



ISSN 2949-2483

Volume

1

Number

3

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2023

ELECTRONIC
SCIENTIFIC
AND PRACTICAL
JOURNAL





Редакционная коллегия

Шеф-редактор

Бегишев Ильдар Рустамович – доктор юридических наук, доцент, заслуженный юрист Республики Татарстан, главный научный сотрудник Научно-исследовательского института цифровых технологий и права, профессор кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова (Казань, Российская Федерация)

Главный редактор

Жарова Анна Константиновна – доктор юридических наук, доцент, директор Центра исследований киберпространства, ассоциированный член международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам» Национального исследовательского университета «Высшая школа экономики», старший научный сотрудник Института государства и права Российской академии наук (Москва, Российская Федерация)

Заместители главного редактора

Громова Елизавета Александровна – кандидат юридических наук, доцент, заместитель директора Юридического института по международной деятельности, доцент кафедры предпринимательского, конкурентного и экологического права Южно-Уральского государственного университета (Национального исследовательского университета) (Челябинск, Российская Федерация)

Залоило Максим Викторович – кандидат юридических наук, ведущий научный сотрудник отдела теории права и междисциплинарных исследований законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации (Москва, Российская Федерация)

Филипова Ирина Анатольевна – кандидат юридических наук, доцент, доцент кафедры трудового и экологического права Национального исследовательского Нижегородского государственного университета имени Н. И. Лобачевского (Нижний Новгород, Российская Федерация)

Шутова Альбина Александровна – кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова (Казань, Российская Федерация)

Редакция

Заведующий редакцией – Дарчинова Гульназ Язкарвна

Выпускающий редактор – Аймурзаева Оксана Анатольевна

Ответственный секретарь – Лапшина Анастасия Денисовна

Редактор – Тарасова Гульнара Абдулахатовна

Технический редактор – Каримова Светлана Альфредовна

Художник-дизайнер – Загреддинова Гульнара Ильгизаровна

Переводчик – Беляева Елена Николаевна, кандидат педагогических наук, член Гильдии переводчиков Республики Татарстан

Специалист по продвижению журнала в сети Интернет –

Гуляева Полина Сергеевна

Адрес: 420111, Российская Федерация,

г. Казань, ул. Московская, 42

Телефон: +7 (843) 231-92-90

Факс: +7 (843) 292-61-59

E-mail: lawjournal@ieml.ru

Сайт: <https://www.lawjournal.digital>

Telegram: <https://t.me/JournalDTL>

ВКонтакте: <https://vk.com/JournalDTL>

Яндекс.Дзен: <https://dzen.ru/JournalDTL>

Одноклассники: <https://ok.ru/JournalDTL>

Учредитель и издатель

Казанский инновационный университет имени В. Г. Тимирязова. Адрес: 420111, Российская Федерация, г. Казань, ул. Московская, 42. Телефон: +7 (843) 231-92-90. Факс: +7 (843) 292-61-59. E-mail: info@ieml.ru. Сайт: <https://ieml.ru>



© Казанский инновационный университет имени В. Г. Тимирязова, оформление и составление, 2023.

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации средства массовой информации: ЭЛ № ФС 77-84090 от 21 октября 2022 г. Территория распространения: Российская Федерация; зарубежные страны.

Статьи находятся в открытом доступе и распространяются в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа процитирована с соблюдением правил цитирования.

Важно!

16+

При цитировании любых материалов журнала ссылка обязательна. Ответственность за изложенные в статьях факты несут авторы. Высказанные в статьях мнения могут не совпадать с точкой зрения редакции и не налагают на нее никаких обязательств.

Возрастная классификация: Информационная продукция для детей, достигших возраста шестнадцати лет.

Дата подписания к публикации – 15 августа 2023 г. Дата онлайн-размещения на сайте <https://www.lawjournal.digital> – 20 августа 2023 г.

Международные редакторы

Галлезе-Нобиле Кьяра – доктор наук, научный сотрудник (постдок) по управлению исследовательскими данными Эйндховенского технологического университета (Эйндховен, Королевство Нидерландов), научный сотрудник (постдок) департамента математики и наук о земле Университета Триеста (Триест, Итальянская Республика)

Джайшанкар Каруппаннан – доктор наук, директор и профессор Международного института исследований в сфере криминологии и безопасности (Бенгалуру, Республика Индия)

Мохд Хазми бин Мохд Русли – доктор наук, доцент факультета шариата и права Международного исламского университета Малайзии (Куала-Лумпур, Федерация Малайзия)

Кастилло Парилла Хосе Антонио – доктор наук, магистр новых технологий и права (Севилья, Королевство Испания), научный сотрудник Гранадского университета (Гранада, Королевство Испания)

Члены редакционной коллегии

Арзуманова Лана Львовна – доктор юридических наук, доцент, профессор кафедры финансового права Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Бажина Мария Анатольевна – доктор юридических наук, доцент, доцент кафедры предпринимательского права Уральского государственного юридического университета имени В. Ф. Яковлева (Екатеринбург, Российская Федерация)

Бахтеев Дмитрий Валерьевич – доктор юридических наук, доцент, доцент кафедры криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева, руководитель группы проектов CrimLib.info (Екатеринбург, Российская Федерация)

Беликова Ксения Михайловна – доктор юридических наук, профессор, профессор кафедры предпринимательского и корпоративного права Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Берсей Диана Давлетовна – кандидат юридических наук, доцент, доцент кафедры уголовного права и процесса Северо-Кавказского федерального университета (Ставрополь, Российская Федерация)

Будник Руслан Александрович – доктор юридических наук, профессор, заместитель директора международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам» Национального исследовательского университета «Высшая школа экономики» (Москва, Российская Федерация)

Дремлюга Роман Игоревич – кандидат юридических наук, доцент, заместитель директора по развитию Института математики и компьютерных технологий, профессор Академии цифровой трансформации Дальневосточного федерального университета (Владивосток, Российская Федерация)

Егорова Мария Александровна – доктор юридических наук, профессор, начальник Управления международного сотрудничества, профессор кафедры конкурентного права Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Ефремов Алексей Александрович – доктор юридических наук, доцент, профессор кафедры международного и евразийского права Воронежского государственного университета (Воронеж, Российская Федерация)

Ефремова Марина Александровна – доктор юридических наук, доцент, профессор кафедры уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия (Казань, Российская Федерация)

Камалова Гульфия Гафиятовна – доктор юридических наук, доцент, заведующий кафедрой информационной безопасности в управлении Удмуртского государственного университета (Ижевск, Российская Федерация)

Ковалева Наталия Николаевна – доктор юридических наук, профессор, руководитель департамента права цифровых технологий и биоправа факультета права Национального исследовательского университета «Высшая школа экономики» (Москва, Российская Федерация)

Лопатина Татьяна Михайловна – доктор юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин Смоленского государственного университета (Смоленск, Российская Федерация)

Минбалеев Алексей Владимирович – доктор юридических наук, доцент, заведующий кафедрой информационного права и цифровых технологий Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Миронова Светлана Михайловна – доктор юридических наук, доцент, профессор кафедры финансового и предпринимательского права Волгоградского института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Волгоград, Российская Федерация)

Наумов Виктор Борисович – доктор юридических наук, главный научный сотрудник сектора информационного права и международной безопасности Института государства и права Российской академии наук (Санкт-Петербург, Российская Федерация)

Пашенцев Дмитрий Алексеевич – доктор юридических наук, профессор, заслуженный работник высшей школы Российской Федерации, главный научный сотрудник отдела теории права и междисциплинарных исследований законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации (Москва, Российская Федерация)

Петренко Сергей Анатольевич – доктор технических наук, профессор, профессор кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» имени В. И. Ульянова (Ленина), профессор Университета Иннополис (Иннополис, Российская Федерация)

Полякова Татьяна Анатольевна – доктор юридических наук, профессор, заслуженный юрист Российской Федерации, и. о. заведующего сектором информационного права и международной информационной безопасности Института государства и права Российской академии наук (Москва, Российская Федерация)

Пономарева Карина Александровна – доктор юридических наук, ведущий научный сотрудник Центра налоговой политики Научно-исследовательского финансового института Министерства финансов Российской Федерации, профессор департамента публичного права Национального исследовательского университета «Высшая школа экономики» (Москва, Российская Федерация)

