «АЛРУД»

125040, Россия, Москва, ул. Скаковая, д. 17, стр. 2

Аннотация

Статья посвящена комплексному анализу изменений в отечественном антимонопольном регулировании в связи с цифровизацией экономики. Цифровизация привела к повышению роли информации и цифровых платформ в деятельности компаний, размыванию географических границ цифровых рынков, а также к видоизменению структуры рынков в целом. Ключевыми факторами роста в современной экономике стали инновационные технологии, большие данные и объекты интеллектуальной собственности.

Авторами охарактеризованы новые нарушения антимонопольного законодательства в цифровую эпоху, в частности, сговоры на торгах, заключаемые с помощью аукционных роботов, и антиконкурентные эффекты, связанные с использованием программного обеспечения для осуществления мониторинга цен. Кроме того, в рамках статьи были проанализированы первые правовые позиции антимонопольного органа, касающиеся применения ценовых алгоритмов, а также рассмотрены новые подходы регулятора к анализу цифровых рынков на примере согласования сделок экономической концентрации с учетом сетевых эффектов и обладания большими данными и технологиями. В статье также исследуется первая практика применения трансфера технологий антимонопольным органом для снижения антиконкурентного влияния сделок экономической концентрации в России. Наконец, авторами изучены новые правовые нормы, регулирующие обязательную предварительную установку приложений российских разработчиков, и предпосылки для введения такого регулирования на территории России. При рассмотрении вышеуказанных вопросов авторами проанализировано действующее российское и зарубежное законодательство, проекты нормативно-правовых актов, а также правоприменительная практика Федеральной антимонопольной службы.

Новые подходы регулятора к анализу цифровых рынков в рамках антимонопольных расследований и согласования сделок экономической концентрации, а также автоматизация процессов выявления антимонопольных нарушений требуют повышенного внимания со стороны бизнеса. Компаниям рекомендуется учесть указанные тренды в своей деятельности, уделить им внимание в программах антимонопольного комплаенса, а также внедрить дополнительные меры для предотвращения возможных антимонопольных нарушений на цифровых рынках, в особенности, совершаемых с использованием ценовых алгоритмов.

Ключевые слова

большие данные, цифровые рынки, ценовые алгоритмы, сетевые эффекты, злоупотребление доминирующим положением, аукционные роботы, антимонопольное право, конкурентное право

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Для цитирования

Тархова, К. В., Алифиров, В. И., Горохова О. Н. (2020). Эволюция антимонопольного регулирования в России в цифровую эпоху. *Цифровое право*, 1(4), 38–55. <https://doi.org/10.38044/2686-9136-2020-1-4-38-55>

* Автор, ответственный за переписку

Поступила: 19.10.2020, принята в печать: 27.11.2020, опубликована: 20.12.2020

ARTICLES

THE EVOLUTION OF ANTITRUST REGULATION IN RUSSIA IN THE DIGITAL ERA

Ksenia V. Tarkhova, Vladislav I. Alifirov*, Olga N. Gorokhova

ALRUD Law Firm

2–17, Skakovaya str., Moscow, Russia, 125040

Abstract

The article includes a comprehensive analysis of changes that have been taking place in Russian antitrust enforcement in response to the digitalization of the economy. Digitalization has led to increase of the role of information and digital platforms in day-to-day business activities of the market players. Digitalization vanished geographical boundaries of the digital markets and modified market structures in general. Innovative technologies, big data, and intellectual property have become the key drivers of economic growth.

The authors analyze new violations of antimonopoly legislation in the digital era (in particular collusive tendering using auction robots), the anticompetitive effects resulting from the use of pricing algorithms, and the first approaches of the antitrust authority to regulations of the algorithmic pricing. In addition, within the framework of this article, the first legal positions of the antitrust authority regarding the use of pricing algorithms, as well as the new approaches of the regulator to the analysis of digital markets in merger control are considered, taking into account such factors as network effects, big data and technologies. Moreover, the authors analyze the first practice of using the technology transfer as a remedy in merger control by the antitrust authority to mitigate anti-competitive effects of the transactions planned in the Russian market. Finally, the authors conduct an overview of the new legal provisions governing the mandatory pre-installation of applications by Russian developers, and also describe the background for this initiative. When considering the above topics, the authors deeply analyze the relevant Russian and foreign legislation, draft laws, and the law enforcement practice of the Federal Antimonopoly Service.

New approaches of the regulator to the analysis of digital markets in the framework of antitrust investigations and merger control, as well as automation of the processes of detecting antitrust violations, demand more attention from market players. Companies are encouraged to take these trends into account in their business activities, reflect them in antitrust compliance programs, as well as implement additional measures to prevent potential antitrust violations in digital markets, in particular, committed with the use of pricing algorithms.

Keywords

big data, digital markets, pricing software, network effects, abuse of dominance, auction robots, antitrust law, competition law

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study had no sponsorship.
For citation	Tarkhova, K. V., Alifirov, V. I., & Gorokhova, O. N. (2020). The evolution of antitrust regulation in Russia in digital era. <i>Digital Law Journal</i> , 1(4), 38–55. https://doi.org/10.38044/2686-9136-2020-1-4-38-55

* Corresponding author

Submitted: 19 Oct. 2020, accepted: 27 Nov. 2020, published: 20 Dec. 2020

Цифровизация охватила экономики всех развитых и большинства развивающихся стран, а также повлияла на деятельность компаний, ведущих бизнес в России. Как подчеркнула Федеральная антимонопольная служба (далее — ФАС России), динамично меняющиеся рынки становятся все более сложными и цифровыми¹. На практике регулятор готов рассматривать практически любую компанию как цифровую, например, если она (1) обрабатывает или хранит большие данные, базы данных клиентов или иную информацию; (2) использует цифровые алгоритмы для изучения конкурентной среды, планирования своей бизнес-стратегии на рынке или мониторинга деятельности своих дистрибьюторов; (3) разрабатывает и производит любые продукты с использованием больших данных и инновационных технологий. При этом особое внимание ФАС России привлекают глобальные цифровые корпорации и их практики поведения на российском рынке, что следует из анализа недавно рассмотренных антимонопольной службой значимых дел.

Кроме того, цифровизация привела к стиранию географических границ товарных рынков. Транзакционные издержки стремятся к нулю, и цифровые услуги способны мгновенно доставляться в любую точку мира по желанию клиента. Наряду с изменением географических границ меняются и факторы, определяющие рыночную власть компаний. Так ключевыми факторами экономического роста в современной экономике становятся инновационные технологии, большие данные и интеллектуальная собственность.

Несмотря на то, что действующее антимонопольное законодательство распространяется, в том числе и на цифровые рынки (с учетом некоторых оговорок, касающихся антимонопольных «IP иммунитетов»), объективно назрела необходимость его доработки для повышения эффективности антимонопольного регулирования на цифровых рынках (Egorova, 2018). Законодательство не успевает за изменениями, связанными с цифровизацией экономики, поэтому ФАС России вынуждена в своей правоприменительной практике разрабатывать и тестировать новые механизмы антимонопольного регулирования для предотвращения различных нарушений на цифровых рынках и эффективного рассмотрения сделок фактически еще до того, как эти механизмы закрепляются на законодательном уровне.

Задачи настоящей статьи состоят в том, чтобы обобщить тренды правоприменительной практики антимонопольного органа, а также системно изложить вытекающие из указанных трендов законодательные инициативы, влияющие на экономику страны и деятельность компаний на территории России.

¹ Федеральная антимонопольная служба. (2019, ноябрь 18). ФАС в СМИ: «Раньше слияния цифровых гигантов никто не контролировал». <https://fas.gov.ru/publications/19760>

Сговоры на торгах, заключаемые посредством аукционных роботов

«Пресечение новых форм нарушений является вызовом для антимонопольного регулирования. Антимонопольные органы должны уравновесить прогресс в техническом оснащении участников картеля и современные методы сбора и анализа информации и доказывания нарушений. Также представляется необходимым реформирование законодательства», — так заместитель руководителя ФАС России А. Г. Цыганов обосновывает необходимость совершенствования борьбы с картелями в условиях цифровой экономики².

Безусловно, электронные торги имеют положительный эффект для рынка в целом, а также их проведение направлено на обеспечение конкуренции, активизацию экономических процессов и защиту интересов участников торгов (Belickája et al., 2019). Вместе с тем по данным ФАС России за 2019 г. 87 % возбужденных дел об антиконкурентных соглашениях (320 дел) составили сговоры на торгах (картели и сговоры с заказчиком (организатором) торгов)³. На протяжении последних нескольких лет участники антиконкурентных соглашений все чаще используют различные инновационные решения для заключения и реализации сговоров на торгах. ФАС России уже расследовала порядка 20 дел о картелях на торгах в различных регионах России, заключаемых с использованием специального программного обеспечения — аукционных роботов⁴.

Аукционный робот — это программное обеспечение, функционал личного кабинета участника аукциона на электронной площадке, позволяющий подавать заявки, делать ставки, выполнять другие действия в заранее определенное время в автоматическом режиме для участия в торгах. Подобный робот позволяет компаниям устанавливать частоту подачи заявок и размер ставки, а также иные характеристики аукционной стратегии. Когда конкуренты, участвующие в торгах, используют аукционных роботов, адаптированных друг к другу, подобная практика может позволить им устанавливать и поддерживать цены на торгах. ФАС России склонна квалифицировать подобные действия как картели.

Различают два вида аукционных роботов: легальные и нелегальные. Легальные аукционные роботы интегрированы в интерфейс электронных торговых площадок, позволяя участникам торгов эффективнее делать предложения о цене контракта в автоматизированном режиме, экономя свое время и усилия. Вместе с тем недобросовестные участники оборота могут использовать такие программные модули в качестве инструмента нарушения антимонопольного законодательства, используя специфические настройки для синхронизации своей стратегии на торгах с поведением конкурентов. В таких случаях доказательствами участия в антиконкурентном соглашении могут послужить одинаковые параметры аукционных роботов (предельное значение цены, ниже которой нельзя опускаться, шаг аукциона), а также факт их активации/деактивации⁵. Нелегальные аукционные роботы, напротив, являются сторонними программами, функционирующими через прокси-серверы и при помощи программ-проксификаторов (Tenishev & Teslenko, 2019).

² Федеральная антимонопольная служба. (2018, сентябрь 13). Андрей Цыганов: Пресечение цифровых форм нарушений — новый вызов для антимонопольного регулирования. <https://fas.gov.ru/news/25854>

³ Федеральная антимонопольная служба. (2020, август 27). Доклад о состоянии конкуренции в Российской Федерации за 2019 г. <https://fas.gov.ru/documents/687048>

⁴ Федеральная антимонопольная служба. (2019, сентябрь 18). Андрей Цыганов: В раскрытии сговоров на торгах ФАС активно использует анализ открытых источников данных. <https://fas.gov.ru/news/30480>

⁵ Решение УФАС по Мурманской области по делу № 05-03-16/6 (2016).

Практика ФАС России по рассмотрению дел об антиконкурентных соглашениях, заключенных с использованием аукционных роботов, активно развивается. Так, поставщики медицинских материалов для государственных больниц ООО «Валирия» и ООО «Эгамед»⁶ использовали аукционных роботов, встроенных в интерфейс электронной торговой площадки ЗАО «Сбербанк-АСТ» и настроенных на поддержание цен на торгах. Участники картеля заранее настроили аукционных роботов таким образом, чтобы у них был одинаковый лимит снижения цены, а также одинаковые ценовые предложения, подаваемые с разницей в 0,003 секунды. В 2018 г. ФАС России признала компании виновными в заключении картеля на торгах, направленного на поддержание цен.

Другим известным примером антимонопольного нарушения, совершенного с использованием аукционных роботов, стало первое антимонопольное дело о картеле на бирже. Так, АО «Солид — товарные рынки» и ООО «А-ОЙЛ»⁷ были признаны виновными в заключении картельного соглашения на биржевых торгах нефтепродуктами в 2018 г. 26 октября 2020 г. Верховный Суд Российской Федерации поддержал позицию ФАС России, отказав АО «Солид — товарные рынки» в передаче кассационной жалобы в Судебную коллегия по экономическим спорам Верховного Суда Российской Федерации⁸.

Экс-руководитель ФАС России И. Ю. Артемьев выражал позицию, что «роботы действуют самостоятельно в сети интернет, сами заключают горизонтальные соглашения, которые приводят к росту цен»⁹. Он подтверждал, что ФАС России имеет технические средства, позволяющие обнаруживать не только «сговорившихся» роботов, но и стоящих за ними лиц, чтобы привлечь их к ответственности. Так, ФАС России разработала комплексное автоматизированное решение для выявления и доказательства картелей — веб-сервис «Большой цифровой кот»¹⁰.

Скрининговый сервис в автоматическом режиме анализирует данные в открытом доступе (например, в единой информационной системе в сфере закупок, СМИ) и закрытые сведения (например, в базах данных Федеральной налоговой службы) на предмет соответствия заданным критериям с помощью алгоритмов; выявляет сговоры на торгах на основе проведенного анализа и формирует доказательную базу¹¹. Кроме того, в рамках данной программы ФАС России развивает функцию скоринга — просчёта вероятности наличия сговора в процентах. Первый модуль программы, связанный с анализом данных в единой информационной системе в сфере закупок, уже запущен и активно применяется ФАС России для выявления сговоров на торгах с 2019 г.¹² При этом «Большой цифровой кот» постоянно обновляется и модернизируется с помощью современных технологий.

Таким образом, в настоящее время регулятором все активнее разрабатываются меры, направленные на борьбу с использованием аукционных роботов для заключения сговоров на торгах. В свою очередь, автоматизация расследований, проводимых антимонопольной

⁶ Решение по делу № 1-11-166/00-22-17 (2018).

⁷ Определение Верховного Суда РФ по делу № 1-11-13/00-22-19 (2020).

⁸ Определение Верховного Суда Российской Федерации № 305-ЭС20-13656 (2020).

⁹ Гайва, Е. (2019, май 20). *Картель роботов. ФАС выявила новые формы сговоров*. Российская газета. <https://rg.ru/2019/05/20/reg-cfo/fas-vyavila-novye-formy-monopolizacii-rynka.html>

¹⁰ Федеральная антимонопольная служба. (2018, октябрь 18). *ФАС создает веб-сервис «Большой цифровой кот»*. <https://fas.gov.ru/news/26154>

¹¹ Федеральная антимонопольная служба. (2019, сентябрь 18). *Андрей Цыганов: В раскрытии сговоров на торгах ФАС активно использует анализ открытых источников данных*. <https://fas.gov.ru/news/30480>

¹² Федеральная антимонопольная служба. (2019, ноябрь 20). *Цифровой кот подрос и обрел «лицо»*. <https://fas.gov.ru/news/28865>

службой, повышает риски для бизнеса. В связи с этим, компаниям, принимающим регулярное участие в торгах, для снижения антимонопольных рисков рекомендуется уделять особое внимание информированию своих сотрудников о том, в каких случаях использование программного обеспечения на торгах может иметь признаки нарушения антимонопольного законодательства. Более того, может быть полезен предварительный аудит юридической службой программного обеспечения, которое сотрудники компании планируют использовать на торгах, а также планируемых настроек такого программного обеспечения, отражающих намеченную стратегию автоматического участия в торгах.

Риски нарушения антимонопольного законодательства, связанные с использованием ценовых алгоритмов

Помимо аукционных роботов, сфера применения которых ограничивается торгами, компании начали использовать специальное программное обеспечение и онлайн-платформы, позволяющие им анализировать конкурентную среду и в короткие сроки адаптировать свои бизнес-стратегии к изменениям на рынке.

С одной стороны, мониторинг параметров рынка для выработки ценовой стратегии хозяйствующего субъекта необходим для эффективного ведения бизнеса любой компанией (Kozhina & Artjushenko, 2019). С другой стороны, прозрачность информации о ценах (интернет-магазины, общедоступные рекомендуемые цены и т. д.) и наличие цифровых инструментов для сбора и обработки этих данных из открытых источников создают благоприятную среду для заключения антиконкурентных соглашений, осуществления согласованных действий и антиконкурентной координации экономической деятельности хозяйствующих субъектов (Abramov, 2020). Например, если два конкурента, реализующие товары через Интернет, запускают программное обеспечение, позволяющее отслеживать цены друг друга и немедленно адаптировать их уровень относительно установленного на рынке, экономический эффект от использования подобного программного обеспечения и действий на рынке может оказаться в результате таким же, как в случае прямого заключения картеля между компаниями-конкурентами, а именно — установление и поддержание цен.

Позиции антимонопольных регуляторов по данному вопросу раскрываются в отдельных разъяснениях об использовании алгоритмов и расследовании сговоров на рынке (“Algorithms and Collusion — Note from the European Union”¹³ и “Algorithms and Collusion — Summaries of Contributions”¹⁴) (далее — Разъяснения), изданных Организацией экономического сотрудничества и развития (далее — ОЭСР).