Рожкова Марина Александровна – доктор юридических наук, главный научный сотрудник Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, советник по науке декана юридического факультета Государственного академического университета гуманитарных наук, президент IP CLUB (Москва, Российская Федерация)

Рускевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Сидоренко Элина Леонидовна – доктор юридических наук, доцент, директор Центра цифровой экономики и финансовых инноваций, профессор кафедры уголовного права, уголовного процесса и криминалистики Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации, генеральный директор платформы забизнес.рф (Москва, Российская Федерация)

Степанян Армен Жоресович – кандидат юридических наук, доцент, доцент кафедры интеграционного и европейского права Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Стрельцов Анатолий Александрович – доктор юридических наук, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, член-корреспондент Академии криптографии Российской Федерации, ведущий научный сотрудник Центра проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова (Москва, Российская Федерация)

Талапина Эльвира Владимировна – доктор юридических наук, доктор права (Франция), главный научный сотрудник Института государства и права Российской академии наук, ведущий научный сотрудник Центра технологий государственного управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Москва, Российская Федерация)

Терентьева Людмила Вячеславовна – доктор юридических наук, доцент, профессор кафедры международного частного права Московского государственного юридического университета имени О. Е. Кутафина (Москва, Российская Федерация)

Харитонов Юлиа Сергеевна – доктор юридических наук, профессор, руководитель Центра правовых исследований искусственного интеллекта и цифровой экономики, профессор кафедры предпринимательского права Московского государственного университета имени М. В. Ломоносова (Москва, Российская Федерация)

Хисамова Зарина Илдузовна – кандидат юридических наук, начальник отделения планирования и координации научной деятельности научно-исследовательского отдела Краснодарского университета Министерства внутренних дел Российской Федерации (Краснодар, Российская Федерация)

Чеботарева Анна Александровна – доктор юридических наук, доцент, заведующий кафедрой правового обеспечения государственного управления и экономики Российского университета транспорта (Москва, Российская Федерация)

Шугуров Марк Владимирович – доктор философских наук, доцент, профессор кафедры международного права Саратовской государственной юридической академии, главный научный сотрудник Алтайского государственного университета (Саратов, Российская Федерация)

Иностранные члены редакционной коллегии

Абламейко Мария Сергеевна – кандидат юридических наук, доцент, доцент кафедры конституционного права Белорусского государственного университета (Минск, Республика Беларусь)

Аванг Низам Мухаммад – доктор наук, профессор факультета права и шариата Международного исламского университета (Негери-Сембилан, Федерация Малайзия)

Айсан Ахмет Фарук – доктор наук, профессор и координатор программы Исламских финансов и экономики Университета имени Хамада бин Халифа (Доха, Государство Катар)

Ападхьяй Нитиш Кумар – доктор юридических наук, доцент факультета права Университета Галготиас (Большая Нойда, Республика Индия)

Банкио Пабло – доктор наук, профессор Университета Буэнос-Айреса, постдок в области фундаментальных принципов и прав человека, член центра изучения частного права Национальной академии наук Буэнос-Айреса (Буэнос-Айрес, Аргентинская Республика)

Басарудин Нур Ашикин – доктор наук, старший преподаватель Университета технологий МАРА (Синток, Федерация Малайзия)

Бахрамова Мохинур Бахрамовна – доктор наук, старший преподаватель кафедры права интеллектуальной собственности Ташкентского государственного юридического университета (Ташкент, Республика Узбекистан)

Варбанова Гергана – доктор наук, доцент Университета экономики (Варна, Республика Болгария), доцент Университета мировой экономики (София, Республика Болгария)

Вудро Барфилд – доктор наук, приглашенный профессор Туринского университета (Турин, Итальянская Республика)

Гозстоный Гегели – доктор наук, кафедра истории венгерского государства и права Университета Эотвос Лоранд (Будапешт, Венгрия)

Гостожиц Стеван – доктор наук, доцент, глава цифровой криминалистической лаборатории Университета Нови Сад (Нови Сад, Республика Сербия)

Гош Джаянта – доктор наук, научный сотрудник Западно-Бенгальского национального университета юридических наук (Калькутта, Республика Индия)

Гудков Алексей – доктор наук, старший преподаватель Вестминстерского международного университета в Ташкенте (Ташкент, Республика Узбекистан)

Дауд Махауддин – доктор наук, доцент кафедры гражданского права Международного исламского университета Малайзии (Куала-Лумпур, Федерация Малайзия)

Дахдал Эндрю – доктор наук, доцент факультета права Катарского университета (Доха, Государство Катар)

- Дэнни Тэйм Даниэль Мендес** – доктор наук, научный сотрудник Азиатско-Тихоокеанского центра экологического права Национального университета Сингапура (Сингапур, Республика Сингапур)
- Иванц Тяша** – доктор наук, доцент кафедры гражданского, международного частного и сравнительного права Мариборского университета (Марибор, Республика Словения)
- Иоаннис Револидис** – доктор наук, преподаватель кафедры медиаправа и права технологий Мальтийского университета (Мсида, Республика Мальта)
- Йованич Татьяна** – доктор наук, доцент факультета права Белградского университета (Белград, Республика Сербия)
- Карим Ридоан** – доктор наук, профессор кафедры предпринимательского и налогового права Университета Монаша (Санвэй, Федерация Малайзия)
- Кастро Дуглас** – доктор наук, профессор международного права школы права Ланьчжоуского университета (Ланьчжоу, Китайская Народная Республика)
- Кера Решеф Дениза** – доктор наук, профессор Центра исследований технологий распределенного реестра Мальтийского университета (Мсида, Республика Мальта)
- Кипурас Павлос** – доктор наук, профессор Школы судебной графологии (Неаполь, Итальянская Республика)
- Мараньяо Альбукерке де Соуза Джулиано** – доктор наук, доцент факультета права Университета Сан-Паулу (Сан-Паулу, Федеративная Республика Бразилия)
- Мелипатаки Габор** – доктор наук, профессор кафедры аграрного и трудового права Университета Мишкольца (Мишкольц, Венгрия)
- Мехрдад Райеджиан Асли** – доктор наук, профессор Института исследований и развития в области гуманитарных наук, доцент кафедры ЮНЕСКО по правам человека, мира и демократии, заместитель декана по науке Университета имени Алламеха Табатабаи (Тегеран, Иран)
- Морина Менсур** – доктор наук, доцент, заместитель декана факультета права Университета бизнеса и технологий (Приштина, Республика Сербия)
- Мохсин Камшад** – доктор наук, доцент юридического факультета Международного университета Махариши (Махариши, Республика Индия)
- Муратаев Серикбек Алпамысович** – кандидат юридических наук, заведующий кафедрой теории государства и права Ташкентского государственного юридического университета (Ташкент, Республика Узбекистан)
- Нуреддин Мухамад** – доктор наук, старший преподаватель кафедры публичного права Университета Байеро (Кано, Федеративная Республика Нигерия)
- Праюди Юди** – доктор наук, профессор кафедры компьютерных наук и электроники Университета Гаджа Мада (Булаксур, Республика Индонезия)
- Рахметов Бауржан Жанатович** – доктор наук, ассистент-профессор Международной школы экономики Университета КАЗГЮУ имени М. С. Нарикбаева (Нур-Султан, Республика Казахстан)
- Тран Ван Нам** – доктор наук, директор факультета права Национального экономического университета (Ханой, Социалистическая Республика Вьетнам)
- Феррейра Даниэл Брантес** – доктор наук, старший научный сотрудник Южно-Уральского государственного университета (Челябинск, Российская Федерация), профессор Университета АМБРА (Орландо, Соединенные Штаты Америки), исполнительный директор Центра альтернативного разрешения споров (Рио-де-Жанейро, Федеративная Республика Бразилия)
- Чен Чао Хан Кристофер** – доктор наук, доцент факультета права Тайваньского национального университета (Тайпэй, Китайская Народная Республика)
- Шахновская Ирина Викторовна** – кандидат юридических наук, заведующий кафедрой конституционного права и государственного управления Полоцкого государственного университета (Новополоцк, Республика Беларусь)
- Эллул Джошуа** – доктор наук, директор Центра исследований технологии распределенного реестра Мальтийского университета (Мсида, Республика Мальта)
- Юхневич Эдвард** – доктор наук, профессор кафедры финансового права Гданьского университета (Гданьск, Республика Польша)