Так, ценовые алгоритмы признаются допустимой практикой, анализ которой основывается на двух важных принципах. Во-первых, если методы ценообразования признаются незаконными при их использовании «офлайн» (например, заключение антиконкурентных соглашений по установлению одинаковых цен после личного наблюдения за ценами; покупки данных о ценах у специализированных поставщиков или сбора информации от клиентов, которые сообщают

¹³ Directorate for Financial and Enterprise Affairs Competition Committee. (2017, June 21–23). *Algorithms and Collusion — Note from the European Union*. Organisation for Economic Co-operation and Development. [https://one.oecd.org/document/DAF/COMP/WD\(2017\)12/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf)

¹⁴ Directorate for Financial and Enterprise Affairs Competition Committee. (2017, June 21–23). *Algorithms and Collusion — Summaries of Contribution*. Organisation for Economic Co-operation and Development. [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD\(2017\)2&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD(2017)2&docLanguage=En)

о лучших предложениях у иных производителей), то велика вероятность того, что они будут являться незаконными и при их использовании в Интернете.

Во-вторых, компании, вовлеченные в незаконные практики ценообразования, не могут избежать ответственности лишь на том основании, что их цены были определены ценовыми алгоритмами. Подобно сотруднику или внешнему консультанту, работающему под «руководством или контролем» компании, ценовые алгоритмы остаются под ее контролем, поэтому компания несет ответственность за их действия как за свои. При этом ценовые алгоритмы рассматриваются как средство совершения правонарушения. В вертикальных соглашениях ценовые алгоритмы могут использоваться поставщиками для установления и контроля за соблюдением фиксированных и минимальных цен перепродажи, установление которых является антимонопольным нарушением. В горизонтальных соглашениях ценовые алгоритмы могут использоваться для отслеживания согласованных цен в рамках реализации сговора, а также в качестве средства коммуникации и информирования участников соглашения о действиях на рынке. Кроме того, использование ценовых алгоритмов может учитываться Европейской комиссией в качествеотягчающего обстоятельства при назначении размера штрафа за совершенное противоправное деяние.

В России использование ценовых алгоритмов само по себе также не является нарушением антимонопольного законодательства, если такое использование не содержит состава одного из существующих антимонопольных нарушений. При этом, как следует из доклада «Алгоритмы и сговоры», опубликованного ФАС России в июне 2017 г.¹⁵, регулятор впервые заинтересовался проблемой ценовых алгоритмов еще в 2016 г., направив соответствующие запросы участникам рынка и одному из разработчиков подобных программных продуктов. В результате проведенного исследования ФАС России выделила четыре группы ценовых алгоритмов в зависимости от их функциональности и целей. Итак, выделяют следующие виды алгоритмов, направленные на:

1. Сбор и / или анализ информации о ценах конкурентов, об ассортименте и иной информации.
2. Автоматический расчёт цен и / или автоматическое установление цен на основании загруженных пользователем данных.
3. Сбор и / или анализ информации о ценах конкурентов, об ассортименте и иной информации и автоматический расчёт цен и / или автоматическое установление цен на основании собранных программным продуктом данных.
4. Сбор и / или анализ информации о ценах реселлеров на продукцию конкретных брендов, автоматическое сопоставление розничных цен с рекомендованными / минимальными ценами (в отличие от перечисленных выше, данные программные продукты используются вендорами для контроля розничных цен реселлеров на продукцию брендов).

При этом антимонопольный орган указывает, что наибольшие опасения вызывает использование ценовых алгоритмов, описанных в пунктах 3 и 4, поскольку может быть потенциально связано с координацией экономической деятельности, приводящей к ограничению конкуренции. Впоследствии ФАС России подтвердила данные теоретические выводы в своей правоприменительной практике.

Так, в 2018 г. ФАС России рассмотрела дело в отношении российской дочерней компании LG Electronics Inc. о координации экономической деятельности реселлеров, которая привела

¹⁵ Комитет по конкуренции ФАС России. (2017, июнь). *Алгоритмы и сговоры*. Федеральная антимонопольная служба. <http://fas.gov.ru/attachment/192263/download?1549357072>

к установлению и поддержанию розничных цен на отдельные модели смартфонов бренда LG¹⁶. Как следует из решения ФАС России, представители компании указывали своим дистрибьюторам на необходимость увеличить розничные цены на смартфоны до рекомендованного уровня на основании автоматических отчетов об отклонении цен от рекомендованного уровня, подготовленных с помощью специального программного обеспечения.

Это был первый случай, когда ФАС России проанализировала использование программного обеспечения для осуществления мониторинга цен в рамках дела о нарушении антимонопольного законодательства. По итогам рассмотрения дела ФАС России пришла к следующему выводу относительно возможности использования ценовых алгоритмов: «Комиссия ФАС России отмечает, что использование ценовых алгоритмов <...> само по себе не является нарушением антимонопольного законодательства. Однако в рассматриваемом деле характер использования таких ценовых алгоритмов оценивается как обстоятельство, способствовавшее совершению <...> противоправных действий».

При этом под «способствованием» антимонопольный орган имеет в виду фактическое расширение масштабов совершеняемого правонарушения путем автоматизации и ускорения процессов мониторинга и контроля за уровнем цен. Однако действующая редакция Кодекса об административных правонарушениях РФ (далее — КоАП РФ) не позволяет рассматривать использование ценовых алгоритмов в качествеотягчающего обстоятельства при совершении антимонопольных нарушений, поскольку установленный КоАП РФ перечень отягчающих обстоятельств является закрытым. На начальном этапе обсуждения проекта Пятого антимонопольного пакета¹⁷ предлагалось внести использование ценовых алгоритмов в перечень отягчающих обстоятельств в КоАП РФ, однако впоследствии ФАС России отказалась от этой идеи.

В 2019 г. ФАС России рассмотрела аналогичное дело и в отношении российской дочерней компании Samsung Electronics¹⁸. По результатам проведенных расследований ФАС России выпустила Рекомендацию «О практиках в сфере использования информационных технологий в торговле, в том числе связанных с использованием ценовых алгоритмов» (далее — Рекомендация), которые были впоследствии одобрены Методическим советом ФАС России и Президиумом ФАС России¹⁹.

В Рекомендациях содержится определение «ценового алгоритма». Так, ценовой алгоритм представляет собой программный продукт, используемый для определения цен на товары, с использованием которого осуществляется расчет и (или) установление и (или) мониторинг цен, исходя из параметров, определяемых пользователем алгоритма.

Рекомендациями установлено, что само по себе использование информационных технологий в хозяйственной деятельности, если оно не влечет нарушения запретов, установленных Федеральным законом «О защите конкуренции» № 135-ФЗ от 26 июля 2006 г. (далее — Закон о защите конкуренции), должно признаваться допустимым. Кроме того, в Рекомендациях содержится открытый перечень допустимых целей осуществления мониторинга розничных цен, в частности:

¹⁶ Решение ФАС России по делу № 1-11-18/00-22-17 (2018).

¹⁷ Проект 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>

¹⁸ Решение ФАС России по делу № АЦ/37701/19 (2019).

¹⁹ Федеральная антимонопольная служба. (2019, март 18). Рекомендации «О практиках в сфере использования информационных технологий в торговле, в том числе связанных с использованием ценовых алгоритмов». <https://fas.gov.ru/documents/684828>

1. Сравнение с ценами на конкурирующий товар для определения спроса и окупаемости затрат на реализацию товара.
2. Сравнение с ценами на аналогичный товар, установленными конкурентами реселлера (продавца).
3. Контроль за соблюдением установленного соглашением реселлера и вендора либо дистрибьютора условия о максимальной цене перепродажи товара.
4. Соблюдение согласованных условий приобретения рекламных или маркетинговых услуг (в том числе, для повышения спроса на товар, например, с целью контроля за предоставлением минимальной скидки конечному потребителю).

Более того, приводятся примеры недопустимых практик, основанные на действующих запретах Закона о защите конкуренции, включая:

1. Установление и контроль за соблюдением минимальных или фиксированных розничных цен (в том числе посредством автоматизированных уведомлений о нарушении установленного уровня цен, наложения штрафов / иных санкций, установления ограничений к приобретению продукции или предоставления стимулов к поддержанию установленного уровня минимальных розничных цен).
2. Координация вендором третьих лиц с целью поддержания фиксированного или минимального уровня цен.
3. Установление запрета вендором к применению реселлерами скидок к розничной цене товаров или ограничение максимального размера скидок к розничной цене, которые может предоставить реселлер на соответствующий товар (в том числе, путем установления штрафных санкций, ограничения поставки товаров, досрочного расторжения договора).

Таким образом, ФАС России активно развивает правоприменительную практику в сфере расследования антимонопольных нарушений, совершенных с использованием программного обеспечения для осуществления мониторинга цен и иных ценовых алгоритмов. Это означает, что компаниям следует более тщательно анализировать последствия использования ценовых алгоритмов в своей повседневной деятельности, чтобы предотвратить потенциальные риски совершения антимонопольных правонарушений.

В качестве конкретных мер для предотвращения использования ценовых алгоритмов сотрудниками компании в качестве средств совершения антимонопольных правонарушений могут использоваться: включение информации о рисках использования ценовых алгоритмов в программы тренингов по антимонопольному комплаенсу; предварительный детальный аудит юридической службой функционала любого планируемого к внедрению программного обеспечения в сфере мониторинга или формирования цен; разработка систем контроля за использованием сотрудниками существующих ценовых алгоритмов (например, выборочный аудит рабочей переписки таких сотрудников для выявления признаков антимонопольных нарушений).

Новые подходы регулятора к анализу рынка на примере рассмотрения сделок экономической концентрации

Цифровизация экономики неразрывно связана с ростом глобальных цифровых гигантов и усилением их рыночной власти, что зачастую приводит к монополизации товарных рынков и создает предпосылки для совершения антимонопольных нарушений. Данная глобальная тенденция в равной степени актуальна и для России.

В условиях цифровой экономики, анализируя рынки и оценивая рыночную власть компаний, антимонопольному органу приходится все чаще уделять повышенное внимание не только количественным (доли компаний на рассматриваемом рынке), но и качественным критериям. К ним относятся, в том числе, сетевые эффекты, доли компаний на связанных рынках, обладание большими данными и технологиями, объем инвестиций в инновации и другие факторы, которые могут создавать преимущества для определенных компаний и влиять на состояние конкуренции на рассматриваемых рынках. Так, например, обширные базы данных усиливают рыночную власть правообладателя, позволяя ему не только повышать эффективность своей деятельности, предлагая потребителям сопутствующие и смежные товары, работы, услуги, но и удерживать потребителей, создавая антиконкурентные ограничения (Popondopulo et al., 2019).

Впервые ФАС России столкнулась с необходимостью учета новых факторов рыночной власти при рассмотрении сделки Bayer / Monsanto²⁰. По мнению ФАС России, сделка оказывала влияние на социально значимые рынки, определяющие продовольственную безопасность государства, и приводила к радикальной трансформации агропромышленного комплекса, что, несомненно, требовало более детального анализа не только деятельности компаний и пересечений на рынках, но и условий функционирования экономики и данных рынков в глобальном масштабе.

При рассмотрении сделки ФАС России отошла от традиционного подхода к анализу рынка, основанному на оценке рыночных долей участников сделки, и сконцентрировалась на исследовании больших данных, цифровых платформ и технологий в качестве ключевых факторов рыночной власти сторон сделки.

Несмотря на наличие пересечений в деятельности сторон исключительно на рынках семян и средств защиты растений, ФАС России пришла к выводу, что потенциальные антиконкурентные эффекты от сделки возникали, в первую очередь, вследствие владения обеими компаниями знаниями, инновациями, цифровыми платформами, алгоритмами и технологиями, позволявшими им влиять на рыночные условия, создавать барьеры входа на рынок для других игроков и диктовать условия дальнейшего развития агропромышленного комплекса. В результате проведенного анализа ФАС России были выявлены следующие основные риски ограничения конкуренции ввиду совершения планируемой сделки: (1) риск создания закрытой цифровой платформы, которая могла заблокировать выход на рынок новых конкурентоспособных цифровых решений; (2) снижение инновационной активности других игроков рынка в области цифрового сельского хозяйства; (3) возникновение новых и усиление действующих барьеров входа на рынки; (4) повышение вероятности того, что объединенная компания будет злоупотреблять доминирующим положением; и (5) усиление стимулов для антиконкурентных согласованных действий и соглашений после совершения сделки. В результате сделка была согласована с выдчей обширного предписания, основным требованием которого стала организация трансфера технологий российским конкурентам (подробнее оно будет проанализировано в следующем разделе настоящей статьи).

Следующим ярким примером применения ФАС России новых подходов к анализу рынка является сделка Yandex / Uber²¹, направленная на заключение соглашения о совместной деятельности между двумя ключевыми игроками на российском рынке онлайн-агрегаторов такси (определен ФАС России как «рынок услуг информационного взаимодействия пассажиров и водителей для заказа такси через мобильное приложение»).

²⁰ Решение ФАС России по делу № ИА/28180/18 (2018).

²¹ Решение ФАС России по делу №АГ/82029/17 (2017).

В ходе анализа вышеуказанной сделки ФАС России изучила сетевые эффекты, влияющие на рыночную власть сторон и усиливающиеся в результате заключения соглашения о совместной деятельности (чем больше пассажиров присоединяется к приложению, тем оно становится привлекательнее для водителей; в свою очередь, чем больше водителей присоединяются к приложению, тем удобнее оно становится для пассажиров). В результате ФАС России пришла к выводу, что сделка может привести к ограничению конкуренции, и согласовала ее с выдачей поведенческого предписания, направленного на обеспечение безопасности поездок, а также закрепление возможности водителей и пассажиров пользоваться различными агрегаторами такси одновременно.

Концепции, примененные при анализе недавних громких сделок экономической концентрации на цифровых рынках (оценка влияния больших данных, цифровых платформ и сетевых эффектов на рыночную власть участников сделки), легли в основу подготовленного ФАС России проекта поправок в действующее антимонопольное законодательство — Пятого антимонопольного пакета²², который находится в настоящее время на стадии разработки.

В частности, законопроект обязывает ФАС России учитывать сетевые эффекты при анализе конкуренции на цифровых рынках. Под «сетевыми эффектами» в законопроекте понимается зависимость потребительской ценности товара от количества пользователей одной и той же группы (прямой сетевой эффект) либо изменение ценности товара для одной группы пользователей при уменьшении или увеличении количества пользователей в другой группе (косвенный сетевой эффект).

Помимо этого, законопроект содержит ряд положений, направленных на совершенствование режима контроля за экономической концентрацией в цифровую эпоху. В частности, в дополнение к существующим пороговым значениям, приводящим к необходимости согласования сделок экономической концентрации, а именно размеру выручки и активов участников сделки (их групп лиц), проект вводит такой дополнительный критерий, как объем сделки. Предполагается, что в случае, если объем сделки превысит 7 миллиардов рублей, то финансовые пороги для ее согласования с ФАС России будут соблюдены. Данная норма направлена в первую очередь на решение проблемы антиконкурентного поглощения стартапов, которой обеспокоена ФАС России²³. С учетом действующих порогов подобные сделки зачастую не подпадают под необходимость согласования, что лишает ФАС России возможности оценить их влияние на российский рынок и потенциальные антиконкурентные эффекты.

Наконец, Пятый антимонопольный пакет создает правовую базу для уже применявшейся ранее практики «трансфера технологий» в рамках выдаваемых ФАС России предписаний (подробнее описывается далее в настоящей статье), вводит институт «доверенного лица» для контроля за исполнением обязательств, а также совершенствует ряд процедурных аспектов рассмотрения сделок экономической концентрации (предусматривает возможности дополнительного продления сроков рассмотрения значимых трансграничных сделок, вводит институт «экспертов» и устанавливает порядок их привлечения и т. д.).

Таким образом, совершенствование подходов к анализу цифровых рынков с учетом сетевых эффектов, цифровых платформ и больших данных является одним из приоритетов ФАС России, что выражается в недавней правоприменительной практике и новых законодательных

²² Проект 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>

²³ Федеральная антимонопольная служба. (2020, июнь 18). *Поглощения стартапов попадут в поле зрения ФАС*. <https://fas.gov.ru/news/29978>

инициативах. Важно отметить, что аналогичные подходы применяются регулятором также при анализе цифровых рынков по делам о нарушении антимонопольного законодательства.

В связи с этим, компаниям, ведущим деятельность на цифровых рынках, рекомендуется заранее учитывать подходы регулятора при оценке возможности признания компании, занимающей доминирующее положение на российском рынке (что влечет необходимость соблюдения запретов, установленных ст. 10 Закона о защите конкуренции, и влияет на процесс согласования сделок экономической концентрации с участием таких компаний). Достаточное внимание к проблеме позволит корректно выявить и оценить антимонопольные риски в деятельности цифровой компании и принять своевременные меры для их снижения, либо разработать эффективную стратегию согласования сделки, в случаях, когда речь идет о сделках экономической концентрации.

Трансфер технологий как новая мера при согласовании сделок экономической концентрации

В последние годы в России наметилась сильная тенденция к поддержке отечественных производителей и импортозамещению на территории России. Кроме того, регуляторы все чаще стали отмечать наличие некоторого технологического отставания в отдельных отраслях российской экономики, в особенности, в промышленном секторе, на устранение которого должна быть направлена деятельность государственных органов и компаний в целом. Для устранения указанных проблем и для целей обеспечения технологического прогресса на территории России российские регуляторы начали вести переговоры с иностранными инвесторами о возможности передачи определенных технологий российским производителям с целью развития конкуренции и поддержания российских рынков в качестве условия согласования сделок, совершаемых данными инвесторами.