Содержание

Будник Р. А. Риски и перспективы токенизации творчества	587
Лендваи Г. Ф. «Чисто крысиная страна» – размышления о решении по делу 2022-001-FB-UA Наблюдательного совета Фейсбука (Дело мультфильма о городе Книн)	612
Бажина М. А. Интеллектуальные транспортные системы – основа de lege ferenda транспортной системы Российской Федерации	629
Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности	650
Роблес-Каррильо М. Суверенитет и цифровой суверенитет	673
Ермакова Е. П. Особенности онлайн-урегулирования потребительских споров платформами электронной торговли в Китайской Народной Республике	691
Йи Рэн Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии	712
Ярутин Я. К., Гуляева Е. Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция	725
Перетолчин А. П. Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации	752
Минич С. А. Совершенствование системы обязательных требований, предъявляемых к бизнесу в условиях цифрового преобразования экономики	775
Тихалева Е. Ю. «Умные города»: правовое регулирование и потенциал развития	803
Утеген Д., Рахметов Б. Ж. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования	825



Научная статья

УДК 34:347.211:75:78:808.1:004

EDN: <https://elibrary.ru/xhasaw>

DOI: <https://doi.org/10.21202/jdtl.2023.25>

Риски и перспективы токенизации творчества

Руслан Александрович Будник

Национальный исследовательский университет «Высшая школа экономики»

г. Москва, Российская Федерация;

Университет «МГУ-ППИ в Шэньчжэне»

г. Шэньчжэнь, Китайская Народная Республика

Ключевые слова

NFT,
блокчейн,
искусство,
музыка,
право,
произведение,
творчество,
токен,
токенизация,
цифровые технологии

Аннотация

Цель: токенизация творчества в одном ряду с криптоэкономикой и сетевой инфраструктурой Web3 представляет собой заметный тренд развития современного общества в третьем десятилетии двадцать первого века. Цель настоящей статьи заключается в исследовании рисков и перспектив, возникающих в процессе распоряжения результатами творческого труда в виде невзаимозаменяемых токенов.

Методы: методика настоящей работы построена на анализе различных точек зрения ученых на эту проблему, включая диаметрально противоположные концепции. Полярные позиции наблюдателей характеризуют их отношение к токенизации творческих продуктов как к спекулятивной схеме, с одной стороны, и перспективному инструменту развития творческих индустрий – с другой.

Результаты: выявлены возможные негативные последствия токенизации результатов интеллектуальной деятельности, а также авторские рекомендации по управлению этими рисками. Еще одним результатом настоящей публикации выступает анализ экономико-правовых перспектив, вытекающих из токенизации объектов авторских и смежных прав на примере музыкальных произведений.

Научная новизна: состоит в выдвижении и обосновании гипотезы о том, что отношения, сформировавшиеся в музыкальной индустрии в современных социокультурных и технологических реалиях, будут воспроизводиться в других творческих индустриях. Кроме того, научная новизна также заключается в анализе перспектив токенизации таких результатов интеллектуальной деятельности, как игровые артефакты, произведения художественного и цифрового изотворчества, патентов и достижений науки. Применение невзаимозаменяемых токенов в экосистеме сетевых компьютерных игр позволит геймерам покупать

© Будник Р. А., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

и продавать права на игровые произведения независимо от издателя. Токенизация объектов промышленной собственности и средств индивидуализации обеспечит защиту интеллектуальных прав их авторов в период ожидания выдачи государственного охранного документа. В современном обществе найдется немало желающих стать собственником токена на научное произведение, поскольку популярность науки и инноваций непрерывно растет в развитых странах. Владение токеном на научное произведение будет считаться моральной инвестицией, повышать престиж и статус его правообладателя. Токены на произведения науки имеют высокий потенциал в качестве средства измерения ценности в постэкономическом обществе.

Практическая значимость: практическая значимость исследования состоит в описании инновационных способов использования творческих продуктов и бизнес-моделей, основанных на токенизации результатов интеллектуальной деятельности, готовых к воплощению на практике.

Для цитирования

Будник, Р. А. (2023). Риски и перспективы токенизации творчества. *Journal of Digital Technologies and Law*, 1(3), 587–611. <https://doi.org/10.21202/jdtl.2023.25>

Содержание

Введение

1. Методика исследования токенизации творчества
2. NFT как социотехническое мошенничество
3. Результат: NFT как будущее творческих индустрий
4. Токенизация творчества на примере музыкальной индустрии
5. Критика токенизации музыкальной индустрии
6. Токенизация гейминга и кибербезопасность
7. Токенизация классического и цифрового изотворчества
8. Токенизации патентов
9. Токенизация произведений науки

Выводы

Список литературы

Введение

В третьем десятилетии двадцатого века одним из наиболее заметных трендов развития является формирование криптоэкономики и сетевой инфраструктуры Web3 (Momtaz, 2022; Goel et al., 2022; Jelil, 2022).

Web3 представляет собой следующую ступень развития Интернета, которая призвана реализовать те функции, которые ранее не возлагались на информационно-коммуникационную инфраструктуру мира (Murray et al., 2023). В частности, речь идет об обеспечении надежной фиксации права собственности, хранении информации о коммерческих транзакциях, правовом статусе вещей и нематериальных объектов в децентрализованном распределенном реестре с надежностью, которая многократно превышает централизованные и проприетарные системы. Web3 снижает

возможности внешнего контроля и противоправного использования частных данных пользователей, поскольку они хранятся в децентрализованной сети, а не на централизованных серверах (Petcu et al., 2023). На практике технологии Web3 представлены в виде криптовалют, невзаимозаменяемых токенов (non-fungible token – NFT), децентрализованных приложений и сервисов, смарт-контрактов, а также прототипов метавселенных.

Криптоэкономика, как и Web3, – понятие многомерное. С одной стороны, криптоэкономика – это область информатики, которая решает проблемы координации участников в цифровых экосистемах с помощью криптографии и экономических стимулов. С другой стороны, криптоэкономика представляет собой не часть традиционной экономики, но совокупность постэкономических институтов, образующих экосистему, вобравшую в себя теорию игр, математические методы моделирования функций, механизмы проектирования и реализации полезных сервисов, виртуальные активы, игровые ценности и утилитарные цифровые права (Yue et al., 2021). Кроме того, криптоэкономика меняет назначение и смысл фундаментальных экономических институтов, таких как деньги, активы, собственный и заемный капитал, корпоративная организация, стимулы производства, распределение рисков и отношение к традиционным финансовым инструментам (Chey, 2022). Здесь уместен пример стирания границы между понятиями долга и собственного капитала. Такие финансовые технологии, как конвертируемые облигации, привилегированные акции, свопы на совокупный доход, представляют собой нечто среднее между заемными и собственными средствами, они открывают новые возможности по привлечению и использованию инвестиций. Выпуск токенов на существующий или будущий виртуальный актив либо идею реализации стартапа обеспечивает финансирование, которое не является ни заемным, ни собственным капиталом, но имеет некоторые признаки каждого из них.

Важным элементом криптоэкономики и инфраструктуры Web3 выступают невзаимозаменяемые токены (Wilson et al., 2022). Модный термин «токенизация» относится к процессу преобразования актива в цифровой токен. Этот цифровой токен представляет собой небольшой фрагмент программного кода, который записан в распределенный реестр (блокчейн) и служит подтверждением права собственности на актив, плюс он содержит в себе технологические атрибуты о принадлежности к системе, поддерживающей проведение транзакций с ним. Токен может передаваться между пользователями без посредников, т. е. он является объектом коммерческого оборота, юридическим наполнением которого выступают права собственности на токенизированный актив, оформленные средствами смарт-контракта.