Между тем, идея трансфера технологий в рамках сделок экономической концентрации не является абсолютной новеллой в мировой практике антимонопольного регулирования. Так, китайские регуляторы активно применяют трансфер технологий в качестве обязательного условия для согласования определенных сделок, совершаемых иностранными инвесторами (в особенности, когда речь идет о создании совместных предприятий с участием иностранных инвесторов и китайских партнеров)²⁴.

Впервые ФАС России реализовала концепцию трансфера технологий при согласовании сделки Bayer / Monsanto²⁵. По итогам ее рассмотрения ФАС России выдала компаниям предписание о совершении мер, направленных на развитие конкуренции в агротехнологическом секторе России путем укрепления потенциальной конкуренции со стороны российских компаний за счет обеспечения доступа третьих лиц (российских участников рынка) к определенным технологиям и базам данных компаний. Согласно предписанию Bayer должна была обеспечить технологический трансфер молекулярных средств селекции и гермоплазмы (генные ресурсы семенного материала, ответственные за передачу наследственности), необходимых для создания высокопродуктивных семян сельскохозяйственных культур, обладающих

²⁴ European Commission. (2018, December 21). *China – Certain measures on the transfer of technology – Request for consultations by the European Union*. https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157591.12.20%20-%20REV%20consultation%20request%20FINAL.pdf

²⁵ Bayer. Россия и СНГ. (2018, апрель 20). *ФАС согласовала сделку по слиянию Bayer и Monsanto на территории РФ*. https://www.bayer.ru/media/news/20182004_monsanto_bayer_agreed.php

заданными свойствами. Помимо этого, Bayer была обязана предоставить недискриминационный доступ к цифровым платформам точного земледелия, в том числе доступ к историческим данным, относимым к России, а также к данным, которые будут собираться компанией Bayer после коммерциализации компанией своих программных продуктов на территории России. Доступ к таким данным является ключевым фактором для разработки и внедрения российскими компаниями своих IT-разработок в области точного земледелия с учетом уже существующих наработок. Кроме того, выданное предписание включало требование о создании Центра технологического трансфера на базе Национального исследовательского университета «Высшая школа экономики»²⁶, назначенного доверенным лицом для мониторинга исполнения предписания, и организацию обучения российских специалистов в данной области.

Центр технологического трансфера уже ведет активную деятельность, реализуя предписание ФАС России²⁷. Так, для получения гермоплазмы сельскохозяйственных растений в рамках первого этапа трансфера технологий от компании Bayer обратились тринадцать российских компаний, из которых Наблюдательный совет Центра технологического трансфера отобрал семь частных селекционных компаний для передачи гермоплазмы кукурузы, сои, пшеницы и масличного рапса²⁸. Осуществление передачи гермоплазмы планируется в течение ближайших месяцев. Кроме того, предстоит передача молекулярных средств селекции кукурузы, сои, рапса, пшеницы, томата, огурца и капусты с актуальными протоколами их использования в рамках второго этапа трансфера технологий. Отбор претендентов компаний-получателей уже произведен, они ожидают утверждения Наблюдательным советом. Третье направление трансфера включает в себя передачу цифровой базы исторических агрономических данных, прием заявок на него еще идет²⁹.

Важно отметить, что компании получают технологии Bayer на условиях значительно более благоприятных, чем рыночные. В частности, в зависимости от ряда условий получатели технологий могут освобождаться от выплаты роялти, либо выплачивать роялти с существенной скидкой³⁰. Особый акцент делается на передаче знаний и протоколов по работе с передаваемыми материалами, что необходимо для их успешного использования российскими компаниями. Таким образом, первые итоги трансфера технологий свидетельствуют о том, что принятая мера оказалась успешной и востребованной среди представителей российского агротехнологического сектора.

Инновационный подход, примененный в ходе рассмотрения сделки Bayer / Monsanto, имеет прецедентный характер, поэтому он был взят за основу ряда положений Пятого антимонопольного пакета, касающихся трансфера технологий. В частности, Пятым антимонопольным пакетом вводится институт независимого доверенного лица (аналог европейского “trustee”), которое будет назначаться ФАС России по согласованию со сторонами сделки для контроля за исполнением обязательств и реализацией процедуры трансфера технологий.

²⁶ Высшая школа экономики. (n.d.). Центр технологического трансфера. <https://cct.hse.ru/>

²⁷ Федеральная антимонопольная служба. (2019, октябрь 18). Трансфер технологий в действии. <https://fas.gov.ru/news/28618>

²⁸ Федеральная антимонопольная служба. (2019, октябрь 24). ФАС в СМИ: Центр техтрансфера отобрал первые семь компаний-получателей гермоплазмы от Bayer. <https://fas.gov.ru/publications/19592>

²⁹ Федеральная антимонопольная служба. (2020, сентябрь 3). ФАС в СМИ: Bayer не будет брать роялти с российских селекционеров. <https://fas.gov.ru/publications/21661>

³⁰ Федеральная антимонопольная служба. (2020, сентябрь 2). ФАС в СМИ: Bayer упростил для российских селекционеров условия технологического трансфера – ФАС. <https://fas.gov.ru/publications/21657>

В ходе рассмотрения сделки Schlumberger / Eurasia Drilling Company (EDC)³¹ ФАС России и Правительственная комиссия также выявили необходимость в обеспечении трансфера технологий и предъявили к международной нефтесервисной компании Schlumberger требования предоставить российской буровой компании EDC ряд инновационных технологий бурения и гарантировать, что EDC сохранит права на эти технологии в случае, если Schlumberger придется покинуть российский рынок ввиду западных санкций. Однако в итоге Schlumberger приняла решение отказаться от сделки и направила в ФАС России официальное заявление об отзыве ходатайства на покупку доли в EDC, поэтому трансфера технологий на практике не произошло.

По словам экс-руководителя ФАС России И. Ю. Артёмьева, регулятор планирует в будущем транслировать опыт трансфера технологий и на другие сделки на инновационных рынках, подпадающие под антимонопольный контроль³². По мнению ФАС России, целями данной практики являются устранение потенциальных ограничений конкуренции, обеспечение развития рынков и перераспределение рыночной власти, а также повышение технологической конкурентоспособности российского бизнеса, как в национальном, так и в глобальном масштабе, в ответ на трансформацию рынков в цифровую эпоху.

Между тем, существуют и практические сложности, связанные с реализацией трансфера технологий, в частности, связанные с поиском компромиссного решения между тем, какие объекты стороны сделки готовы передать, и тем, какие объекты действительно требуются для развития индустрии (учитывая также, что выявить заранее такие необходимые объекты достаточно сложно). Кроме того, специалисты сталкиваются со множеством практических вопросов при определении правовой формы передачи технологий, при соблюдении прав и законных интересов сторон сделки, и при обеспечении поиска получателей технологии, которые смогут на практике их использовать в целях, заложенных законодателем и антимонопольным органом в данный институт.

Компаниям, обладающим существенным объемом данных, технологий и знаний и планирующим согласование сделок экономической концентрации с российскими регуляторами, рекомендуется:

- заранее оценить возможное влияние планируемой сделки на состояние конкуренции на российском рынке и на будущее развитие индустрии в целом,
- оценить потенциальные вопросы регулятора относительно возможных антимонопольных рисков,
- подготовить соответствующие правовые позиции,
- а также, при необходимости, рассмотреть возможность инициативного предложения ФАС России мер для снижения негативных эффектов сделки (например, в рамках ч. 10 ст. 32 Закона о защите конкуренции).

Предустановка приложений российских разработчиков как новелла отечественного антимонопольного регулирования

Введение обязательной предварительной установки приложений российских разработчиков, вызванное волной дел о злоупотреблении глобальными компаниями своим доминирующим положением на цифровых рынках, является еще одним цифровым нововведением в отечественном

³¹ Федеральная антимонопольная служба. (2019, февраль 5). ФАС в СМИ: Schlumberger отозвала ходатайство на покупку доли в российской Eurasia Drilling. <https://fas.gov.ru/publications/17473>

³² Федеральная антимонопольная служба. (2019, октябрь 18). Трансфер технологий в действии. <https://fas.gov.ru/news/28618>

антимонопольном законодательстве. За последние несколько лет ФАС России рассмотрела ряд дел о злоупотреблении доминирующим положением глобальными технологическими корпорациями (Google³³, Microsoft³⁴, Apple³⁵). В рамках данных дел основные претензии антимонопольного регулятора сводились к тому, что, являясь одновременно владельцами операционных систем / цифровых маркетплейсов и разработчиками программ / приложений, IT гиганты препятствовали доступу независимых разработчиков на рынок и / или навязывали потребителям свои собственные программные продукты (аналогичные предложениям конкурентов).

По мнению начальника управления регулирования связи и информационных технологий ФАС России Е. А. Заевой, глобальные компании получили конкурентные преимущества для продвижения собственных приложений и сервисов, используя практику связывания продуктов³⁶. Предустановка, как самый эффективный канал распространения приложений, приоритетно используется разработчиками операционных систем, что может приводить к дискриминации независимых разработчиков приложений. Отсутствие возможности для потребителя удалить предустановленные приложения усиливает конкурентные преимущества глобальных корпораций. Таким образом, в целях снижения рисков ограничения конкуренции, а также для уравнивания рыночной власти глобальных корпораций и небольших отечественных разработчиков приложений, ФАС России выступила с инициативой разработки законопроекта о предустановке приложений российских разработчиков.

Установление дополнительных ограничений в деятельности глобальных игроков на данном рынке сложно назвать специфической российской новеллой — скорее, оно является глобальным трендом. Например, Европейская комиссия ведет работу над законопроектом, запрещающим владельцам платформ отдавать преимущество своим сервисам в поиске, а также ограничивать удаление любого из своих приложений³⁷.

В отечественной дорожной карте по развитию конкуренции 2018 г. было предусмотрено принятие федеральных законов о предустановке российских приложений на пользовательские устройства и об обеспечении возможности полной удаляемости предустановленных программ³⁸.

2 декабря 2019 г. был принят Закон о предустановке приложений³⁹. В результате длительного и сложного обсуждения с представителями отрасли, во исполнение данного закона было разработано и принято Постановление Правительства Российской Федерации от 18.11.2020 № 1867 «О перечне отдельных видов технически сложных товаров...»⁴⁰, которое

³³ Решение ФАС России по делу №АД/54066/15 и предписание по делу № 1-14-21/00-11-15 (2015).

³⁴ Решение ФАС России по делу №АГ/56549/17. База решений и правовых актов (2017).

³⁵ Решение ФАС России по делу № 11/01/10-24/2019. База решений и правовых актов (2020).

³⁶ Управление Федеральной антимонопольной службы по Орловской области. (2019, январь 29). *ФАС представила концепцию о предустановке приложений*. <https://orel.fas.gov.ru/news/11619>

³⁷ Drozdziak, N. (2020, September 30). *Big tech faces ban from favoring own services under EU rules*. Bloomberg. <https://www.bloomberg.com/news/articles/2020-09-30/big-tech-faces-ban-from-favoring-own-services-under-eu-rules>

³⁸ Распоряжение Правительства РФ № 1697-р «Об утверждении плана мероприятий (“Дорожной карты”) по развитию конкуренции в отраслях экономики Российской Федерации <...> на 2018–2020 гг.» (2018).

³⁹ Федеральный закон № 425-ФЗ «О внесении изменения в статью 4 Закона Российской Федерации “О защите прав потребителей”» (2019).

⁴⁰ Постановление Правительства Российской Федерации № 1867 «О перечне отдельных видов технически сложных товаров с предварительно установленными российскими программами для электронных вычислительных машин, порядке составления и ведения перечня российских программ для электронных вычислительных машин, которые должны быть предварительно установлены на отдельные виды технически сложных товаров, и порядке их предварительной установки» (2020). <http://publication.pravo.gov.ru/Document/View/0001202011230051>

закрепило перечень технически сложных товаров («ТСТ»), на которые распространяются требования Закона о предустановке критерии к программам российских разработчиков, подлежащих предустановке, перечень программ и порядок его ведения, а также порядок осуществления предустановки изготовителями устройств.

Стоит отметить, что, по сравнению с первоначальным проектом документа, в итоговой версии был расширен спектр ТСТ, на которые распространяются требования о предустановке, а также перечень категорий программ, подлежащих предустановке. При этом, определенные вопросы вызывает включение в список категорий программ для предустановки сервисов государственных услуг и национальной платежной системы «МИР». Представляется, что в данной части документа целью правового регулирования является не защита конкуренции, а продвижение конкретных государственных инициатив.

На изготовителя ТСТ возложена обязанность обеспечить предустановку российских программ в рамках каждой из обязательных категорий (предполагается, что в КоАП РФ будет дополнен ответственностью за нарушение этой обязанности).

Вступление новых требований в силу ожидается 1 апреля 2021 г., и соблюдение этого срока потребует серьезных усилий со стороны участников рынка (особенно, изготовителей ТСТ). Вместе с тем, вопрос о том, как в действительности предустановка приложений повлияет на состояние конкуренции на российском рынке, пока остается открытым.

Основные выводы и рекомендации

В заключение следует отметить, что в настоящее время правоприменительная практика и антимонопольное законодательство России активно развиваются, чтобы ответить на новые вызовы цифровой экономики. Можно выделить основные направления развития:

- трансформация подходов к борьбе с антимонопольными нарушениями, совершаемыми с использованием аукционных роботов и ценовых алгоритмов,
- новые подходы к анализу рынка с учетом влияния больших данных, сетевых эффектов и новых технологий,
- совершенствование норм о контроле за экономической концентрацией, включая концепцию трансфера технологий,
- усиление антимонопольного регулирования на рынках мобильных приложений,
- автоматизация процессов выявления ФАС России антимонопольных нарушений, что повышает риски для бизнеса.

В связи с данными трендами компаниям рекомендуется рассмотреть возможность принятия дополнительных мер для минимизации антимонопольных рисков в условиях цифровой экономики, а именно:

1. Включить в свои программы антимонопольного комплаенса разделы, посвященные антимонопольным рискам при использовании ценовых алгоритмов и аукционных роботов, а также дополнительные практические рекомендации для сотрудников по поведению на цифровых рынках.
2. Проводить предварительный детальный аудит юридической службой функционала любого планируемого к внедрению программного обеспечения в сфере мониторинга или формирования цен, а также аукционных роботов и планируемых параметров их настройки, отражающих намеченную стратегию участия в торгах.

3. Осуществлять контроль за формами использования сотрудниками существующих ценовых алгоритмов и аукционных роботов на предмет соблюдения антимонопольного законодательства.
4. Своевременно выявлять, оценивать и предотвращать антимонопольные риски компаний в связи с ведением ими деятельности на цифровых рынках, применяя актуальные подходы ФАС России к анализу рынка с учетом сетевых эффектов, обладания цифровыми платформами и большими данными.

Список литературы / References:

1. Tenishev, A. P., & Teslenko, A. V. (2019). Uголовно-pravovaja ohrana konkurencii v uslovijah razvitija cifrovyh tehnologii [Criminal legal protection of competition in the context of the development of digital technologies]. *Zakon*, 6, 124–131.
2. Belickaja, A. V., Belyh, V. S., Beljaeva, O. A., Bolobonova, M. O., Vajpan, V. A., Gerasimov, O. A., Gorodov, O. A., Egorova, M. A., Karelina, S. A., Kasymov, R. Sh., Lebedev, K. K., Levushkin, A. N., Molchanov, A. V., Palehova, E. A., Parashhuk, S. A., Petrov, D. A., Poberezhnyj, S. G., Rahmatullina, L. Je., Rahmatullin, T. Je., & Rusakov, V. I. (2019). *Pravovoe regulirovanie jekonomicheskikh otnoshenij v sovremennyh uslovijah razvitija cifrovoj jekonomiki* [Legal regulation of economic relations in modern conditions of development of the digital economy]. Justicinform.
3. Egorova, M. A. (2018). Osobennosti normativnogo regulirovanija cifrovoj jekonomiki i problemy antimonopol'nogo regulirovanija na cifrovyh rynkah kak sredstvo zashhity nacional'nyh interesov [Peculiarities of the statutory regulation of the digital economy and issues of the antimonopoly regulation in digital markets as a national interest protection means]. *Jurist*, 11, 7–10. <https://doi.org/10.18572/1812-3929-2018-11-7-10>
4. Abramov, S. G. (2020). Juridicheskie i institucional'nye mehanizmy sozdaniya modeli sovershennoj konkurencii v sfere finansovogo rynka [Legal and institutional mechanisms of creation of a model of perfect competition on a financial market]. *Konkurentnoe Pravo*, 2, 33–36.
5. Kozhina, K. E., & Artjushenko, D. V. (2019). Cenovye algoritmy kak instrument vedenija biznesa: Antimonopol'nye riski i voprosy dopustimosti [Pricing algorithms as a tool of doing business: The antitrust risks and compatibility issues]. *Russian Competition Law and Economy*, 4(20), 54–59.
6. Popondopulo, V. F., Petrov, D. A., & Silina, E. V. (2019). Problemy pravovoj zashhity jekonomicheskoi konkurencii v uslovijah cifrovizacii jekonomiki [Issues of legal protection of economic competition in the conditions of digitization of the economy]. *Konkurentnoe Pravo*, 3, 7–11.

Вклад авторов:

Тархова К.В. — общее руководство и редактирование.

Алифиров В.И. — подготовка материала и редактирование.

Горохова О.Н. — подготовка материала.

The authors' contribution:

Ksenia V. Tarkhova — general guidance and editing.

Vladislav I. Alifirov — preparation of the article and editing.

Olga N. Gorokhova — preparation of the article.

Сведения об авторах:

Тархова К.В. — старший консультант антимонопольной практики, юридическая фирма «АЛРУД», член Международной ассоциации юристов (IBA), Тихоокеанской ассоциации юристов (IPBA), Ассоциации антимонопольных экспертов и Евразийской антимонопольной ассоциации, Москва, Россия.

ktarkhova@alrud.com

Алифиров В.И.* — консультант антимонопольной практики, юридическая фирма «АЛРУД», член Международной ассоциации юристов (IBA), Ассоциации антимонопольных экспертов и Евразийской антимонопольной ассоциации, Москва, Россия.

valifirov@alrud.com

Горохова О.Н. — юрист антимонопольной практики и практики интеллектуальной собственности и защиты данных, юридическая фирма «АЛРУД», Москва, Россия.

ogorokhova@alrud.com

Information about authors:

Ksenia V. Tarkhova — Senior Associate of Competition/Antitrust Practice, ALRUD Law Firm, Member of International Bar Association, Inter-Pacific Bar Association, Competition Experts Association and Eurasian Antimonopoly Association, Moscow, Russia.

ktarkhova@alrud.com

Vladislav I. Alifirov* — Associate of Competition/Antitrust Practice, ALRUD Law Firm, Member of the International Bar Association, Competition Experts Association and Eurasian Antimonopoly Association, Moscow, Russia.

valifirov@alrud.com

Olga N. Gorokhova — Attorney of Competition/Antitrust, Intellectual Property and Data Protection Practices, ALRUD Law Firm, Moscow, Russia.

ogorokhova@alrud.com

СТАТЬИ

ПЕРСОНАЛИЗИРОВАННОЕ ПРАВО И ФУНДАМЕНТАЛЬНЫЕ ПРАВА

Т.З. Мисостишхов

Национальный исследовательский университет
«Высшая школа экономики»
101000, Россия, Москва, ул. Мясницкая, 20

Аннотация

В последние годы в научном сообществе возрос интерес к идее персонализированного права, предполагающего разработку и реализацию индивидуализированных правовых норм посредством алгоритмической обработки данных подобно тому, как компании персонализируют свои услуги с использованием технологий больших данных. Статья ставит целью определить место и роль персонализированного права, оценить риски и последствия персонализации в условиях становления цифровой экономики. В работе обосновывается теоретическая интерпретация персонализированного права сквозь призму концепции «мягкого позитивизма», обеспечивающего равновесие между социологической фактичностью права и нормативизмом. В исследовании раскрываются содержание и основные признаки, а также дается определение понятия «персонализированное право». Проводится анализ соотношения персонализированного права с фундаментальными правами, в рамках которого оцениваются риски и последствия персонализации. В частности, существует вероятность дискриминации вследствие ошибочного принятия решения алгоритмом вразрез с реальной волей лица. Алгоритмическая персонализация представляется оправданной на первых порах только в тех сферах правоотношений, где минимален риск нарушения фундаментальных норм и вторжения в пространство общественной дискуссии. Подчеркивается, что прозрачность публичного сектора и процесса принятия решения алгоритмом на основе данных имеет ключевое значение в условиях персонализированного права, но в то же время способна обесценить его вследствие оппортунистических практик. Обнаруженные вызовы приводят к выводу о востребованности в будущем профессионалов, обладающих фундаментальными правовыми знаниями и необходимым уровнем познания в области компьютерных наук, которые могут исполнить роль независимых экспертов и органа контроля, обеспечивающего права субъекта персональных данных.

Ключевые слова

принятие решений на основании исключительно автоматизированной обработки персональных данных, права человека, большие данные, цифровая экономика, оборот данных, персональные данные, детализированные правовые нормы, дискриминация, комплаенс, персонализированное право

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Для цитирования

Мисостишхов, Т. З. (2020). Персонализированное право и фундаментальные права. *Цифровое право*, 1(4), 56–73. <https://doi.org/10.38044/2686-9136-2020-1-4-56-73>

Поступила: 22.09.2020, принята в печать: 09.11.2020, опубликована: 20.12.2020

ARTICLES

PERSONALIZED LAW AND FUNDAMENTAL RIGHTS

Tembot Z. Misostishkhov

National Research University Higher School of Economics
(HSE University)
20, str. Myasnitckaya, Moscow, Russia, 101000

Abstract

In recent years, scholars have focused increased attention on the idea of personalized law. It suggests the creation and enforcement of individualized legal norms based on the algorithmic processing of data in the similar manner companies personalize their services using Big Data tools. The article aims to define the role and position of personalized law and to evaluate the risks and consequences of personalization in the context of the emerging digital economy. The research analyses the theoretical grounds of personalized law and justifies its interpretation from the perspective of Hart's legal positivism striking a balance between the sociological facticity of law and normativism. The study reveals the content, essential features of personalized law and defines its concept. The author analyses the correlation of personalized law with fundamental rights, thus evaluating the risks and consequences of personalization. Particularly, the errors of the approximation of a person's actual will could occur as part of algorithmic decision-making thereby resulting in discrimination. It appears reasonable that at the beginning, algorithmic personalization should cover only those domains which have the minimal risk of the violation of fundamental norms and of intrusion into the field of social debates. The study underscores, that the transparency of the public sector and of the data-based algorithmic decision-making process is crucial in the context of personalized law, but nevertheless could debase its idea due to opportunistic practices. The issues identified during the research lead one to suggest that professionals who have both legal education and expertise in computer sciences would be in demand in the future. Such professionals could perform the role of independent experts and neutral authority monitoring compliance with data subject's rights.

Keywords

automated decision making, human rights, Big Data, digital economy, data sharing, personal data, granular legal norms, discrimination, compliance, personalized law

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The study had no sponsorship.

For citation

Misostishkhov, T. Z. (2020). Personalized law and fundamental rights. *Digital Law Journal*, 1(4), 56–73. <https://doi.org/10.38044/2686-9136-2020-1-4-56-73>

Submitted: 22 Sep. 2020, accepted: 09 Nov. 2020, published: 20 Dec. 2020

«Если машины могут обеспечить соблюдение закона, это здорово. Но для начала должен быть закон».

Лоуренс Лессиг

Число девайсов, ежеминутно «снимающих цифровые отпечатки» с наших действий, реакций и атрибутов каждодневной деятельности, экспоненциально растет. Рост качества и количества данных, сегодня часто именуемых нефтью цифровой эры, наряду с инструментами их аналитики, не только способствуют инновациям в экономике, но и обуславливают смену парадигмы в правовом регулировании.

С момента проведения в 2018 г. на базе Юридической школы Чикагского университета симпозиума “Personalized Law” в научном сообществе стал оживленно обсуждаться феномен персонализированного права¹, выражающийся в том, что данные и технологии их обработки в контексте правового регулирования создают предпосылки для фундаментальных изменений относительно порядка принятия и реализации правовых норм: единообразные правила могут уступить место детализированным нормам, которые «примеяются» к нуждам, ожиданиям, особенностям и условиям жизни конкретного человека, открывая возможности для достижения беспрецедентной степени регулятивной точности.

При всех своих достоинствах концепция персонализации заставляет задуматься о соотношении такой модели регулирования с фундаментальными правами, в частности, с принципом равенства, гарантируемым ст. 19 Конституции Российской Федерации², и запретом дискриминации, закрепленным в ст. 1 Протокола № 12 к Конвенции о защите прав человека и основных свобод³ (далее — Европейская конвенция). Кроме того, индивидуализация права немыслима без динамичной обработки различного рода персональных данных (например, о скорости движения автомобиля или о покупках в супермаркетах), аспекты защиты которых в цифровую эпоху обретают более чувствительный характер. В частности, на способность правительств, организаций и физических лиц в условиях цифровизации «отслеживать, перехватывать и собирать информацию» и, как следствие, ущемлять право на свободу мнений и право на неприкосновенность частной жизни, указано в Резолюции Генеральной Ассамблеи ООН от 18.12.2013 № 68/167 «Право на неприкосновенность личной жизни в цифровой век»⁴. Ученое сообщество также обращает внимание на остроту вопросов интерпретации и объяснения логики принятия алгоритмом тех или иных решений — в особенности для таких областей, как безопасность, здравоохранение и право (Abdrakhmanova et al., 2019).

Значимость сказанного для российской правовой системы подтверждается политикой перехода к цифровой экономике и цифровому здравоохранению. Постановлением Правительства РФ от 26.12.2017 № 1640 «Об утверждении государственной программы Российской Федерации «Развитие здравоохранения» определена подпрограмма «Развитие и внедрение инновационных методов диагностики, профилактики и лечения, а также основ персонализированной медицины»⁵. Приказом Министерства здравоохранения РФ от 24.04.2018

¹ Parins, C. (2018, May 29). *Personalizing the law. Law Review Conference examines possibilities and pitfalls of using predictive technology to tailor the law.* The University of Chicago. The Law School. <https://www.law.uchicago.edu/news/personalizing-law>

² Конституция Российской Федерации. Собрание законодательства РФ. № 31, ст. 4398 (1993).

³ Конвенция о защите прав человека и основных свобод. ЕСПЧ. Бюллетень международных договоров. № 3 (1950).

⁴ Resolution 68/167 on the right to privacy in the digital age. UN General Assembly (2013). <https://undocs.org/A/RES/69/166>

⁵ Постановление Правительства РФ № 1640 «Об утверждении государственной программы Российской Федерации «Развитие здравоохранения» (2017).

№ 186 утверждена «Концепция предиктивной, превентивной и персонализированной медицины»⁶. Отмечается, что в России имеются все ресурсы для развития персонализированной медицины и что отсутствие внедрения ее подходов может обернуться отставанием показателей экономического роста⁷. Однако, как видно, нормативные сдвиги в сторону персонализации на основе современных технологий имеют фрагментарный характер и лежат преимущественно в административно-правовой плоскости. Очевидно, что сейчас необходим комплексный и всесторонний анализ научным сообществом данного направления в развитии права.

Понятие персонализированного права

Впервые идею о правовых нормах, приведенных в соответствие с условиями рынка и индивидуальными характеристиками его участников, высказал Ян Айрес, который еще в 1989 г. принял попытку разработать теорию «оптимальной индивидуализации» (Ayres, 1993). Ученый, в частности, опирался на исходные данные в виде наблюдений И. Эрлиха и Р. А. Познера (Ehrlich & Posner, 1974), которые, проводя экономический анализ законотворчества, писали, что «в качестве правонарушения можно квалифицировать не просто езду на автомобиле со скоростью выше шестидесяти миль в час ... но езду, являющуюся необоснованно быстрой в конкретных обстоятельствах». В 2006 г. Дж. Гейс поставил вопрос о том, должны ли законодательные органы принимать более сложные правовые нормы, которые могут обеспечить «кастомизированное» регулирование для различных рынков или даже различных участников правоотношений (Geis, 2006). Весомый вклад в проработку данного направления также сделал один из авторов теории подталкивания К. Санстейн (Sunstein, 2013), указавший, что, в принципе, персонализированные нормы могут быть предусмотрены в отношении каждого индивида. Рассуждая о персонализации диспозитивных норм, ученый полагал, что в идеальном представлении они сочетают в себе преимущества как универсальных (стандартизированных) норм, так и активного свободного выбора самого лица. Как и универсальные нормы, они упрощают жизнь, не требуя активных действий со стороны индивида, но при этом обеспечивают достижение полезного эффекта за счет технологических возможностей, как если бы такие активные действия были предприняты, обеспечивая тем самым точность в регулировании без необходимости затрачивания большого количества времени. Автор одним из первых указывает на серьезность вопроса защиты права на неприкосновенность частной жизни, а также обращает внимание на значимость фактора доверия публичным институтам, риски пристрастности или недостаточной информированности государственных служащих.

Само понятие «персонализированное право» (англ. “personalized law”) впервые было упомянуто в 2014 г. в работе А. Пората и Л. Страхилевича (Porat & Strahilevitz, 2014) как амбициозная идея персонализировать не только диспозитивные нормы наследственного, договорного права или законодательство в сфере раскрытия информации, но право в целом.

Весомый вклад в развитие теоретических оснований персонализированного права был сделан немецким исследователем Ф. Бендером (Bender, 2020), обозначившим и противопоставившим две концепции персонализации. Первая концепция — эмпирический субъективизм, имеющий в своей основе немецкую доктрину юриспруденции интересов, повлиявшую

⁶ Приказ Министерства здравоохранения РФ № 186 «Об утверждении Концепции предиктивной, превентивной и персонализированной медицины» (2018).

⁷ Иванов, Р. (2018, Октябрь 30). *Вице-президент по разработкам «Биокад» Р. Иванов: «Все ресурсы для развития персонализированной медицины в России есть»*. Interfax.ru. <http://www.interfax-russia.ru/NorthWest/exclusives.asp?id=979068>

на становление американской доктрины правового реализма. Данная траектория персонализации права согласуется с идеями поведенческой экономики и юриспруденции и опирается на конкретные, осязаемые предпочтения и волю индивидов (Bender, 2020). Вторая траектория персонализации является, по сути, контрконцепцией, предложенной самим автором, и именуется как «нормативный объективизм». В качестве конечного легитимирующего источника права данный подход признает не сугубо волю субъектов, а объективные политические соображения, в основе которых лежит ценностно-ориентированный подход (Bender, 2020).

Автор критикует как социологические теории, так и юридический позитивизм, который, по его мнению, возводит в закон эмпирически распознаваемые предпочтения, не обеспечивая теоретического базиса для анализа содержания принятой нормы. Персонализация в экстремальном ее понимании, по замечанию ученого, аналогично транслирует индивидуальные предпочтения в правовые нормы, даже если эти предпочтения являются дискриминационными (Bender, 2020). Более того, реальные предпочтения индивидов бывают незаметны, т. к. могут непрерывно изменяться и противоречить друг другу. В итоге получается, что персонализированные правовые нормы, в основе которых лежат лишь предпочтения, обретают в значительной степени оторванный от реальности, иллюзорный характер. Исходя из этого, возникает необходимость в дополнительном критерии, выходящего за рамки эмпирического субъективизма как подхода к персонализации права (Bender, 2020).

Нормативный объективизм как подход к персонализации права рассматривает нормативно-правовые акты в качестве основанных на некоем авторитете, стоящем выше воли конкретного субъекта, и подразумевает телеологический, ценностный анализ правовых норм, методологически характерный для юриспруденции ценностей, используемой в немецком праве (Bender, 2020). В рамках юриспруденции ценностей законодатель призван установить баланс частных и публичных интересов путем построения некоей системы ценностей, в системе координат которой «происходит поиск решения в каждом конкретном случае». При формировании системы ценностей принципиальное значение отводится конституции (Kurzynski-Singer, 2011). Напротив, подходы, сущность которых состоит лишь в воспроизведении предпочтений (юриспруденция интересов) или максимизации благосостояния (экономический анализ права), и которые утверждают нейтральность по отношению к ценностям, по мнению Ф. Бендера, потенциально тоталитарны. Так, например, максимизация благосостояния — это только одна из ценностей, и она должна быть сбалансирована с принципами справедливости и недискриминации (Bender, 2020).

Тем не менее, как представляется, немецкий исследователь недостаточно всесторонне оценивает социологический подход к пониманию персонализированного права, несколько упуская такие особенности права в представлении социологии, как значительная «диверсифицированность, подвижность и относительность». В действительности, фундаментальные нормы, ценностный характер которых признается автором, также могут иметь социологические корни. Так, школа естественного права и права народов, начало которой положил Г. Гроций, основывалась на социологических данных: в частности, Ж.-Ж. Руссо развивал идею естественного состояния, исследуя «быт племен до открытия Америки европейцами» (Karbon'ye, 1986). Это, в свою очередь, соответствует позитивистскому правопониманию Г. Харта, согласно которому естественно-правовые установки, выраженные в законе, не всегда обязательно обусловлены моралью, а являются результатом объективно сложившихся социальных взаимодействий. Дж. Раз, продолживший развивать концепцию своего учителя, также отмечал, что содержание закона обусловлено прежде всего социальным фактом (Nekhayev, 2019).

Социологический подход к пониманию персонализированного права также позволяет учитывать существование внутри одной правовой системы разнородных правовых пространств (в терминологии Ж. Карбонье) — частных групп, в которых может возникать спонтанное правотворчество. Это справедливо, если мы говорим не о праве в строго догматическом понимании, а о правовой системе в целом, охватывающей весь комплекс юридических явлений, существующих в обществе (Karbon'ye, 1986). Это могут быть обычаи и сложившиеся устойчивые практики внутри мелких групп, которые не охватываются издаваемыми государством нормами, что характерно для сложных правовых систем. В принципе, персонализированное право посредством технологий больших данных может объять и правовые явления, ныне незаметные для взгляда государственных органов и существующих стихийно, и, не разрушая их, придать сложившимся институциональным правилам большую четкость и действенность.