Одним из вариантов использования токенизации является недвижимость, где общая стоимость имущества дробится и перераспределяется в токенах. Эти токены позволяют инвесторам выходить на рынок и приобретать определенные участки недвижимости быстро и по невысокой цене (Far et al., 2022). Иными словами, токенизация снижает входные барьеры, устраняет посреднические сборы и издержки, повышает ликвидность актива, что дает инвесторам большую гибкость и безопасность инвестиций. Помимо недвижимости, процесс токенизации может охватывать практически любые активы, такие как ценные бумаги, акции, драгоценные металлы, интеллектуальная собственность, лицензионные права, продажа билетов и изобразительное искусство (Kraizberg, 2023).

В данном исследовании фокус нашего внимания сконцентрирован на токенизированных результатах творческой деятельности, поскольку они наиболее ярко высвечивают положительные и отрицательные стороны, а также противоречия данного явления. Для извлечения дохода правообладатели объектов авторских и смежных прав в токенизированном виде действуют совершенно противоположным способом по отношению к традиционным механизмам копирайта. В частности, NFT-рынок устроен так, что цена токена на произведение складывается на основе консенсуальной ценности произведения, т. е. на основе восприятия достоинства творческого продукта его целевой аудиторией. Таким образом, пользователи получают возможность беспрепятственного доступа и как минимум некоммерческого использования произведения без оплаты полученных привилегий деньгами.

К настоящему моменту в арсенале приобретателей токенов накоплен широкий спектр инновационных способов их монетизации, не связанных с ограничением доступа к произведению (Okediji, 2017), однако они обычно являются косвенными, а не прямыми, как товар или код доступа в обмен на деньги; реализуются на смежных рынках – внимания, впечатлений, рекламы, мерча¹; требуют специальных навыков – использования приемов поисковой оптимизации и цифрового маркетинга; создания уникальных ресурсов – организации и развития тематических интернет-сообществ, или особых условий, например, формирования внутригруппового спроса, вне которых они не работают (Colicev, 2023).

1. Методика исследования токенизации творчества

Методика настоящей работы строится на рассмотрении противоположных позиций в отношении токенизации творчества. Точка зрения первой группы наблюдателей строится на их убежденности в том, что рынок NFT представляет собой нечто похожее на финансовую пирамиду, схему обмана граждан, продажи им несуществующей ценности через злоупотребление их доверием.

Второй подход, напротив, постулирует положительный эффект токенизации творческих индустрий. Адепты данной системы взглядов анализируют и конструируют перспективные бизнес-модели и схемы извлечения дохода из токенизированных произведений для вознаграждения авторов и заработка собственников токенов. Приверженцы такого видения проблемы приводят аргументы в пользу того, что токенизация устраняет посредников между творцами, пользователями и приобретателями прав, снижает транзакционные издержки и комиссии на данном рынке, а также укрепляет отношения между авторами и их аудиторией.

Подробный прогноз последствий токенизации творчества сделан на основе музыкальной индустрии. Замечено, что в силу специфики данного вида искусств, и особенно его популярных жанров, оно наиболее отчетливо высвечивает разворачивающиеся эволюционные процессы, которые впоследствии реализуются и в других творческих сферах (Henry, 2007). Кроме того, рассмотрены перспективы токенизации произведений науки, патентов на объекты промышленной собственности, произведений аналогового и цифрового изобразительного творчества, артефактов индустрии компьютерных игр и онлайн-гейминга.

¹ Мерч – сленговое понятие (от английского merchandise – «товары, атрибутика, торговать»), обозначающее официальную продукцию с символикой музыкальных коллективов, отдельных исполнителей, спортивных команд, кинофильмов и пр.

2. NFT как социотехническое мошенничество

Одна из точек зрения гласит, что рынок невзаимозаменяемых токенов на объекты цифрового искусства представляет собой финансовую схему обмана с использованием информационно-технических средств, настроенную на причинение имущественного ущерба согласно ст. 165 Уголовного кодекса Российской Федерации² (далее – УК РФ) или мошенничество по определению ст. 159 УК РФ³, которая вскоре может прекратить свое существование (Walker, 2022; Scharfman, 2023).

В соответствии с этой точкой зрения покупатель поступает безрассудно, когда покупает NFT на спекулятивном неструктурированном рынке, и в конечном итоге он с высокой вероятностью потеряет свои деньги. Для обоснования этой позиции приводятся более и менее убедительные аргументы, которые имеет смысл рассмотреть подробнее.

Первое соображение, которое высказывают критики NFT, – это отсутствие материальной составляющей товара, т. е. приобретатель токена не получает вещного носителя с объектом авторских или смежных прав. Данный аргумент представляется поверхностным и неубедительным в том смысле, что результаты интеллектуальной деятельности все как один являются нематериальными или невещественными, что не мешает развитию рынка прав интеллектуальной собственности вот уже более трехсот лет. В течение всего этого периода исправно работает доктрина, предполагающая, что право владения вещью, в которой выражен результат интеллектуальной деятельности, отделено от авторских прав на произведение.

Второй аргумент заключается в том, что возможность копирования произведения обесценивают как сами копии, так и оригинал произведения. Развивая это соображение, необходимо добавить, что с разрешения правообладателя произведения потенциально существует возможность создания бесконечного множества производных произведений. Легитимно созданные производные произведения получают самостоятельную охрану, таким образом, они действительно снижают редкость оригинального произведения, что, как считают некоторые аналитики, обесценивает и сам оригинал (Hilko, 2021). Данный аргумент видится более состоятельным как с точки зрения права интеллектуальной собственности, так и экономики материального продукта, характерной для индустриального периода развития цивилизации, в рамках которой стоимость ресурса выступает функцией его редкости.

Третий аргумент носит мировоззренческий характер, и он, по нашему мнению, не должен квалифицироваться в качестве обмана или мошенничества. Речь идет о ситуациях, когда гражданин присоединяется либо получает доступ к определенной социальной группе, в рамках которой работает специфическая система ценностей. Внутри такого сообщества высокую художественную ценность и коммерческую стоимость могут иметь такие произведения, достоинства которых для внешних наблюдателей представляются неочевидными, а цена прав на них явно завышенной. Тем не менее люди проникаются взглядами группы единомышленников, совершают импульсные покупки и впоследствии сожалеют о своих действиях, если цена токена не

² Уголовный кодекс Российской Федерации № 63-ФЗ от 13 июня 1996 г. (1996). *Собрание законодательства Российской Федерации*, № 25, ст. 2954.

³ Там же.

выросла, как прогнозировалось «просвещенными» членами сообщества, а снизилась. Однако если мы обратимся к законному определению понятия мошенничества, то увидим, что в действиях участников группы, которые выдали обнадеживающую оценку или рекомендовали неопиту совершить сделку, такого состава преступления, как мошенничество, нет. Данный шаг можно сравнить с неудачной игрой на бирже с использованием ошибочных рекомендаций, которая предполагает риск убытков, о чем покупатель токена должен быть осведомлен и проявлять разумную осмотрительность.

Далее мы приведем примеры злонамеренных деяний с использованием невзаимозаменяемых токенов, которые могут квалифицироваться в качестве хищения чужого имущества, незаконного приобретения прав на него, нарушения авторских прав, а также причинения имущественного ущерба путем обмана или злоупотребления доверием.

Первый вид техники обмана характеризуется как мошенничество с «пустышкой». Оно реализуется так, что разработчики рекламируют и продают токены на объект цифрового искусства или целую их коллекцию, но после получения средств от инвесторов либо приобретателей токенов отказываются от своих обязательств и исчезают, так ничего и не создав и не выпустив на рынок. Организаторы этой схемы часто используют социальные сети для активной рекламы своего NFT-проекта внутри целевых групп, с тем чтобы завоевать доверие икратно максимизировать стоимость токена⁴. Достигнув достаточно высокой цены токена, которая может измеряться сотнями тысяч и даже миллионами долларов, ее основатели скрываются с полученными средствами. Классическим случаем мошенничества с NFT-«пустышкой» является проект Frosties NFT, в рамках которого продавались «эксклюзивные» токены на игру в метавселенной. Основатели проекта закрыли свой веб-сайт и учетные записи в социальных сетях сразу после того, как инвесторы вложили в него более 1,3 млн американских долларов⁵.