Таким образом, очевидна сущностная связь персонализированного права с конкретным теоретическим подходом и концепцией правопонимания, от которых зависит практический эффект его реализации и влияния на правовой статус отдельного лица. Исходя из вышесказанного, представляется, что, с одной стороны, нельзя приоритизировать социологический подход в чисто эмпирическом и субъективистском смысле, не признающим за законодательно оформленной нормой как таковой должной обязывающей силы, как, например, в представлении правовых реалистов. С другой стороны, нормативистский подход демонстрирует минимальную детерминированность нормативных предписаний в социальных практиках или же полное ее отсутствие. Неопозитивистская концепция Г. Харта наиболее полно отражает все достоинства, как социологических течений, так и позитивистских представлений о праве, в условиях формирования доктринального подхода к пониманию персонализированного права. Концепция предполагает существование неких фундаментальных норм и соответствие юридической действительности специфическим моральным принципам и ценностям, не игнорируя естественно-правовые и социологические взгляды на сущность права (Kasatkin, 2008).

Отвлекаясь от теоретических аспектов персонализированного права, целесообразно осветить его историко-экономические предпосылки, содержание и признаки с учетом практико-ориентированной логики преобладающих на сегодняшний день исследований, а также возможные сферы персонализации права. Отталкиваясь от концепции мягкого позитивизма, планируется сформулировать авторское определение понятия «персонализированное право», предварительно установив для этой цели соотношение персонализированного права с фундаментальными правами.

Согласно определению, данному И. Земаном (Zeman, 1966), информация — это «сведения, полученные в процессе познания, отражающие объективные факты и закономерности мира в системе точных понятий, дающих возможность предвидения и преобразования действительности в интересах общества». Эта дефиниция интересна тем, что в ней указана функция информации, выражающаяся в предоставлении возможности предвидеть и преобразовывать реальность и подчеркивающая генетическую взаимосвязь информации с понятиями «управление» и «регулирование». Ученые в области информационного права также отмечают, что большая информированность управляющего позволяет снизить долю неопределенности и риска, являющихся составной частью принимаемых решений (Khizhnyakov & Lebedev, 2011), а анализ информации занимает предваряющую ступень в ходе подготовки и принятия решений по отношению к другим функциям управления (Khizhnyakov & Lebedev, 2011).

Данные особенности информации можно назвать ключевыми с точки зрения цели персонализированного права и содержания его понятия. В демократическом государстве право

выполняет важную роль регуляции общественных отношений сообразно сигналам, которые исходят от субъектов этих правоотношений и формируют содержание нормативно-правового корпуса.

Однако в привычном нам виде право максимально унифицировано и однообразно, что вполне можно объяснить экономическими причинами. Создание казусного законодательства, предусматривающего разного рода исключения (возможно, перекрестные), учет в нем огромного количества нюансов общественных отношений были бы связаны с необходимостью осуществления несоизмеримых затрат. Создание такой сложной системы правил явило бы собой сложность не только для законодателя. Адресаты норм могли бы столкнуться с трудностями в понимании и реализации правовых норм. Отсутствие единообразия норм также могло бы стать барьером при рассмотрении споров.

К. Буш полагает, что стандартизованность правовых норм явилась прямым следствием возможностей человека и общества обрабатывать информацию, и представляет собой продукт доцифровой, индустриальной эпохи (Busch, 2019), направленный на охват как можно большего количества субъектов. Современное право, возможно, в некоторой степени по инерции, продолжает данные тенденции. Хотя, как видно, стандартизованное правовое регулирование было направлено на снижение транзакционных издержек, с другой стороны, оно порождает или не учитывало другие — психологические, поведенческие (Porat & Strahilevitz, 2014), временные, а также связанные с асимметрией информации. Как в случае с написанием завещания, неиспользование предоставляемой законодателем диспозиции для многих людей может быть следствием слишком высоких издержек (Porat & Strahilevitz, 2014), в связи с чем они смиряются с действием норм, работающих «по умолчанию».

Цифровая революция, позволившая улучшать продукты и сервисы и оптимизировать решения на основе информации, имеет потенциал преодоления вышеуказанных барьеров. Благодаря машинному обучению стало возможным обнаруживать кластеры и паттерны в данных, позволяющие строить прогнозы на базе взаимосвязи различных параметров.

Так, в одном из последних исследований персонализированное право определяется как направленное на использование преимуществ технологических прорывов в области сбора данных и науки о данных, которые позволяют передавать, хранить, организовывать и анализировать данные эффективно и своевременно с целью «специально разработать» (англ. “tailor”) правовые нормы под конкретных лиц (Elkin-Koren & Gal, 2019). Например, вместо установления единого скоростного лимита скоростные лимиты могут быть персонально «спроектированы» под конкретных водителей на основании их опыта, водительской истории и дорожных условий в режиме реального времени (Elkin-Koren & Gal, 2019). Правореализация в отношении субъектов может происходить мгновенно посредством смартфонов, умных автомобилей и других смарт-устройств. Тем самым закон может «взвесить» все имеющие значение факты, тотчас проанализировать, какое поведение допустимо «в каждом возможном сценарии», как следствие, максимизируя полезный эффект правового регулирования (Barry et al., 2020).

Немецкие правоведы Г. Григолейт и Ф. Бендер (Grigoleit & Bender, 2019) указывают на генетическое родство персонализированного права с двумя изменениями технологической сферы: во-первых, со значительным ростом объема собираемых и доступных данных (англ. “Big Data”), и, во-вторых, с повсеместным распространением современных информационно-коммуникационных систем, позволяющим довести информацию до каждого отдельного лица и тем самым связывающим такое лицо с остальным обществом (англ. “Big Link”). В целом, идею того, как два

этих явления способны преобразовать правовой ландшафт, авторы выражают в следующем: на первом этапе при помощи алгоритмов может быть обработан огромный массив доступных в отношении конкретного индивида данных с целью выявить посредством корреляций на основе различных косвенных показателей поведенческие паттерны и предпочтения, которые затем учитываются в процессе разработки нормативных предписаний. На втором этапе современные девайсы делают возможным коммуникацию предписаний соответствующим индивидам или правоприменителям. Как следствие, правовые нормы приобретают тенденцию к большей персонализации, а право в целом может быть весьма существенно (или даже бесконечно) персонализировано (Grigoleit & Bender, 2019).

В частности, персонализация права обладает потенциалом в сфере раскрытия информации потребителю. Вообще, нормы потребительского законодательства о раскрытии информации основаны на модели среднего потребителя, являющегося в известной мере внимательным и информированным. Эффективность такого единого регулятивного подхода ставится под сомнение, поскольку раскрытие информации в стандартизированном формате часто не имеет пользы и, более того, может нанести ущерб, т. к. человек оказывается перегруженным irrelevantными сведениями, в массиве которых теряется то, что действительно актуально (Busch, 2019). Посредством персонализации раскрытие информации может стать более осмысленным: в случае, если беременная женщина приобретает лекарство и в инструкции мелким шрифтом указано, что оно имеет определенные побочные последствия для беременных, эта информация будет подсвечена и явным образом доведена до внимания как наиболее релевантная.

Вместе с тем не будет ошибкой сказать, что персонализация в некоторой степени уже присутствует в отечественном законодательстве. П. 10.1 Постановления Правительства РФ от 23.10.1993 № 1090 «О Правилах дорожного движения»⁸ устанавливает различные допустимые значения скорости движения в зависимости от типа используемого транспортного средства, характера местности и класса автомобильной дороги, а также обязанность учитывать интенсивность движения, особенности и состояние транспортного средства и груза, дорожные и метеорологические условия, в частности видимость в направлении движения. Можно представить, что в цифровых реалиях данные условия могут быть достоверно установлены автоматически и доля неопределенности в вопросе необходимости корректировки управления автомобилем, соответственно снижена. В этом отношении, наверное, можно говорить о персонализированном праве не как о нечто совершенно новом, а как о «революции» в персонализации. Эта мысль находит подтверждение у профессоров Э. Дж. Кейси и Э. Ниблетта (Casey & Niblett, 2019), по словам которых «идея, что право должно наилучшим образом соответствовать релевантному контексту, который оно призвано регулировать, является очевидной и существует с момента возникновения права как такового».

Исходя из сказанного, представляется преждевременным говорить о взаимосвязи персонализированного права с цифровыми устройствами как об исключительной и неотъемлемой составляющей с точки зрения создания правовых норм. Электронные девайсы также не всегда могут быть необходимы для их реализации. Конечно, они задействуются непосредственно в случае, когда, например, врач, спешащий оказать медицинскую помощь, едет на автомобиле, на дисплее которого напрямую отображается скоростной лимит, а перекрестные светофоры активируют зеленый сигнал при его приближении. Однако можно представить ситуацию персонализированного налогообложения, когда данные о совершении человеком социально

⁸ Постановление Правительства РФ № 1090 «О Правилах дорожного движения». Собрание актов Президента и Правительства РФ. 22.11.1993, № 47, ст. 4531 (1993).

полезных действий учитываются налоговым органом и оптимизируют налогооблагаемую базу. Приведение в исполнение нормы или ее коммуникация лицу посредством информационных технологий в таком случае необязательны.

Обобщая сказанное, можно выделить следующие основные признаки персонализированного права: зависимость от степени распространенности и использования цифровых устройств и технологий; зависимость от количества и качества доступных данных, в особенности — персональных данных; правотворчество преимущественно на базе алгоритмической обработки и анализа данных; правореализация и доведение информации до субъекта, как правило, посредством смарт-устройств.

Между тем, аспекты обеспечения права на неприкосновенность частной жизни в условиях оборота данных в контексте персонализированного права побуждают человека понять для себя, какую меру детализации он хотел бы ожидать от правового регулирования. Намереваясь получить ответ на данный вопрос с позиции доктрины мягкого позитивизма, необходимо установить соотношение персонализированного права с фундаментальными правами.

Соотношение персонализированного права с фундаментальными правами

Одним из основополагающих фундаментальных прав является право на свободу, закрепленное в ст. 22 Конституции РФ и ст. 5 Европейской конвенции. На первый взгляд, персонализация норм в соответствии с ожиданиями индивидов стимулирует свободу и автономию личности, поскольку с большей вероятностью корреспондирует специфическим предпочтениям и сопутствующим обстоятельствам, нежели нормативный правовой акт общего действия. Однако для того, чтобы убедиться, так ли это на самом деле, необходим более тщательный анализ юридической концепции свободы.

Свобода измеряется не только соответствием результата правореализации персональным ожиданиям и предпочтениям. Понятие свободы гораздо шире и содержит определенный элемент свободы выбора (Bratanovskiy & Ostapets, 2019), или свободы воли (англ. “agency element”). Полная свобода проявляется в возможности человека выбирать по своему желанию — в отсутствие подталкивания и навязывания выбора из ограниченного списка альтернатив. Данная концепция свободы тесно связана с рыночной экономикой и демократической организацией общества (Bender, 2020).

Подобная интерпретация принципа свободы приводится и сторонником классического либерализма Ф. А. Хайеком, который с опорой на идеи А. Смита признает ее «совершенную необходимость» в целях «дать место непредсказуемому и непредвиденному» (Khayyuk, 2018), учитывая то обстоятельство, что «человеческое знание расплывлено», а централизованное планирование не способно в полной мере усваивать и контролировать информацию (Khayyuk, 1992). Ученый указывает на необходимость отделять абстрактные нормы, т. е. законы, от «специфических команд-распоряжений», поскольку законы имеют «абстрактно-всеобщий характер», возникают спонтанным образом и никем не спроектированы. Они «наперед известны и определены для всех без изъятия»⁹.

⁹ Antiseri, D., & Reale, J. (Eds.). (1997). Liberalizm Fridrikha fon Khayyeka [Liberalism by Friedrich von Hayek]. In D. Antiseri, & J. Reale (Eds.). Zapadnaya filosofiya ot istokov do nashikh dney (S. A. Mal'tseva, red. i per.) [Western philosophy from its origins to the present day (S. A. Maltseva, Ed., Trans.)]. (vol. 4). Petropolis.

Принимая во внимание либеральную концепцию правопонимания и соответствующую ей интерпретацию свободы, Ф. Бендер признает очевидным, что персонализация норм способствует повышению результативности (англ. “realization-dimension”), но значительно ослабляет свободу выбора (Bender, 2020).

Следует отметить, что персонализированное право ущемляет свободу воли индивида, также вследствие оценки алгоритмами лишь внешних аспектов поведения человека и риска не уловить постоянно меняющиеся предпочтения. Человек в таком случае может лишиться возможности приведения нормы в соответствие с реальными параметрами и ожиданиями (Bender, 2020). Несомненно, алгоритмы становятся все более совершенными и на удивительно высоком уровне способны «замерять» наши предпочтения. Тем не менее, их возможности применительно к возможности «считывать» настроения и интересы субъектов в целях регулирования общественных отношений можно легко переоценить.

Персонализированное право также может знаменовать сужение пространства частной инициативы и переход от фигуры «предпринимателя» к фигуре «потребителя» как наиболее доминантной. Это может быть проиллюстрировано на примере функции и роли договора в обществе. Если в контексте традиционного правового регулирования договор представляет собой главный образец реализации транзакционной автономии лица и является фундаментом социального порядка, основанного на рыночной модели, то в системе персонализированного права договор в значительной степени может быть вытеснен государственным регулированием, что создает благоприятную почву для установления патерналистского режима социальной организации. Данную точку зрения можно раскрыть на примере последствий ценовой персонализации. Так, алгоритмы не могут персонализировать диспозитивные нормы в узком смысле, т. е. ограничить свое распространение на такие свободно согласовываемые сторонами положения, как, например, гарантии (Bender, 2020). Они должны быть способны также каким-то образом модифицировать и цену. Ведь если контрагент, стремящийся обезопасить себя от рисков и получающий договорные гарантии, платит ту же цену за товар, что и нечувствительные по отношению к рискам акторы, последние, исходя из соображений справедливости, тоже захотят пользоваться преимуществами гарантий. Следовательно, ценовая чувствительность в системе персонализированных диспозитивных норм неизбежна. При заключении договора купли-продажи алгоритм, соответственно, должен определить, какие дополнительные издержки созданы для продавца включением гарантий. В то же время, если алгоритм имеет такую способность — утверждает Ф. Бендер — вероятно, он также должен суметь рассчитать и расходы на создание самого товара. Логично полагать, что алгоритм, обладающий подобными качествами, также сможет определить наиболее эффективный коэффициент прибыли (англ. “margin of gain”), и если в действительности алгоритм имеет настолько широкие возможности, он вполне способен симулировать (англ. “mimic”) функционирование рынка и в конечном итоге полностью его заменить. Ф. Бендер характеризует складывающуюся в этих условиях организацию общества как «микросоциализм» (Bender, 2020). Представляется, что в таком мире понятие свободы предпринимательства теряет привычно вкладываемый в него смысл.

Аналогичное прогнозное наблюдение отражено в труде профессора права Э. Познера и преподавателя курса проектирования цифровой экономики, д. э. н. Г. Вейла, согласившихся во мнении о том, что сегодняшние вычислительные мощности и методы машинного обучения создали условия для осуществления «укрупненного планирования, обобщения рыночных сигналов и масштабирования планирования на уровне функции полезности индивида». Такие сервисы,

как Amazon, Uber и Netflix, по мнению ученых, уже сейчас успешны и способны реализовать «тотальное планирование с помощью распределенных вычислений и экосистемы из приложений, которые обеспечат долгосрочное администрирование поведения большого количества индивидов». Такое планирование будет не централизованным планированием как таковым, «но уже и не рыночным механизмом». В этой парадигме с использованием «распределенных компьютеров» происходит переход от рынка как способа функционирования экономики к распределенному планированию (Belyavskiy, 2020), где искусственный интеллект может взять на себя выполняемую на данный момент ценовой системой функцию «руководства» эффективным распределением благ (Isztin, 2019).

Персонализация на основе предпочтений также может ограничить свободу выбора в публичной сфере. Для демократии необходимо, чтобы закон был предметом прений на публичном форуме, исполняющего роль «рынка идей» (или «пространства идей») (англ. “marketplace of ideas”). Для того чтобы народ пользовался свободой воли, его представители также должны ею обладать. Однако в мире персонализированного права содержание многих законодательных актов может оказаться детерминированным не дискуссией народных представителей, а экспертами и учеными в области компьютерных наук, контролирующими алгоритмы (Bender, 2020). Кроме того, вызывает опасения возможность ненадлежащего использования данных для каких-либо узковедомственных целей — например, посредством придания «большого веса» в алгоритмах тем или иным характеристикам, способствующим достижению определенной политической выгоды.