Вторая схема обмана с использованием NFT аналогична мошенничеству с банковскими картами, известному как «фишинг». Хакеры используют фишинг с целью доступа к учетной NFT-записи. Для этого они рассылают поддельные ссылки по электронной почте или через популярные каналы социальных сетей и форумов, таких как Twitter⁶ и Discord. После клика на ссылку и ввода реквизитов для входа хакеры используют злонамеренное программное обеспечение (далее – ПО), такое как кейлоггеры и другое шпионское ПО, для получения доступа к учетной записи пользователя с целью кражи денег или компрометации его аккаунта. Сегодня количество фишинговых атак с использованием NFT растет. Так, в феврале 2022 г. злоумышленники похитили токены на сумму почти 1,7 млн долларов в ходе фишинговой атаки на популярную NFT-платформу OpenSea. В рамках кампании по обновлению информации о контрактах мошенники скопировали базу контактных данных и разослали владельцам токенов ссылки на мошеннические веб-сайты⁷.

⁴ Например, в десять раз – до «десяти икс» – это так называемые желанные «иксы» мультипликатора цены токена.

⁵ Kaaru, Steve. (2022, March 22). Frosties NFT: 2 charged in US over \$1.3M rug pull. *CoinGeek*. <https://coingeek.com/frosties-nft-2-charged-in-us-over-1-3m-rug-pull>

⁶ Социальная сеть, заблокированная на территории Российской Федерации.

⁷ Russell, B. (2022, February 20). \$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users. *The Verge*. <https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft>

Третий пример связан с продажей токена на вторичном рынке. Мошенник делает наиболее высокую ставку на лот, что побуждает владельца продать токен этому «лучшему из покупателей». Однако, пользуясь неопытностью продавца на рынке криптоактивов, злоумышленник меняет валюту сделки без уведомления контрагента. Например, мошенник предлагает 10 эфиров за токен на объект цифирного арта, что на сегодня эквивалентно почти 15 000 американских долларов, но в процессе сделки ему удастся подменить криптовалюту на 10 тонов, что на текущий момент приблизительно равно 10 долларам. Для защиты от такого трюка необходимо внимательно контролировать процесс сделки, включая тип валюты, и не соглашаться на уменьшающие цену альтернативы.

Четвертая схема – памп-энд-дамп – «накачать и сбросить». Ее суть заключается в том, что группа мошенников распространяет вводную в заблуждение информацию для повышения цены NFT, имитируя рыночный характер данного процесса. Как только находится инвестор, который вкладывается в проект по искусственно разогнанной цене, мошенники исчезают с деньгами, оставляя покупателей с бесполезными активами. Для создания ажиотажа вокруг проекта используются как открытые, так и теневые манипулятивные рекламные механизмы в социальных сетях, включая поддержку со стороны знаменитых персон – селебрити. Дополнительно злоумышленники имитируют спрос на токен с помощью личных средств, которые на практике движутся между их собственными счетами и кошельками, что привлекает внимание активных инвесторов и не позволяет им проигнорировать данный актив. Примером такого мошенничества является обман инвесторов проекта Evil Ape. Анонимный создатель несостоявшейся коллекции исчез с 798 эфирами (ETH) на сумму более 2,7 млн долларов, и больше о нем ничего не было слышно⁸.

Пятая схема связана с присвоением авторства (плагиатом) на произведение, в отношении которого выпускается токен лицом, которому не принадлежат права на него. В 2022 г. менеджмент платформы OpenSea сообщил, что более 80 % NFT на данной платформе выпущены с нарушением прав законных правообладателей⁹. Таким образом, на сегодняшний день высока вероятность приобрести токен на противозаконно присвоенный объект авторских прав. Если данный факт устанавливается, то стоимость такого токена резко падает. По этой причине необходимо проверять права на произведение до заключения сделки.

Чрезвычайную важность имеет тот факт, что правила платформ (в качестве примера приведем все тот же наиболее успешный на сегодняшний день NFT-ресурс OpenSea) возлагают обязанность по проверке прав на токенизируемые работы на самого покупателя токена. В тексте лицензионного соглашения платформа совершенно определенно и подчеркнуто недвусмысленно слагает с себя ответственность за противоправные действия пользователей. В соглашении зафиксировано, что платформа не проверяет прав продавца на произведение, токен на которое он создает и продает. Нормы лицензионного соглашения прямо постулируют, что

⁸ Chalk, A. (2021, October 6). 'Evolved Apes' NFT creator Evil Ape disappears with \$2.7M7. *PC Gamer*. <https://www.pcgamer.com/evolved-apes-nft-creator-evil-ape-disappears-with-dollar27m>

⁹ Volpicelli, Gian M. (2022, February 10). Why OpenSea's NFT Marketplace Can't Win. *WIRED*. <https://www.wired.co.uk/article/opensea-nfts-twitter>

площадка не осуществляет так называемую очистку прав, поэтому риски, вытекающие из противозаконных действий продавцов, целиком и полностью ложатся на покупателя. Площадка выступает лишь маркетплейсом, т. е. предоставляет место и инструменты для совершения сделки, но она не является классическим брокером, который гарантирует сторонам чистоту сделки и взаимное исполнение обязательств. В рамках разумной осмотрительности покупатель токена обязан проверить правомочия продавца, для этого он должен потребовать у него правоустанавливающие документы – лицензионное соглашение на использование токенизируемого произведения. Либо он должен убедиться в авторстве создателя произведения, если тот действует без посредников, изучив его историю и профиль в социальных сетях, что снижает риски вовлечения в противоправную сделку.

В шестую категорию мы можем поместить несколько иных, не столь популярных, но опасных видов обмана на NFT-рынке. Известна афера с «подарочной раздачей» токенов, в рамках которой жертве обещают подарить токен в обмен на усилия по продвижению коллекции. После выполнения работы организаторы схемы присылают исполнителю ссылку для получения приза в электронный кошелек, что требует введения реквизитов доступа к нему. Однако мошенникам нужны лишь данные учетной записи хранилища чужих цифровых активов с целью их присвоения.

Еще одна известная с начала эпохи информатизации махинация – подмена службы поддержки. Злоумышленник связывается с клиентом якобы для решения проблемы с учетной записью. Под предлогом оказания помощи клиенту направляется ссылка на поддельную NFT-площадку, алгоритм которой требует введения ключа личного кошелька, который считывается и используется для хищения средств.

В настоящем разделе проанализированы известные на сегодня приемы обмана посредством NFT. Эти знания приведены в качестве иллюстрации тезиса о мошенническом характере отношений на данном рынке. Позволим себе сформулировать несколько практических рекомендаций для повышения безопасности при работе в этой среде и защиты от жульнических схем.

Необходимо отметить, что предлагаемые рецепты представляют собой типичные меры информационно-технологической предосторожности и приемы самозащиты в сетевой среде. Не стоит кликать на подозрительные ссылки, поскольку так злоумышленник может получить данные учетной записи. Никому и никогда нельзя сообщать пароль и/или код доступа к аккаунту и кошельку. Имеет смысл применять двухфакторную аутентификацию учетной записи для повышения уровня ее защиты. Прежде чем осуществить сделку, необходимо проверить личность и историю продавца токена. Следует использовать виртуальную частную сеть (VPN) для шифрования и анонимизации NFT-трафика. В дополнение к рабочему кошельку для осуществления транзакций целесообразно завести так называемый холодный кошелек, который не применяется для проведения операций, но используется лишь для хранения цифровых активов в автономном и наиболее безопасном режиме.

Далее мы перейдем к исследованию диаметрально противоположного взгляда на блокчейн/NFT как на позитивную в социальном, культурном и технологическом аспекте инновацию, которая может придать новую энергию и открыть ранее неизвестные пути развития творческих индустрий в технологическом обществе.

3. Результат: NFT как будущее творческих индустрий

Согласно концепции о светлом будущем творческих индустрий в блокчейн-экосистеме, технология распоряжения правами на произведения посредством токенов представляет собой прорывную инновацию (*disruptive innovation*), которая способна изменить отношения и правила игры в данной области. Одним из ключевых преимуществ блокчейн-платформ считается высокая эффективность реализации юридических и экономических (в их неразрывном синтезе – институциональных)¹⁰ отношений (Hale, 1952), возникающих вокруг криптовалют и токенов. Приверженцы институционального направления научной мысли определяют результат образования новых юридико-экономических взаимосвязей под влиянием достижений прогресса в качестве институциональной среды более высокого порядка (Commons, 1959; Ayres, 1962). При этом потребность в юридико-экономических новациях и их технологическом подкреплении обусловлена общественным запросом на реализацию вновь складывающихся отношений, природу которых мы анализируем в настоящей статье.