Данные суждения порождают размышления и об аспектах внутренней свободы человека и связанных с этим негативных последствиях. В условиях персонализированного регулирования человек может ощущать себя несвободным, ограниченным в возможности демонстрировать разнообразные грани своей персоны в различных условиях. В качестве примера можно привести меры «сортировки пассажиров» в метро, о реализации которых в ближайшее время объявили в Китае. Согласно принятым мерам, для цели сокращения времени на проход через рамки металлоискателей и рентгеновскую проверку багажа в час пик планируется использование алгоритмов анализа внешнего вида, походки, жестов и других индивидуальных атрибутов, в результате которого будет приниматься решение о том, является ли тот или иной человек подозрительным, и происходит выборочное направление на досмотр¹⁰. Возникает мысль о том, не вторгаются ли эти акции в сферу действия презумпции невиновности и не будут ли они нарушать принцип недискриминации. Рассуждая о проблемах объективности алгоритмических систем, профессор Нива Элкин-Корен отмечает, что субъект может намеренно быть осторожным и рассудительным в большинстве сфер своей жизни, в то же время позволяя себе рискованные действия в такой области, где отсутствует возможность причинить вред другим людям (Elkin-Koren & Gal, 2019). Неизвестны гарантии того, что таким действиям не будет придаваться непропорционально большее значение, вследствие чего о данном лице алгоритм придет к выводам, аналогичным, например, степени рискованности опрометчивого водителя, представляющего опасность для пешеходов. В любом случае, очевидно, такое использование алгоритмов для целей персонализированного правоприменения вступает в конфронтацию с концепцией многогранности личности. Даже те люди, которые не признают ощущения морального дискомфорта

¹⁰ Feng, G. (2019, October 30). *Beijing metro to begin security “sorting” based on facial recognition*. Radio Free Asia. <https://www.rfa.org/english/news/china/facial-10302019162222.html>; Zhou, V. (2019, November 1). *Beijing subway plans to “sort passengers” with facial scan*. Inkstone. <https://www.inkstonenews.com/society/beijing-subway-plans-sort-passengers-facial-recognition/article/3035898>

в условиях слежки, соглашаются с тем, что эффект внутренней скованности может иметь место, когда слежка влечет за собой риск возникновения неблагоприятных последствий (Kaminski & Witnov, 2015). Испытываемые индивидом ощущения, в свою очередь, могут напрямую воздействовать на волю лица. Пример предпосылок к этому — китайская система социального кредита, на основе методов стимулирования и наказания способствующая формированию у индивидов конкретных паттернов поведения¹¹. Указанная причинно-следственная связь неоднократно подтверждается в литературе: применение персонализированных «стандартов» в данном случае также представляет собой инструмент, который может в действительности придавать конкретную форму поведению субъектов персональных данных (Elkin-Koren & Gal, 2019).

Представляется, что такое воздействие обработки данных на человека объективно может способствовать ограничению его участия в определенной деятельности, данные о которой фиксируются, или использования девайсов, собирающих данные. Следовательно, существенно снизится количество доступных для обработки данных (Elkin-Koren & Gal, 2019).

Можно допустить, что персонализированное право при задействовании техник подталкивания в ряде случаев будет вступать в противоречие с принципом неприкосновенности человеческого достоинства (ст. 1 Хартии основных прав Европейского союза¹²), помещенным европейским законодателем перед нормой о праве на жизнь, и принципом достоинства личности (п. 1 ст. 21 Конституции РФ). Интересна в этой связи мысль Р. Дворкина (Dvorkin, 2004), который пишет, что без необходимости защиты человеческого достоинства утверждение об обладании лицом фундаментальным правом по отношению к государству (например, правом на свободу слова) не имеет смысла. Высказываемая теоретиком права идея человеческого достоинства предполагает существование способов крайне несправедливого обращения с человеком, «несовместимым с признанием его полноправным членом человеческого общества» (Dvorkin, 2004). Соглашаясь с приведенной логикой и рассуждая об особенностях принятия алгоритмических решений на основе больших данных, А. И. Савельев (Savel'ev, 2019) справедливо указывает, что «прогнозирование поведения» с использованием манипулятивных практик «дегуманизирует человека, упрощая его до ограниченного набора характеристик, выраженных в виде переменных, вводимых в прогнозную модель алгоритма».

Очередная проблема, потенциально ограничивающая реализацию принципа свободы, связана с тем, что в условиях правовой системы с высокой степенью персонализации возникают вопросы относительно уяснения содержания закона. В этом смысле можно говорить также о невозможности в определенных случаях реализовать конституционное право на информацию. В обычных условиях образованный человек может понять, как закон функционирует, обратившись к официальному тексту. Вместе с тем персонализированный закон может быть представлен в виде алгоритма и сложного набора взаимосвязанных, взаимоотсылающих норм. Это может вызвать необходимость обладания новыми навыками (например, в сфере науки о данных или программирования). Иначе может случиться, что даже законодатели будут испытывать сложности в понимании того, за что они проголосовали. Соответственно, если речь идет не просто о потребности в формальном разрешении определенного спора, персонализация может чинить препятствия для объективного анализа закона с целью установить, является ли он в целом «хорошим» (Verstein, 2019), правовым, справедливым.

¹¹ Perryer, S. (2019, May 22). *China's social credit system awards points to citizens who conform*. The New Economy. <https://www.theneweconomy.com/strategy/116498>

¹² Хартия основных прав Европейского Союза (2000).

В этой связи показательны решения Федерального Конституционного суда Германии, указавшего, что демократия предполагает в качестве необходимого условия непрерывные свободные дебаты между сталкивающимися между собой социальными силами, интересами и идеями, в процессе которых раскрываются и меняются политические цели, в результате которых общественное мнение придает предварительную форму политической воле. Это также подразумевает, что процедуры принятия решения органами, осуществляющими суверенную власть, и преследуемые политические цели в каждом случае должны быть в целом доступными для понимания и распознаваемыми. Данные соображения немецкий суд спроецировал на отношения государств внутри Европейского союза и признал в качестве необходимых критериев их интеграции¹³.

Безусловно, не каждое правовое предписание может быть эффективно рассмотрено на публичном или парламентском форуме. Тем не менее даже открытый дискурс в среде квалифицированных специалистов (ученых и практикующих юристов) имеет важнейшую демократическую легитимирующую силу, которая может быть кардинально уменьшена в результате глубоко укоренившейся алгоритмизации права (Bender, 2020).

Необходимо отметить, что угроза «рынку идей» еще более глубока и потому, что персонализация также влияет на самих участников дискурса, тем самым расшатывая его базис. Именно человеческое взаимодействие и общение обеспечивают согласованную позицию для принятия решения через призму нефактических, ценностных аргументов (в отличие от опоры на сугубо субъективные предпочтения). Для концепции гражданина, являющегося субъектом публичных дебатов, право судить является сущностным, тогда как потребитель может быть охарактеризован лишь определенным набором предпочтений. Можно предположить, что в мире персонализированного права одновременно с уменьшением ценности гражданина «пространство идей» рискует утратить не только свой предмет, но и субъектов (Bender, 2020).

Что касается принципа равенства (англ. “equality”), многие авторы не подвергают его глубокому критическому анализу — напротив, неоднократно подчеркивается, что персонализация может стимулировать равенство благодаря моделированию норм с учетом конкретных нюансов (Elkin-Koren & Gal, 2019).

Вместе с тем может бытовать и такое мнение, что персонализация и детализация де-факто несут в себе новые формы дискриминации, лишь замаскированные «техническим жаргоном». В сущности, есть конкретное опасение, что старые формы «грубой» дискриминации, полностью запрещенные на базе конституционно-правового регулирования, «вернутся через черный ход под маской психологически и научно обоснованного регулирования» (de Franceschi & Busch, 2018).

Многие авторы не усматривают противоречия между персонализированным правом и принципом равенства. Напротив, как утверждает Н. Элкин-Корен, персонализация права может уменьшить институционализированную дискриминацию (Elkin-Koren & Gal, 2019). В качестве примера можно привести укоренившуюся в потребительских отношениях невидимую, на первый взгляд, дискриминацию, вызванную использованием механизма перекрестного субсидирования, когда издержки, вызванные частой практикой возврата товара отдельными потребителями, закладываются в единую для всех покупателей цену за товар (Porat & Strahilevitz, 2014). Ф. Хакер отмечает, что принцип формального равенства может обуславливать применение разных норм, если анализ больших данных обнаруживает различия между индивидами (Hacker, 2017).

¹³ Order of the Second Senate (Bundesverfassungsgericht (BVerfG)), 2 BvR 1877/97, paras. 1–101 (1998); Order of the Second Senate (Bundesverfassungsgericht (BVerfG)), 2 BvL1/12, paras. 1–26 (2015).

В данном аспекте автор приводит позицию Суда справедливости Европейского союза, высказавшего утверждение о том, что дискриминация состоит лишь в применении разных правил к схожим ситуациям или в применении одного и того же правила к различным ситуациям¹⁴.

В дополнение к выводам суда хотелось бы отметить, что оценка релевантных индивидуальных различий должна быть составной частью законодательной процедуры, а не правоприменения. Этой позиции, в частности, придерживаются, А. де Франчески и К. Буш (de Franceschi & Busch, 2018). Авторы утверждают, что вопрос о том, отличаются ли две ситуации до такой степени, чтобы на них распространялся различный правовой режим, является нормативным, а не только эмпирическим. Исследователи также справедливо указывают на потребность в более проработанном теоретическом обосновании индивидуализации правовых норм.

Ф. Бендер гораздо более категоричен. По мнению ученого персонализация на основе личных предпочтений не может быть обоснована и, следовательно, неконституционна, если в перечень принимаемых во внимание алгоритмом предпочтений для принятия решения включены такие неоднозначные элементы, как, например, расовый фактор. Автор свидетельствует об очевидных сложностях критического анализа норм на базе ценностей, лежащих за пределами индивидуальных предпочтений (Bender, 2020).

На фоне высказываний авторов, утверждающих о совместимости персонализации права с принципом формального равенства благодаря усилению «осозаемости» релевантных индивидуальных различий (Hacker, 2017), важно выделить две особенности алгоритма, которые упускаются из виду и вызывают обоснованные опасения.

Первая особенность непосредственно связана с элементом субъективной воли и критерием объективности ее отражения алгоритмом (Grigoleit & Bender, 2019). Поскольку алгоритмы производят оценку предпочтений посредством анализа доступных данных, вполне можно допустить, что эти данные будут неполностью отражать реальную волю субъекта в конкретный момент времени, т. к. персонализированная норма опирается на презюмированные персональные предпочтения, отсутствие их в действительности делает норму произвольной.

Вторая особенность не связана с вопросом «улавливания» реальной воли лица, а относится лишь к внешнему аспекту — точности самого алгоритма. Существует опасение, что неточность анализа данных или неполнота данных, которые алгоритм должен принимать в расчет, могут способствовать формированию не соответствующих действительности профайлов. Необъективность может также вытекать из факта опоры алгоритма на ранее принятые им же самим решения (эффект домино). Представляется, что подобная непредсказуемость может привести к тому, что граждане будут действовать стратегически, намеренно стараясь избежать «попадания» определенных их действий (Elkin-Koren & Gal, 2019) в совокупность данных, анализируемых для принятия решения.

Помимо недостатков точности самого алгоритма человек также может намеренно «подгонять» факты, транслируемые в обрабатываемые алгоритмом данные, для достижения наиболее благоприятного для себя персонализированного правового режима. В таком контексте желание государства скрыть особенности функционирования алгоритмов для предотвращения манипулирования ими субъектов в интересах личной выгоды может быть вполне оправданным (Barry et al., 2020). Дело в том, что если в соответствии с принципом прозрачности, а тем более той логикой, что права и обязанности должны быть закреплены в законе¹⁵, алгоритмы являются прозрачными, то может возникнуть фактическое неравенство граждан

¹⁴ *Firma A. Racke v. Hauptzollamt Mainz*, ECJ (1984).

¹⁵ Терещенко, Л. К. Правовой режим информации: дис. ... д-ра юрид. наук: 12.00.14. М., 2011. С. 107.

вследствие существенных различий в уровне познаний в сфере информационных технологий или попросту неоднородности индивидуальных побудительных мотивов и проявления оппортунистического поведения. Получаемый на выходе результат в таком случае, безусловно, идет вразрез с изначальным смыслом персонализации и может сложиться так, что она будет приносить больше вреда, чем пользы (Barry et al., 2020). В качестве примера подобных нежелательных для регулятора действий можно привести случай Уго Батлера, который за короткое время возвел на первую строчку рейтинга авторитетного веб-портала рекомендаций TripAdvisor несуществующий ресторан¹⁶, ставший основным объектом внимания клиентской аудитории. Учитывая неудачи интернет-гигантов в борьбе с такого рода махинациями и демократически необходимую прозрачность порядка принятия решений алгоритмом, сложно представить, что люди не воспользуются возможностями для манипуляции персонализированными нормами в своих интересах. Таким образом, может возникнуть порочный круг, когда персонализация на основе скрытых алгоритмов может приводить к ущемлению права человека на информацию, а обеспечение их прозрачности — к получению необоснованной выгоды и социальному неравенству.

Сказанное позволяет взглянуть на стандартизированные правовые нормы с нового ракурса и обнаружить их некоторую недооцененность. Так, А. де Франчески и К. Буш (de Franceschi & Busch, 2018) отмечают, что, возможно, одним из преимуществ типифицированных правовых норм является то, что, имея приблизительный характер, они намеренно игнорируют персональные детали и тем самым даруют защитное пространство индивидуальной свободы, в которое право не ступает, и могут играть важную роль для социальной конструкции равенства. Ф. Бендер (Bender, 2020) также делает акцент на их преимуществах по сравнению с персонализированными нормами и высказывает сомнения относительно возможности каким-то образом обеспечить исключение из алгоритмического анализа больших данных неоднозначных факторов, требующих общественного обсуждения. Другими словами, неясно, существуют ли достаточные эффективные механизмы комплаенса для алгоритмов.

Принцип равенства, таким образом, отсылает каждую правовую норму к минимальным требованиям разумности, которым личные предпочтения могут удовлетворять только в связке с общеполитическими ориентирами (Grigoleit & Bender, 2019). Индивидуальные предпочтения относятся преимущественно к категории «сущего», однако для обретения ими правового характера необходимо наладить их взаимосвязь с категорией «должного».

Заключение

По результатам проведенного исследования наиболее оптимальным доктринальным подходом к пониманию персонализированного права видится концепция «мягкого позитивизма», обеспечивающего равновесие между социологической фактичностью права и нормативизмом.

В качестве основных признаков персонализированного права предлагается выделить следующие: 1) зависимость от степени распространенности и использования цифровых устройств и технологий; 2) зависимость от количества и качества доступных данных, в особенности — персональных данных; 3) правотворчество преимущественно на базе алгоритмической обработки и анализа данных; 4) правореализация и доведение информации до субъекта, как правило, посредством смарт-устройств.

¹⁶ Савченко, Г. (2017, Декабрь 7). *Журналист превратил задний двор дома в лучший ресторан Лондона по версии TripAdvisor*. Bird in Flight. <https://birdinflight.com/ru/novosti/20171207-tripadvisor-fake-restaurant.html>

Исследование позволило обнаружить, что персонализированное право может противоречить праву на свободу, праву на информацию, праву на неприкосновенность частной жизни, принципам формального равенства и недискриминации, а также достоинства личности.

Автор предлагает определить понятие персонализированного права как систему принятых или признанных государством норм, индивидуализированных на основе анализа персональных данных лица, в том числе информации о его физиологических и психических характеристиках, культурных особенностях, интересах и предпочтениях, преимущественно посредством алгоритмической обработки данных с обеспечением мер, направленных на соблюдение прав и свобод человека.

Алгоритмы, предназначенные для разработки правовых норм, не должны превышать ту степень детализации на основе индивидуальных предпочтений, которая может привести к ущемлению свободы выбора субъекта, и должны учитывать общепризнанные ценности. Судья должен пользоваться свободой усмотрения в пределах фундаментальных ценностных норм, обеспечивая баланс между правовыми принципами и эффективностью алгоритмов.

Учитывая трудноразличимую многоаспектность проблематики имплементации фундаментальных прав в структуру алгоритмов, целесообразна подготовка в дальнейшем особых кадров — специалистов, обладающих одновременно фундаментальными юридическими знаниями, профессиональными навыками в области компьютерных наук и принимающих непосредственное участие в разработке алгоритмов для персонализированного правового регулирования и их аудите в интересах граждан.

Избрание профессионалов с такими компетенциями представительной властью в качестве независимых экспертов-наблюдателей также может способствовать обеспечению прозрачности и соблюдения прав человека.

В целях надлежащего функционирования системы персонализированной регуляции необходим менеджмент качества данных с точки зрения их достоверности и полноты, а также внедрение процедур аудита алгоритмов.

Как представляется, на первых порах можно допустить персонализацию в тех сферах правоотношений, где это проще осуществить и связано с наименьшими рисками для прав человека. В форме законодательного эксперимента можно провести персонализацию в области обязательного раскрытия информации или диспозитивных норм о механизмах договорной защиты. Институт наследования по закону также может быть такой «тестовой» сферой правоотношений, персонализированной на основе достоверных данных.

Список литературы / References:

1. Abdrakhmanova, G. I., Vishnevskiy, K. O., & Gokhberg, L. M. (Eds.). (2019). *Chto takoye tsifrovaya ekonomika? Trendy, kompetentsii, izmereniye: Doklad k XX Aprel'skoy mezhdunarodnoy nauchnoy konferentsii po problemam razvitiya ekonomiki i obshchestva* [What is the digital economy? Trends, competencies, measurement: Report to the XX April International Scientific Conference on the development of economy and society]. Izdatel'skiy dom Vysshey Shkoly Ekonomiki.
2. Ayres, I. (1993). Preliminary thoughts on optimal tailoring of contractual rules. *Southern California Interdisciplinary Law Journal*, 3, 1–18.
3. Barry, J. M., Hatfield, J. W., & Kominers, S. D. (2020). To thine own self be true? Incentive problems in personalized law. *San Diego Legal Studies Paper No. 20–439*. <http://dx.doi.org/10.2139/ssrn.3536174>
4. Belyavskiy B. A. (2020). «Vrag moyego vraga», ili Ob obyedinyayushchem potentsiale rynochnogo radikalizma. *Retsenziya na knigu: Posner E. A., & Weyl G. E. (2018). Radical markets: Uprooting capitalism and democracy*

- for a just society. Princeton University Press [“The enemy of my enemy”, or on the unifying potential of market radicalism. Book review: Posner E. A., & Weyl G. E. 2018. Radical markets: Uprooting capitalism and democracy for a just society. Princeton University Press]. *Ekonomicheskaya Sotsiologiya*, 21(2), 76–90.
5. Bender, P. M. (2020). Limits of Personalization of default rules — Towards a normative theory. Working Paper 2020–02. Max Planck Institute for Tax Law and Public Finance.
 6. Bratanovskiy, S. N., & Ostapets, O. G. (2019). Konstitutsionnoye pravo Rossiyskoy Federatsii: Uchebnik dlya vuzov [Constitutional law of the Russian Federation: Textbook for universities]. Direkt-Media.
 7. Busch, C. (2019). Implementing personalized law: Personalized disclosures in consumer law and data privacy law. *The University of Chicago Law Review*, 86(2), 309–332. <https://lawreview.uchicago.edu/publication/implementing-personalized-law-personalized-disclosures-consumer-law-and-data-privacy-law>
 8. Casey, A. J., & Niblett, A. (2019). Framework for the new personalization of law. *The University of Chicago Law Review*, 86(2), 333–358. <https://lawreview.uchicago.edu/publication/framework-new-personalization-law>
 9. De Franceschi, A., & Busch, C. (2018). Granular legal norms: Big Data and the personalization of private law. In V. Mak, E. T. T. Tai, & A. Berlee (Eds.), *Research handbook on data science and law*. (pp. 17). Edward Elgar.
 10. Dvorkin, R. (2004). O pravakh vser'yey [Taking rights seriously]. ROSSPEN.
 11. Ehrlich, I., & Posner, R. A. (1974). An economic analysis of legal rulemaking. *The Journal of Legal Studies*, 3(1), 257–286. <http://dx.doi.org/10.1086/467515>
 12. Elkin-Koren, N., & Gal, M. S. (2019). The chilling effect of Governance-by-Data on data markets. *The University of Chicago Law Review*, 86 (2), 403–432.
 13. Geis, G. S. (2006). An experiment in the optimal precision of contract default rules. *Tulane Law Review*, 80, Article 1109.
 14. Grigoleit, H. C., & Bender, P. (2019). The law between generality and particularity — Chances and limits of personalized law. In C. Busch, & A. de Franceschi (Eds.), *Data economy and algorithmic regulation: A handbook on personalized law* (pp. 45). Beck C. H.
 15. Hacker, P. (2017). Personalizing EU private law: From disclosures to nudges and mandates. *European Review of Private Law*, 25(3), 651–678.
 16. Isztin, P. (2019). Eric Posner and E. Glen Weyl, radical markets: Uprooting capitalism and democracy for a just society. *Oeconomia*, 9(4), 873–880. <https://doi.org/10.4000/oeconomia.6984>
 17. Kaminski, M. E., & Witnov, S. (2015). The conforming effect: First Amendment implications of surveillance, beyond chilling speech. *University of Richmond Law Review*, 49, 465–518. <https://lawreview.richmond.edu/2015/01/15/the-conforming-effect-first-amendment-implications-of-surveillance-beyond-chilling-speech/>
 18. Karbon'ye, ZH. (1986). Yuridicheskaya sotsiologiya (V. A. Tumanova, Per. i Vstup.). [Legal sociology (V. A. Tumanova, Trans. and Intr.)]. Progress.
 19. Kasatkin, S. N. (2008). Osnovnyye idei «Postskriptuma» Herbert L. A. Kharta [The main ideas of “Postscript” by Herbert L. A. Hart]. *Vestnik Samarской Gumanitarnoy Akademii. Seriya “Pravo”*, (1), 3–26.
 20. Khayyek, F. A. (2018). Konstitutsiya svobody [The Constitution of Liberty]. Novoye Izdatel'stvo: Biblioteka Svobody.
 21. Khayyek, F. A. (1992). Pagubnaya samonadeyannost'. Oshibki sotsializma [Pernicious arrogance. The mistakes of socialism]. “Novosti” pri uchastii izd-va “Catallaxy”.
 22. Khizhnyakov, D. P., & Lebedev, S. D. (2011). Informatsionnyye bar'yery v sisteme gosudarstvennogo upravleniya [Information barriers in the public administration system]. *Nauchnyye Vedomosti BelGU. Seriya: Filosofiya. Sotsiologiya. Pravo*, 2(87), 223–232.

23. Kurzinski-Singer, E. (2011). Yurisprudentsiya tsennostey kak osnova metodiki nemetskogo prava [Jurisprudence of values as the basis of the methodology of German law]. *Nauchnyye Trudy Adilet*, (1), 87–94. <https://docplayer.ru/42965789-Yurisprudenciya-cennostey-kak-osnova-metodiki-nemeckogo-prava.html>
24. Nekhayev, A. V. (2019). Plokhoy zakon kak chistoye pravo: Kriticheskiye zametki k filosofii prava H. L. A. Kharta [Bad law as pure law: Critical notes to the concept of law of H. L. A. Hart]. *Vestnik TGU*, (440), 72–80. <http://doi.org/10.17223/15617793/440/10>
25. Porat, A., & Strahilevitz, L. J. (2014). Personalizing default rules and disclosure with Big Data. *Michigan Law Review*, 112(8), 1417–1478. <https://repository.law.umich.edu/mlr/vol112/iss8/2>
26. Savel'yev, A. I. (2019). Na puti k kontseptsii regulirovaniya dannykh v usloviyakh tsifrovoy ekonomiki [Towards a data regulation concept in the digital economy]. *Zakon*, (4), 174–195.
27. Sunstein, C. R. (2013). Deciding by default. *The University of Pennsylvania Law Review*, 162(1), 1–57. https://scholarship.law.upenn.edu/penn_law_review/vol162/iss1/1
28. Verstein, A. (2019). Privatizing personalized law. *The University of Chicago Law Review*, 86(2), 551–580. <https://lawreview.uchicago.edu/publication/privatizing-personalized-law>
29. Zeman, I. (1966). Poznaniye i informatsiya. Gnoseologicheskiye problemy kibernetiki (R. Ye. Mel'tser, Per.) [Knowledge and information. Epistemological problems of cybernetics (R. E. Melzer, Trans.)]. Progress.

Information about the author:

Tembot Z. Misostishkhov — LLM, National Research University Higher School of Economics (HSE University), Moscow, Russia.

tembotmisostishkhov@mail.ru

Сведения об авторе:

Мисостишхов Т.З. — магистр права, Национальный исследовательский университет «Высшая школа экономики», Москва, Россия.

tembotmisostishkhov@mail.ru

СТАТЬИ

МЕСТО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА СРЕДИ ЭЛЕМЕНТОВ СОСТАВА ПРАВООТНОШЕНИЯ

А.А. Васильев, Ю.В. Печатнова*

Алтайский государственный университет
656049, Россия, Алтайский край, Барнаул, пр-кт Социалистический, 68

Аннотация

Развитие искусственного интеллекта вызывает необходимость правового регулирования общественных отношений, связанных с применением новых технологий. На сегодняшний день в российском законодательстве отмечается фрагментарное нормативное регулирование, выраженное, как правило, в стратегических документах, где технологии искусственного интеллекта отражаются как сквозные, способствующие развитию цифровой экономики.

Цель настоящей работы — определение места искусственного интеллекта среди элементов состава правоотношения, что видится необходимым для построения модели правового регулирования искусственного интеллекта.

В статье проведен анализ подходов к определению места искусственного интеллекта в структуре правоотношения. Научная дискуссия состоит в том, что одни авторы относят искусственный интеллект к разновидности объектов правового регулирования; другие авторы допускают возможность рассматривать искусственный интеллект в качестве специфического субъекта права.

В результате проведенного исследования авторы приходят к выводу о том, что на сегодняшний день искусственный интеллект следует относить к разновидности объектов правового регулирования.

В заключение работы также дается оценка возможности и меры участия искусственного интеллекта в юридической деятельности. В настоящее время когнитивный потенциал искусственного интеллекта еще не достиг того уровня развития, который позволил бы ему повторить мыслительные процессы юриста при решении правового спора. Вместе с тем, искусственный интеллект имеет колоссальный потенциал стать незаменимым технологичным «помощником» юриста, способствующим улучшению качества и эффективности оказания юридических услуг.

Ключевые слова

искусственный интеллект, роботы, правовое регулирование, цифровое право, кибербезопасность

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Для цитирования

Васильев, А. А., Печатнова, Ю. В. (2020). Место искусственного интеллекта среди элементов состава правоотношения. *Цифровое право*, 1(4), 74–83. <https://doi.org/10.38044/2686-9136-2020-1-4-74-83>

* Автор, ответственный за переписку

Поступила: 18.06.2020, принята в печать: 01.09.2020, опубликована: 20.12.2020

ARTICLES

THE POSITION OF THE ARTIFICIAL INTELLIGENCE AMONG THE ELEMENTS OF THE LEGAL RELATIONSHIP

Anton A. Vasiliev, Yulia V. Pechatnova*

Altai State University
68, ave. Socialistichesky, Barnaul, Altai Region, Russia, 656049

Abstract

The development of artificial intelligence necessitates the legal regulation of social relations associated with the use of new technologies. Today, fragmented regulatory regulation is noted in Russian law, expressed, as the rule, in strategic documents in which artificial intelligence technologies are reflected as cross-cutting technologies that contribute to the development of the digital economy.

The purpose of this work is to determine the place of artificial intelligence among the elements of legal relations, which is seen as necessary for building the model of legal regulation of artificial intelligence.

The research methodology is based on the set of methods of scientific knowledge, including abstract logical, formal legal and the method of correlation analysis.

The article analyzes approaches to determining the place of artificial intelligence in the structure of legal relations. The scientific discussion is that some authors attribute artificial intelligence to the variety of objects of legal regulation; other authors admit that it is possible to consider artificial intelligence as the specific subject of law.

As the result of research, the authors come to the conclusion that today artificial intelligence should be classified as the type of objects of legal regulation.

In conclusion, the work also evaluates the possibilities and measures of the participation of artificial intelligence in legal activities. The authors come to the conclusion that today the cognitive potential of artificial intelligence has not yet reached the level of development that allowed it to repeat the thought processes of the lawyer in resolving the legal dispute. At the same time, artificial intelligence has tremendous potential to become the irreplaceable technological “assistant” for the lawyer, contributing to the improvement of the quality and efficiency of legal services.

Keywords

artificial intelligence, robots, legal regulation, digital law, cybersecurity

Conflict of interest

The authors declare no conflict of interest.

Financial disclosure

The study had no sponsorship.

For citation

Vasiliev, A. A., & Pechatnova, Yu. V. (2020). The position of the artificial intelligence among the elements of the legal relationship. *Digital Law Journal*, 1(4), 74–83. <https://doi.org/10.38044/2686-9136-2020-1-4-74-83>

* Corresponding author

Submitted: 18 Jul. 2020, accepted: 01 Sep. 2020, published: 20 Dec. 2020

Введение

В современных теоретико-правовых исследованиях активно обсуждаются проблемы правового регулирования общественных отношений, связанных с разработкой, производством и применением искусственного интеллекта.

Вместе с тем, разработка единого доктринального подхода к определению понятия и сущности искусственного интеллекта осложняется многогранностью изучаемого явления.

Так называемая парадигма «думай — действуй» отличает искусственный интеллект от других технологий (Calo, 2015), поэтому искусственный интеллект следует рассматривать через призму высокотехнологичной системы, оснащенной способностями ощущать, обрабатывать и оказывать воздействие на внешний мир.

Вместе с тем, физическое воплощение искусственного интеллекта в сочетании с автономностью действий придает роботам социальную валентность. Тем самым, наблюдается трансформация термина «искусственный интеллект» от технического к социально-ориентированному содержанию.

Эффект настолько систематичен, что команда выдающихся психологов и инженеров выдвинула аргумент в пользу новой онтологической категории для искусственного интеллекта, определяющей место искусственного интеллекта где-то между объектом и живым агентом (Calo, 2015).

Таким образом, проблема определения места искусственного интеллекта в социальном пространстве бросает вызов сложившимся правовым институтам.

В этой связи, целью работы стало выявление особенностей искусственного интеллекта как объекта правового регулирования и как субъекта права.

Практическая значимость обусловлена возможностью использовать полученные результаты исследования для совершенствования механизмов правового регулирования искусственного интеллекта в Российской Федерации.

Методология и результаты исследования

Теоретической основой исследования послужили труды отечественных и зарубежных ученых, посвященные анализу искусственного интеллекта как субъекта права и объекта правового регулирования, позволившие провести сравнительное исследование литературы, а также анализ программных и стратегических документов по изучаемому вопросу.

Появление искусственного интеллекта как научного явления произошло во второй половине XX века. Впервые термин был озвучен Джоном Маккарти на рабочей американской конференции в 1956 году, поэтому Джона Маккарти по праву можно назвать отцом-основателем сферы искусственного разума, наряду с Марвином Ли Минским, Алленом Ньюэллом, Гербертом Саймоном, Клодом Шенноном, Аланом Тьюрингом и другими (Larina & Ovchinskij, 2018).

Исторически первым подходом к определению понятия искусственного интеллекта можно назвать тест Алана Тьюринга, в соответствии с которым программное устройство следует считать искусственным интеллектом, если при общении с компьютером посредством анонимного канала связи нельзя понять, с кем идет беседа — с человеком или машиной.

В этой связи, первоначально правовое регулирование искусственного интеллекта обеспечивалось совокупностью технологических норм, регулирующих рациональное использование новых технологий.

Прогрессивное развитие технологии искусственного разума обусловило появление второго подхода к определению понятия «искусственный интеллект», в соответствии с которым отличительным критерием искусственного интеллекта является его способность к автономным действиям и самосовершенствованию.

Возможности автономного принятия решений искусственным интеллектом и их последующей реализации обусловили выход сферы искусственного разума за границы технологических норм и вызвали необходимость формирования комплекса дополнительных правовых норм для рационального применения и использования технологии.

Легальное определение понятия «искусственный интеллект» закреплено в Национальной стратегии развития искусственного интеллекта на период до 2030 года (далее — Национальная стратегия), утвержденной Указом Президента Российской Федерации от 10.10.2019 № 490.

Согласно Национальной стратегии 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. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений¹.

Итак, к признакам искусственного интеллекта относятся: наличие технического устройства; способность к принятию, обработке и передаче информации; способность к автономной работе; самообучение на основе анализа информации и приобретенного опыта; способность к принятию самостоятельных решений (Vasil'ev & Shproper, 2018).

Несмотря на некоторые преобразования в части стратегического нормотворчества, комплексное правовое регулирование искусственного интеллекта пока не выработано. Вероятно, сложность вызвана неопределенностью, связанной с отношением искусственного интеллекта к объектам правового регулирования или субъектам права.

При рассмотрении искусственного интеллекта в рамках исторически первого подхода, иными словами, как инновационного технического средства, его следует относить к объектам правового регулирования, на которые воздействует право.

Учитывая второй подход, подчеркивающий способность искусственного разума к самостоятельному принятию решений, искусственный интеллект может рассматриваться как субъект права, способный реализовывать субъективные права и осуществлять юридические обязанности. Специалисты-правоведы, изучающие искусственный интеллект, склонны именовать его либо специфическим объектом права, либо квази-субъектом права.

¹ Указ Президента РФ № 490 «О развитии искусственного интеллекта в Российской Федерации» (2019).
http://www.consultant.ru/document/cons_doc_LAW_335184/

Исходя из вышесказанного, искусственный интеллект нельзя в полной мере относить ни к объектам, ни к субъектам права. Иными словами, искусственный интеллект уже нельзя считать классическим объектом правового регулирования, но еще нельзя рассматривать как полноценный субъект права по следующим причинам:

1. Традиционная концепция о субъектах права исходит из того, что участниками правоотношений являются физические и юридические лица.

2. Попытки сравнения искусственного интеллекта с физическими лицами не выдерживают критики с точки зрения физиологии.

3. Когнитивные способности искусственного интеллекта весьма ограничены в сравнении с человеческими функциями мозга.

Несмотря на то, что искусственная нейронная сеть построена по принципу функционирования нервных клеток живого организма, она значительно уступает строению биологической нейронной сети по количеству слоев нейронов. Также в искусственных нейронных сетях слои нейронов срабатывают последовательно; в человеческом мозге обмен информацией между нейронами идет параллельно и асинхронно. Именно поэтому попытки полноценного замещения человеческого мозга искусственным интеллектом несостоятельны, т. к. искусственная нейросеть всегда будет подобием, не способным повторить оригинала.

Ввиду того, что юридические лица являются субъектами права фиктивно, по аналогии с ними искусственный интеллект может также обладать некоторыми признаками субъекта права. Например, иметь регистрацию и учетный номер, обладать производственно-хозяйственной компетенцией, соответствующей целям его деятельности; обладать материальной ценностью; его можно привлечь к юридической ответственности (например, в виде принудительного отключения или доработки программы, а также утилизации) (Laptev, 2019).

Такая аналогия предвосхищает идею того, что искусственный интеллект вполне обоснованно можно рассматривать как очередную юридическую фикцию, созданную в целях упрощения правового регулирования.