На сегодняшний день в мире сформировалась когорта специалистов, мнение которых мы учитываем в данной работе, объединенных видением будущего прогресса творческих индустрий в связи с использованием блокчейн/NFT-инструментов. Аналитики трансформации творческой деятельности и использования ее результатов в конкретных областях интеллектуальной сферы под воздействием научно-технического прогресса подчеркивают, что сами не являются специалистами в блокчейне, смарт-контрактах и чеканке NFT, не имеют доступа к инсайдерской информации и личных интересов в NFT-бизнесе. Данные обстоятельства важны для оценки объективности высказываемых ими позиций, которые подчас выглядят опрокидывающими устоявшиеся взгляды на творчество как социокультурный институт и экономические модели коммерциализации интеллектуальных прав.

4. Токенизация творчества на примере музыкальной индустрии

Одним из наиболее ярких исследователей является Тед Джоя (Gioia, 2019), который в своих трудах системно анализирует и прогнозирует то, как блокчейн и NFT повлияют на музыкальную индустрию. Особую ценность результатам его работ придают следующие обстоятельства. В условиях сложившейся ремикс-культуры именно музыка в силу специфической ограниченности средств выражения форм, позитивно воспринимаемых большинством слушателей (Santiago, 2017), наглядно предъясняет и во многом определяет тенденции развития творческих механик и рынка продуктов интеллекта в эпоху технологий. Наблюдения, выводы и обобщения, сделанные в отношении музыкальных произведений, оказываются релевантными и для других доменов науки и искусства.

Для вхождения в мировоззренческий контекст, вне которого будет сложно воспринять ход мыслей исследователя, процитируем его в нашем авторском переводе: «Я потратил много часов своей юности на прогнозирование технологических трендов и консультирование платных клиентов в Силиконовой долине. Я разрабатывал

¹⁰ Институциональная теория рассматривает право и экономику как юридико-экономическую систему взаимозависимостей, а не автономные подсистемы.

схемы ценообразования, распространения и стимулирования потребления новых продуктов и услуг. Это не лучший способ провести молодость с калькулятором в руке, но правда есть правда. Однако полученный опыт позволил мне разобраться в музыке не только как критику и писателю, но и как аналитику, в том числе благодаря многолетней работе со звукозаписывающими лейблами и стартапами в области музыкальных технологий. Я делал предложения венчурным предпринимателям, привлекал капитал на Уолл-стрит, пил дорогие напитки с инвестиционными банкирами на частных самолетах и т. п., включая всякую бессмыслицу. Другими словами, я знаю достаточно, чтобы быть опасным»¹¹.

Джоя предлагает прогноз перспектив развития NFT-тренда в музыкальной индустрии, который по мере продвижения вперед по списку ожидаемых эффектов выглядит все более парадоксальным.

Во-первых, блокчейн гарантирует отслеживание связи каждого файла, который содержит музыкальное произведение или произведение иного вида творчества, выраженное в цифровой форме, с оригиналом (эталонным цифровым файлом) данного произведения. Таким образом, становится возможным проверить подлинность и правомерность использования каждой цифровой копии. Возникает вопрос, насколько это полезно и к каким юридико-экономическим последствиям может привести. Здесь необходимо помнить, что продукты творчества распространяются и используются не только в сети. Блокчейн не в состоянии остановить их распространение вне сети. Любая звуковая дорожка, визуальный и аудиовизуальный контент, воспроизведенный на одном носителе, может быть повторно записан и воспроизведен на другом носителе. Достигнутый уровень техники позволяет легко фиксировать, копировать и распространять любой контент с помощью различных устройств. Например, записать аудиотрек из теле- или радиопередачи, сделать фотографию картины в музее или копию видеоряда в кинотеатре камерой смартфона. Таким образом, громкие заявления о том, что новые технологии остановят пиратство, являются ошибочными. Пиратство всегда будет с нами, особенно если официальные копии произведений, которые прошли аутентификацию в блокчейне, будут стоить так же дорого, как и сегодня.

Во-вторых, для законопослушных граждан блокчейн мог бы значительно упростить идентификацию правообладателя каждой фонограммы (файла) и при необходимости получение лицензии на ее использование, например, в фильме, рекламе или обучающем видеоролике. Это решение реальной проблемы законным способом, но оно не изменит индустрию и не вызовет восторга у рядового пользователя, поскольку получать лицензию на использование музыки ему приходится не часто. Тем не менее это будет шаг вперед.

Третья новация заключается в аутентификации оригинальных файлов уникальных музыкальных произведений и возможности продажи прав на них по высокой цене. В новой институциональной среде музыкальный файл получит особый статус, «такой же, как оригинал картины Пикассо» и, таким образом, может иметь «изрядный ценник». Однако это в корне меняет отношения музыканта с публикой, и не в лучшую сторону¹². Вместо того чтобы работать в интересах своей аудитории, музыканты будут вынуждены тратить свою энергию на обхаживание элитной группы богатых коллекционеров,

¹¹ Gioia, T. (2022, January 2). Eleven Wild Guesses on How Blockchain and NFTs Will Actually Impact Musicians and Songs. *The Honest Broker*. <https://tedgioia.substack.com/p/eleven-wild-guesses-on-how-blockchain>

¹² Там же.

которые покупают «оригинальную» песню как символ своего статуса. Джоя задается вопросом: правильно ли строить новую музыкальную экосистему на прихотях таких людей, как Мартин Шкрели¹³. Подобного рода случаи уже происходят, но этот «шкре-литизированный» подход представляет собой лишь малую часть возможностей NFT, снижающий к тому же преобразующий потенциал более перспективных и масштабных бизнес-моделей в музыкальной индустрии.

Четвертая перспектива состоит в использовании блокчейна для упрочения отношений между музыкантами и их аудиторией. Токенизация альбомов и отдельных композиций является эффективным способом реализации этой потенциально судьбоносной новации. Поставим мысленный эксперимент по выпуску нового музыкального альбома, который предполагает, что денежные потоки за его использование идут к держателям токенов, а транзакции фиксируются в блокчейне. Представим себе сценарий, в котором правообладатель сохраняет за собой 50 % токенов, а остальные продаются пользователям-поклонникам по разумной цене, например, по 1 500 рублей, что эквивалентно 170 юаням или 25 американским долларам. В дополнение к токенам их покупатели получают копию фонограммы в виде компакт-диска, винилового альбома или файла для скачивания плюс другие подарки и льготы. Некоторые права в дальнейшем могут уступаться, но остальные сохраняются только за участниками первичной сделки. Владельцы смогут держать токены в качестве инвестиционного инструмента либо продавать их и, как следствие, будущие денежные потоки, другим поклонникам. Если фонограмма окажется коммерчески успешной, то токенизированные права на нее станут выгодным вложением. Можно представить себе такой лейтмотив: «Смотри, я получил прибыль, перепродав свой токен на Daft Punk, плюс получил альбом себе»¹⁴. При реализации подобной схемы музыкальные магазины станут похожи на зал фондовой биржи с видеоэкранами, отображающими цену покупки и продажи токенов на фонограммы¹⁵.

Пятым эффектом новой модели являются прозрачность и справедливость в выплате роялти. Многие авторы не доверяют системе учета и распределения вознаграждения звукозаписывающих лейблов. Джоя пишет об информации от известного джазового музыканта с миллионными тиражами альбомов в его дискографии, что за всю карьеру тот не получил ни одной выплаты ни от одного звукозаписывающего лейбла, кроме аванса при подписании контракта¹⁶. Будущие гонорары так и остались пустым обещанием вне зависимости от количества проданных копий фонограммы. Технология блокчейн/NFT может изменить эту ситуацию. С ее помощью доходы от продажи прав на использование фонограммы могут поступать на счет, к которому звукозаписывающая компания или менеджер группы не будут иметь доступа.