В научной литературе предлагается самостоятельный термин, обозначающий искусственный интеллект как субъекта права — «электронное лицо» — и являющийся исключительно юридической формулировкой, а не биоэтической или философской констатацией (Morhat, 2018).

Однако указанная позиция поддерживает интересы разработчиков искусственного интеллекта, освобождая их от социальной и юридической ответственности за последствия своих разработок (Cukanova & Skopenko, 2018). Кроме того, в отличие от нематериального юридического лица, искусственный интеллект материален (если речь идет о роботах, беспилотных автомобилях) или закреплен на материальных носителях — компьютерах (если речь идет о программах).

В научной литературе получил распространение термин «квази-субъект» права, под которым понимается субъект права, не обладающий полноценной правосубъектностью (Golubsov, 2019). Некоторые авторы относят к разновидности квази-субъектов публично-правовые образования (Andreev, 2005). Однако даже для квази-субъектов права характерно наличие такого качества правосубъектности как воля, которой искусственный интеллект не обладает.

Итак, способность к самообучению и автономной деятельности не является достаточным основанием для наделения искусственного интеллекта правосубъектностью. Следует отметить, что с позиции гражданского законодательства к животным применяются общие правила об имуществе, несмотря на их высокие когнитивные способности, возможности самообучения и самосовершенствования.

Таким образом, в ближайшее время искусственный интеллект следует рассматривать в качестве объекта права согласно положениям ст. 128 Гражданского кодекса РФ (далее — ГК РФ) об объектах гражданских прав².

По аналогии со ст. 1079 ГК РФ ответственность за деятельность, связанную с применением искусственного интеллекта, должны нести лица, использующие искусственный интеллект как объект повышенной опасности.

В случае встроенного дефекта или программирования с ошибкой в коде ответственность в порядке регресса может быть возложена на производителя или разработчика искусственного интеллекта.

Дискуссия

В научной литературе отсутствует однозначная позиция в решении проблемы места искусственного интеллекта в социальном пространстве.

С одной стороны, нельзя игнорировать концептуальные и практические аргументы в пользу статуса искусственного интеллекта, сравнимого со статусом физического лица. С другой стороны, признание искусственного интеллекта субъектом права посягает на исключительный статус человека. Поэтому идеальным решением может быть статус «на полпути» или «между ними».

Примером такого «решения на полпути» может служить концепция *Teilrechtsfähigkeit* из гражданского права Германии, под которой понимается частичная правоспособность. Так, применение концепции *Teilrechtsfähigkeit* к искусственному интеллекту одновременно отразит автономность искусственного интеллекта и заполнит большую часть «пробелов ответственности» без негативных побочных эффектов для человека (Schirmer, 2019).

В. А. Шестак и А. Г. Волеводз также проводят анализ идеи наделения правосубъектностью искусственный интеллект и указывают следующие признаки «разумности» роботов: умение анализировать данные; способность адаптировать свое поведение; автономия и возможность самообучения (Shestak & Volevodz, 2019).

Вместе с тем, авторы подтверждают правовую необоснованность признания искусственного интеллекта субъектом права ввиду того, что искусственный интеллект не является носителем критически важных составляющих личности (души, свободного сознания, чувств, интенциональности, личных интересов). Поэтому, несмотря на сверхмощную скорость обработки информации, в разы превосходящую возможности человека, искусственный интеллект остается программой с привязанным к ней материально-техническим обеспечением (Shestak & Volevodz, 2019).

В научной литературе нередко освещается идея отнесения искусственного интеллекта к объектам правового регулирования по аналогии с правовым режимом, предусмотренным для животных.

Так, например, А. В. Малышкин допускает возможность внесения изменений в гражданское законодательство в части предоставления права требования компенсации морального вреда за уничтожение человекоподобных роботов, наделенных искусственным интеллектом, если будет доказано, что между человеком и человекоподобным роботом существовала сильная эмоциональная связь и утрата робота повлекла переживания человека, либо существенно ухудшила условия его жизни (например, слепой человек лишился робота-поводыря) (Malyshekin, 2019).

Среди альтернативных позиций по поводу характеристики термина «искусственный интеллект» следует отметить версию, согласно которой искусственный интеллект может рассматриваться

² Гражданский кодекс Российской Федерации (часть первая) № 51-ФЗ (в ред. 21.05.2020) (1994).
http://www.consultant.ru/document/cons_doc_LAW_5142/f7871578ce9b026c450f64790704bd48cd94bcb/

как еще одна Вавилонская башня, иными словами, еще один пример попытки человечества узурпировать положение Бога в мире (Campbell & Garner, 2016).

На наш взгляд, идея поглощения искусственным интеллектом внутреннего мира человека и превращения в глобальный объект поклонения является бесосновательно преувеличенной. Вместе с тем, эта идея подчеркивает правовые риски, возникающие при разработке искусственного интеллекта, и важность моральной ответственности инженеров-робототехников, изначально вынужденных создавать роботов с учетом этических норм и правил (Asaro, 2007).

Следует отметить, что полемика о правовой сущности искусственного интеллекта не ограничивается дискуссией о наделении искусственного интеллекта правосубъектностью (Begishev et al., 2020).

Мощный когнитивный потенциал искусственного интеллекта позволяет говорить о технической возможности делегирования юридических задач искусственному интеллекту.

С одной стороны, кодирование правовой информации не может точно передать богатство и неоднозначность юридических категорий (таких, например, как «справедливость», «вина» и др.). Более того, сами юристы не всегда могут точно сформулировать методы и мыслительные процессы, сопровождающие их деятельность. Поэтому юристы, которые не привыкли к строгим требованиям языка программирования, будут разочарованы разрывом между тем, что они хотят сказать, и тем, что им позволяет сказать язык программирования. С этой точки зрения делегирование работы юриста компьютеру выглядит крайне проблематичным (Buchanan & Headrick, 1970).

С другой стороны, процесс принятия юридического решения проходит конкретные стадии: определение юридической задачи, установление фактического состава, юридическая квалификация (соотнесение фактического состава с юридической нормой), поиск аналогий. В этой связи, данный процесс подчиняется определенным алгоритмам, которые позволяют моделировать и переносить на язык программирования различные виды юридической деятельности, способствуя тем самым созданию логической, недвусмысленной, последовательной и стабильной правовой системы (Buchanan & Headrick, 1970).

Кроме того, ввиду способности молниеносно анализировать, сопоставлять, обрабатывать массивы информации, оставаться беспристрастным и сохранять нейтралитет, имея безупречную репутацию, (Gadzhiiev, 2018) искусственный интеллект, выступающий в качестве судьи, представляется идеалом правосудия, выраженного в цифровой объективности (Zaplalina, 2019).

Вместе с тем, видится, что запрограммированное единственно верное юридическое решение, исключающее возможность альтернативы, не является справедливым. Категория справедливости неоднозначна и в каждом конкретном случае имеет специфическое содержание, которое пока еще не верифицируется компьютерными технологиями.

Закон должен быть относительно стабилен во времени, в то время как регулируемые им общественные отношения динамичны и изменчивы, как изменчива и оценка этих отношений. Поэтому участие человека в разрешении правовых споров необходимо рассматривать как социально-оправданный элемент творческой деятельности юриста.

Таким образом, проведенный анализ различных точек зрения подтверждает вывод о том, что искусственный интеллект следует рассматривать не в качестве самостоятельного субъекта, автономно принимающего юридические решения, а в качестве объекта — технологии, способствующей снижению технической нагрузки на юриста.

Так, например, новые технологии уже сейчас значительно упрощают поиск судебной практики и нормативного материала для формирования правовой позиции по делу

или вынесения решения. Для действующей системы судопроизводства в перспективе видится возможным, безболезненным и эффективным автоматизировать вынесение стандартных определений суда об оставлении искового заявления без движения в случае несоответствия формальным критериям, об отложении судебного заседания, судебных решений в рамках приказного или упрощенного производства.

По состоянию на сегодняшний день онлайн-платформы ГАС «Правосудие» и «Мой Арбитр» при некоторых технологических усовершенствованиях и под чутким контролем специалистов позволяют провести подобные эксперименты автоматического формирования стандартных определений или решений суда в рамках гражданского или административного судопроизводства.

Заключение

Развитие искусственного интеллекта требует преобразования правового регулирования общественных отношений, связанных с его участием (Cherkasov, 2017).

Искусственный интеллект представляет собой программно-вычислительный комплекс, функционирующий посредством заранее заданного алгоритма со встроенной способностью к самообучению, в связи с чем, позволяющий имитировать когнитивные функции человека и автономно выполнять конкретные задачи или производить результаты, сопоставимые с интеллектуальной деятельностью человека.

Выявили следующие юридически значимые признаки искусственного интеллекта:

- опосредованное функционирование с использованием технического устройства;
- способность к самообучению;
- способность автономно вырабатывать интеллектуальные решения и реализовывать их.

Модель правового регулирования искусственного интеллекта напрямую зависит от определения места искусственного интеллекта среди элементов правоотношения.

Проблема отнесения искусственного интеллекта к субъекту или объекту правоотношения является дискуссионной в юридической науке (Somenkov, 2019).

На основе проведенного исследования, авторы приходят к выводу о том, что относить искусственный интеллект к разновидности субъектов правоотношения преждевременно и нецелесообразно.

В этой связи, следуя логике теории правоотношений, искусственный интеллект по состоянию на сегодняшний день следует относить к объектам правового регулирования.

Стремительное развитие и усовершенствование искусственного интеллекта не гарантирует продолжительного существования указанной точки зрения. Вместе с тем, даже сверхмощный и усовершенствованный искусственный разум является максимально упрощенной моделью созданного миллионами лет эволюции человеческого мозга. Поэтому сопоставление искусственного интеллекта с человеком недопустимо ни с точки зрения физиологии, ни с точки зрения юриспруденции.

Вопрос об отнесении искусственного интеллекта к конкретной разновидности объектов права остается дискуссионным. Одни авторы предлагают относить искусственный интеллект к интеллектуальной собственности по аналогии с программами для электронных вычислительных машин. Другие авторы склонны применять к искусственному интеллекту (роботу) общие правила об имуществе по аналогии с животными (Laptev, 2019).

Таким образом, остаются актуальными существующий пробел в праве и необходимость дальнейшего исследования проблем правового регулирования искусственного интеллекта.

Список литературы / References:

1. Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, 103(3), 513–563.
2. Larina, E. S., & Ovchinskij, V. S. (2018). Iskusstvennyj intellekt. Bol'shie dannye. Prestupnost' [Artificial intelligence. Big data. Crime]. Knizhnyj mir.
3. Vasil'ev, A. A., & Shpopov, D. (2018). Iskusstvennyj intellekt: Pravovye aspekty [Artificial intelligence: Legal aspects]. *Izvestia ASU*, 6(104), 23–26. [https://doi.org/10.14258/izvasu\(2018\)6-03](https://doi.org/10.14258/izvasu(2018)6-03)
4. Laptev, V. A. (2019). Ponyatie iskusstvennogo intellekta i yuridicheskaya otvetstvennost' za ego rabotu [The concept of artificial intelligence and legal responsibility for its work]. *Pravo. Zhurnal Vyshey Shkoly Ekonomiki*, (2), 79–102. <https://doi.org/10.17323/2072-8166.2019.2.79.102>
5. Morhat, P. M. (2018). K voprosu o pravosub'ektnosti "elektronnogo lica" [On the issue of legal personality of an "electronic person"]. *Legal Studies*, (4), 1–8. <https://doi.org/10.25136/2409-7136.2018.4.25647>
6. Cukanova, E. Yu., & Skopenko, O. R. (2018). Pravovye aspekty otvetstvennosti za prichinenie vreda robotom s iskusstvennym intellektom [Legal aspects of liability for harm caused by a robot with artificial intelligence]. *Voprosy Rossijskogo i Mezhdunarodnogo Prava*, 8(2A), 42–48.
7. Golubcov, V. (2019). Rossijskaya Federaciya kak sub'ekt grazhdanskogo prava [The Russian Federation as a subject of civil law]. Statute.
8. Andreev, Yu. N. (2005). Uchastie gosudarstva v grazhdansko-pravovyh otnosheniyah [Participation of the state in civil law relations]. Yurid. Centr Press.
9. Schirmer, J.-E. (2019). Artificial intelligence and legal personality: Introducing "Teilrechtsfähigkeit": A partial legal status made in Germany. *Regulating Artificial Intelligence*, 123–142. https://doi.org/10.1007/978-3-030-32361-5_6
10. Shestak, V. A., & Volevodz, A. G. (2019). Sovremennye potrebnosti pravovogo obespecheniya iskusstvennogo intellekta: Vzglyad iz Rossii [Modern requirements of the legal support of artificial intelligence: A view from Russia]. *Russian Journal of Criminology*, 13(2), 197–206. [https://doi.org/10.17150/2500-4255.2019.13\(2\).197-206](https://doi.org/10.17150/2500-4255.2019.13(2).197-206)
11. Malyshkin, A. V. (2019) Integrirovaniye iskusstvennogo intellekta v obshchestvennyuyu zhizn': Nekotorye eticheskie i pravovye problemy [Integration of artificial intelligence into public life: Some ethical and legal problems]. *Vestnik of Saint Petersburg University. Law*, 10(3), 444–460. <https://doi.org/10.21638/spbu14.2019.303>
12. Campbell, H. A., & Garner, S. (2016). *Networked theology: Negotiating faith in digital culture*. Baker Academic.
13. Asaro, P. (2007). Robots and responsibility from a legal perspective. *Proceedings of the IEEE*, 4(14), 20–24.
14. Begishev, I. R., Latypova, E. Yu., & Kirpichnikov, D. V. (2020). Iskusstvennyj intellekt kak pravovaya kategoriya: Doktrinal'nyj podhod k razrabotke definicii [Artificial intelligence as the legal category: Doctrinal approach to developing the definition]. *Aktual'nye Problemy Ekonomiki i Prava*, 14(1), 79–91. <https://doi.org/10.21202/1993-047X.14.2020.1.79-91>
15. Buchanan, B. G., & Headrick, T. E. (1970). Some speculation about artificial intelligence and legal reasoning. *Stanford Law Review*, 23(1), 40–62. https://digitalcommons.law.buffalo.edu/journal_articles/867
16. Gadzhiev, G. A. (2018). Yavlyaetsya li robot-agent licom? (Poisk pravovyh form dlya regulirovaniya cifrovoj ekonomiki) [Whether the robot-agent is a person? (Search of legal forms for the regulation of digital economy)]. *Journal of Russian Law*, (1), 15–30. https://doi.org/10.12737/art_2018_1_2
17. Zaplatina, T. S. (2019). Iskusstvennyj intellekt v voprose vyneseniya sudebnyh reshenij, ili II-sud'ya [Artificial intelligence in the passing sentences issues or AI judge]. *Courier of Kutafin Moscow State Law University (MSAL)*, (4), 160–168. <https://doi.org/10.17803/2311-5998.2019.56.4.160-168>
18. Cherkasov, V. N. (2017). Novyj sub'ekt prava? [A new subject of law?]. *Bazis*, 1(1), 41–44.

19. Somenkov, S. A. (2019). Iskusstvennyj intellekt: Ot ob"ekta k sub"ektu? [Artificial intelligence: From object to subject?]. *Courier of Kutafin Moscow State Law University (MSAL)*, (2), 75–85. <https://doi.org/10.17803/2311-5998.2019.54.2.075-085>

Вклад авторов:

Васильев А.А. — научное редактирование, общая постановка исследовательской проблемы, исследование искусственного интеллекта с точки зрения субъекта права, проведение сравнительного анализа искусственного интеллекта с иными участниками правоотношения: физическими и юридическими лицами, публично-правовыми образованиями, анализ масштабов и форм влияния искусственного интеллекта на юридическую деятельность.

Печатнова Ю.В. — научное редактирование, определение методологии исследования, исследование искусственного интеллекта с точки зрения объекта правового регулирования, сопоставление искусственного интеллекта с иными объектами правового регулирования, анализ возможности участия искусственного интеллекта в юридической деятельности.

The authors' contribution:

Anton A. Vasiliev — did scientific editing; formulated the general research problem; investigated the artificial intelligence as the subject of law, carried out the comparative analysis of artificial intelligence with other participants in the legal relationship: individuals and legal entities, public law formations; researched the scale and forms of influence the artificial intelligence on legal activities.

Yulia V. Pechatnova — did scientific editing; developed the research methodology; investigated the artificial intelligence as the object of legal regulation, carried out the comparison of artificial intelligence with other objects of legal regulation, researched the possibility of participation of artificial intelligence in legal activities.

Сведения об авторах:

Васильев А.А. — доктор юридических наук, профессор, директор юридического института, заведующий кафедрой теории и истории государства и права Алтайского государственного университета, Барнаул, Россия
ORCID 0000-0003-3122-531X

Печатнова Ю.В.* — магистрант юридического института Алтайского государственного университета, Барнаул, Россия.
ORCID 0000-0003-3091-990X
jp_0707@mail.ru

Information about the authors:

Anton A. Vasiliev — Dr. Sci. in Law, Associate Professor, Head of the Faculty of Law, and Department of Theory and History of State and Law, Altai State University, Barnaul, Russia.
ORCID 0000-0003-3122-531X

Yulia V. Pechatnova* — Master's student, Altai State University, Barnaul, Russia.
ORCID 0000-0003-3091-990X
jp_0707@mail.ru