¹³ Мартин Шкрели – известный предприниматель из США, осужденный за мошенничество в фармацевтической отрасли. Он осуществил выкуп исключительных прав на необнародованный музыкальный альбом группы Wu-Tang Clan для личной коллекции. Впоследствии альбом был конфискован у Шкрели в счет погашения долга. В момент написания статьи альбом остается официально не опубликованным. См. Sisario, B. (2021, October 20). Meet the New Owners of the Wu-Tang Clan's One-of-a-Kind Album. *The New York Times*. <https://www.nytimes.com/2021/10/20/arts/music/wu-tang-clan-once-upon-a-time-in-shaolin.html>

¹⁴ Там же.

¹⁵ Там же.

¹⁶ Там же.

Полученные средства будут распределяться между авторами, исполнителями, иными правообладателями и держателями токенов автоматически алгоритмом блокчейна в соответствии с условиями смарт-контракта, например, Ethereum, который гарантирует корректное проведение транзакций. Этот метод не обеспечивает абсолютную справедливость, но обделять артистов станет сложнее.

Шестой прогноз состоит в том, что технология блокчейн/NFT может сделать результаты творческой деятельности предметом сетевого маркетинга¹⁷, включая негативные стороны данной бизнес-схемы (Michalski et al., 2012). В этом сценарии покупатель токена получает вознаграждение за привлечение новых покупателей токенов. Эта схема NFT «с турбонаддувом» будет стимулировать пользователя становиться дистрибьютором токенов.

Седьмым пунктом идут эксцентричные варианты предыдущей модели. Токены могут быть структурированы в зависимости от выполнения установленных условий, например, определенного объема продаж. Достигнутые результаты конвертируются в полномочия и делегируются вниз по организационной структуре. Например, у меня есть право продать сотню токенов топового артиста, и если вы покупаете один, то получаете право продать десять субтокенов и т. п. Возможен вариант выпуска «платформенных» токенов с правом использования произведения, ограниченным определенной платформой. Разум перебирает подобные варианты и вариации. Музыкальный бизнес может воспринять франчайзинговую модель в виде структурированной сети, которая максимизирует денежный поток за счет роялти, получаемых каждым участником. Джоя предлагает музыкантам задуматься о перспективах такого положения, когда поклонники выигрывают в финансовом отношении, если новое произведение или альбом становится хитом, и что это намного эффективнее, чем продавать футболки и мерч на концертах.

Восьмое. В рамках настоящего анализа невозможно умолчать о том, что токенизация творчества создает потенциал для всевозможных неэтичных практик и конфликтов интересов. Представьте себе в качестве владельца токенов на музыкальные произведения радиодиджея, куратора плейлиста на стриминговом сервисе или диджея на вечеринке в колледже и то, какие возможности для разгонки цены токенов открывают названные позиции. Эту ситуацию можно сравнить с инсайдерской торговлей на бирже или пэйолой¹⁸ на стероидах. Однако здесь нет преступления или масштабных общественно опасных последствий. Вознаграждение аудитории в случае успеха артиста представляется вполне справедливым. Можно представить себе поклонников, хранящих верность артисту на протяжении многих лет в том числе потому, что в этих отношениях присутствует инвестиционный аспект: «Я уже много лет держу токены этих групп, и когда-нибудь они окупятся»¹⁹.

¹⁷ Сетевой маркетинг (или многоуровневый маркетинг; англ. multilevel marketing, MLM) – концепция реализации товаров и услуг через сбытовых агентов, каждый из которых строит свою сеть и получает комиссию с продаж ее членов.

¹⁸ Пэйола (англ. payola, синтез слов pay – «платить» и Victrola – торговая марка фонографов) – тайные выплаты от компаний звукозаписи радиостанциям и телевизионным каналам с целью раскрутки принадлежащих им музыкальных композиций (ротация в эфире, имитации интереса к ним зрителей, повышения в рейтингах, чартах и т. п.).

¹⁹ Gioia, T. (2022, January 2). Eleven Wild Guesses on How Blockchain and NFTs Will Actually Impact Musicians and Songs. *The Honest Broker*. <https://tedgioia.substack.com/p/eleven-wild-guesses-on-how-blockchain>

Девятый аспект связан с известным в мире живописи фактом, что цена на работы художника резко увеличивается после его смерти. В области музыкального творчества, как выяснилось, существует аналогичная зависимость. Статистическое исследование 446 альбомов 77 умерших музыкантов показало, что доходы от использования фонограммы увеличиваются в среднем на 54 % после смерти автора или исполнителя²⁰. И это не мелочь, но значимый фактор, который создает стимул для поклонников-инвесторов покупать токены артистов, находящихся в преклонном возрасте. Этот источник средств может стать пенсионным фондом для музыкантов. По мере того, как они становятся старше, их токены растут в цене, а инвесторы увеличивают стоимость портфеля. Возрастной музыкант может выпускать даже больше токенов – точно так же, как компания выпускает больше акций для покрытия расходов на медицинское обслуживание и другие траты в конце жизни.

Умозаключение номер десять состоит в том, что курс на токенизацию как минимум части результатов творческой деятельности взят вполне уверенно и уже подтвержден практикой, поэтому мейджоры музыкальной индустрии должны были бы прямо сейчас создавать собственные платформы и торговые площадки для фонографических токенов. Они могли бы сгенерировать новые бизнес-модели и вытекающие из них финансовые потоки для увеличения своей прибыли, доходов музыкантов и иных правообладателей. Однако представляется, что мейджоры сделают совсем мало или почти ничего, чтобы воспользоваться этими возможностями. Вместо этого они будут наблюдать со стороны, как технологические стартапы внедряют каждую из них, а традиционные посредники становятся все менее полезными и более неуместными на данном рынке²¹. Учитывая чрезвычайную зависимость бизнеса крупных лейблов от юридической поддержки, можно с уверенностью спрогнозировать, что музыкальные компании старой школы подадут множество исков в их «неолуддитской» попытке остановить развитие технологий²². И эта попытка окажется столь же успешной, как и намерение предотвратить распространение музыки через Интернет двадцать лет назад.

Подводя краткий итог исследованию перспектив токенизации музыкального бизнеса, стоит напомнить, что его выводы касаются и других доменов искусства и науки, продукты и результаты которых поддаются оцифровке. Первый вывод на сегодняшний день таков. Нынешнее увлечение богатых покупателей приобретением токенов художественно значимых произведений в качестве трофеев, актов статусного потребления, артефактов символической ценности, а также оппортунистические покупки произведений «цифрового фан-арта» в спекулятивных целях мало что меняют в творческих индустриях. Эта ситуация наглядно демонстрирует совокупность упущенных и нереализованных возможностей. Если все, что творческие индустрии смогут извлечь из блокчейна, – это статусно ориентированный нишевый рынок для небольшого количества богатых коллекционеров, то большая часть этих инноваций окажется растраченной зря²³.

²⁰ Там же.

²¹ Там же.

²² Там же.

²³ Там же.

Вышеописанный потенциал применения блокчейн/NFT-технологий может оказать по-настоящему трансформирующее воздействие на творческие индустрии. Результатом его полнофункционального использования может стать новая институциональная модель рынка творческих продуктов, предполагающая вовлечение широких масс, которые, к своему удовольствию, обнаружат, что блокчейн/NFT-стек позволил им разделить успех с предпочитаемыми артистами, наладить социокультурные связи с ними²⁴, инвестировать и получать доход от использования произведений, а также обеспечил высокую эффективность транзакций в новых юридико-экономических реалиях.

5. Критика токенизации музыкальной индустрии

Критический подход к высказанным суждениям обязывает поставить под сомнение несколько моментов.

Во-первых, вряд ли можно с уверенностью разделить оптимизм автора в части, касающейся упрочения отношений между музыкантами и аудиторией вследствие токенизации произведений. Проблема в том, что наступление подобного эффекта прогнозировали в отношении каждой новации, связанной с Интернетом. Именно этого ожидали от самого Интернета как базовой технологии. В приведенном прогнозе скорее отражено желание автора, нежели названы основательные причины для его осуществления. Там, где появляется такая сложная технология, как блокчейн/NFT, всегда возникают упрощающие ее использование посредники, и зачастую это совершенно новые игроки на рынке. Так, в музыкальной индустрии на смену лейблам-мейджорам пришли Spotify, Apple и Google. Можно предположить, что образуется целая волна стартапов, нацеленных на облегчение работы с NFT для продавцов и покупателей за процент от сделки.

Тезис о том, что музыкальный бизнес может воспринять франчайзинговую модель в виде сетевой структуры, которая максимизирует денежный поток за счет роялти, получаемых каждым участником, также вызывает сомнения. Ситуация видится так, что количество людей, которые имеют желание глубоко погружаться и заниматься подобными вещами, исчезающе мало. Здесь уместно вспомнить попытку организовать бизнес-схему микроплатежей за использование единицы контента: за прослушивание песни – 15 центов и 8 центов – за доступ к газетной статье. Такая модель оказалась нерентабельной, не нашлось даже заинтересованного оператора для ее осуществления. В результате на рынке выиграла более простая и менее избирательная модель подписки на любой контент по приемлемой фиксированной цене, эквивалентной примерно 10 американским долларам в месяц²⁵.

Третье возражение заключается в том, что по-настоящему значимый размер аудитории имеет всего лишь несколько процентов артистов, поэтому большинство из них не смогут рассчитывать на существенные роялти при продаже токенов. Кроме того, идея о том, что поклонники поддерживают артиста ради собственной прибыли, представляется вступающей в противоречие с самой сутью творчества.

²⁴ Там же.

²⁵ Case, A. (2021). Who killed the micropayment? A history. *Medium*. <https://caseorganic.medium.com/who-killed-the-micropayment-a-history-ec9e6eb39d05>

6. Токенизация гейминга и кибербезопасность

Ян Хартман выделяет рынок творческих продуктов, создаваемых внутри электронных игр сегодня и геймифицированной метавселенной завтра. Количество игроков в мире в 2022 г. достигло 3,24 млрд человек, и перед многими из них стоит вопрос прав на оригинальные и производные произведения, которые они создают внутри игр, а также проблема легального распоряжения этими правами. Исследователь отмечает высокий потенциал технологии блокчейн/NFT для решения данного вопроса на игровом рынке. По его мнению, игровые артефакты, такие как личные предметы, оружие, скины и награды, можно и нужно упаковывать в NFT и продавать на открытом рынке. Типичная ситуация такова, что если игрок имеет желание приобрести аксессуары для своего персонажа, то у него есть только одна легитимная возможность – купить их у издателя игры. С приходом юридико-экономической блокчейн/NFT-платформы в игровую экосистему геймеры смогут покупать и продавать права на игровые произведения и артефакты независимо от издателя. Такая демонополизация представляет собой серьезный сдвиг в структуре отрасли и точку роста рынка токенов на игровые артефакты²⁶.

Хартман и другие исследователи задаются вопросом о полезности NFT за пределами рынка цифрового искусства. В этом контексте упоминаются продукты для цифровой идентификации и обеспечения кибербезопасности. По мнению аналитиков, технология блокчейн/NFT эффективна для разработки и поддержки решений, обеспечивающих конфиденциальность пользователей, процедуру проверки подлинности (аутентификацию) информации, идентификацию личности и псевдонима, цифровую подпись транзакций, шифровку сообщений и надежное хранение данных. Совокупность этих решений образует цельную платформу кибербезопасности. Ученые делают вывод о том, что технология блокчейн/NFT может стать основой кибербезопасности нового поколения.

7. Токенизация классического и цифрового изотворчества

Монти Престон выражает согласие с тем, что блокчейн/NFT-технологии помогут создать новые каналы коммуникации между художниками и покупателями их работ, расширить возможности доступа граждан к миру искусства и демократизировать его, а также сформировать новый взгляд на ценности арт-пространства. Раскрывая тезис о демократизации, аналитик говорит, что NFT обеспечивают художникам возможность создавать произведения и распространять их через онлайн-каналы, минуя традиционных посредников, которые веками диктовали правила доступа к искусству, а также навязывали свои представления о том, что является искусством и что нельзя считать таковым. Эффект от использования исследуемой технологии заключается в том, что она способна вовлечь в арт-пространство людей, которые не имели возможности быть в нем полноценно представленными. Сюда можно отнести творцов из географически удаленных регионов, женщин и юных, не достигших совершеннолетия художников. Юридико-экономическая основа блокчейн/NFT предоставляет им необходимый инструмент для продвижения и заработка на результатах творческой деятельности, уравнивая возможности этих социальных групп.

²⁶ Hartmann, J. (2022, April, 19). Is there a future for the NFT beyond digital art? *Forkast*. <https://forkast.news/is-there-future-for-nft-beyond-digital-art>

Аналитик также считает, что данная технология изменит отношения в части, касающейся поддержки художников и искусства в целом. Поскольку транзакции в блокчейне являются прямыми и не опосредуются третьей стороной, то коллекционеры и поклонники смогут напрямую поддерживать артистов. Вследствие того, что NFT допускает долевое и фракционное владение, правообладатели и коллекционеры смогут делиться доходами от использования работ художников. Такие особенности NFT-модели монетизации творчества, как получение гонораров без участия посредников и в счет будущих продаж, были названы в качестве наиболее востребованных в результате специализированного опроса действующих художников. В случае реализации блокчейн/NFT-новаций в области изобразительного искусства будущее художников может быть наполнено большей свободой и независимостью от корпоративного покровительства, мегаколлекционеров и претенциозных кураторов²⁷.

8. Токенизации патентов

Исследовательская группа ученых под руководством профессора Цюй Цяна из Шэньчжэньского института передовых технологий Китайской академии наук и профессора Сейеда Моджтабы Хоссейни Бамакана из Йездского университета (Иран) предложила многоуровневую архитектуру системы управления патентами на основе NFT (Bamakan et al., 2022).

В обоснование целесообразности проекта исследователи называют следующие аргументы. Патентование изобретения, полезной модели, промышленного образца или регистрация товарного знака представляет собой длительный, трудоемкий и дорогостоящий процесс. Процедура получения охранного документа занимает многие месяцы и даже годы. Исследователи считают, что с помощью уникальных особенностей невзаимозаменяемых токенов этот процесс можно ускорить, а также повысить уровень защиты прав на токенизированные объекты промышленной собственности и средства индивидуализации.

По заявлению ученых, проект не ставит своей целью подменить или вытеснить государственную регистрацию объектов промышленной собственности и средств индивидуализации, но он может обеспечить охрану интеллектуальных прав в период ожидания выдачи государственного охранного документа. Кроме того, токенизация патентов и товарных знаков направлена на упрощение процесса лицензирования патентных прав для изобретателей, коммерческих компаний и университетов с помощью юрико-экономических механизмов технологии блокчейн/NFT. Вследствие фиксации каждой транзакции в блокчейне отслеживать изменения прав собственности на патенты станет проще. За счет усовершенствования лицензирования прав на использование охраняемых решений токенизация патентов поспособствует повышению доходов правообладателей. Ученые также считают, что такой юрико-экономический инструмент NFT, как автоматически исполняемый смарт-контракт, который фиксирует условия и цену использования запатентованного решения, способен поддерживать эффективность рынка интеллектуальных прав. Этот результат будет

²⁷ Preston, M. (2020, March 16). Curators Inside The Industry. *Art Plugged*. <https://artplugged.co.uk/monty-preston-curators-inside-the-industry>

достигнут в том числе вследствие автоматизации сбора лицензионных отчислений за использование решений правообладателей. Патентные токены могут использоваться как индивидуально, так и объединяться в коммерческий портфель решений для определенной предметной области с последующим распределением роялти между авторами и правообладателями патентов.

Разработчики предлагают следующий алгоритм создания и работы с патентными токенами. Авторы изобретения регистрируют свое техническое решение на блокчейн-платформе с целью его запатентовать. Далее они загружают информацию, которая представляет собой содержание патента и принадлежащую им интеллектуальную собственность. Встроенный механизм обеспечивает проверку данных для предотвращения их дублирования и иных манипуляций. Здесь необходимо отметить, что конструкторы схемы не раскрывают важный момент, связанный с экспертизой заявки по форме и по существу, а также механизм ее дальнейшей конвертации в патент, либо в отказ от его выдачи. Основываясь на достигнутом уровне техники, можно предположить, что решение этих задач возлагается на встроенные в платформу средства искусственного интеллекта. Далее, в случае выдачи патента он становится видимым для всех пользователей блокчейн-реестра.

Потенциальные потребители, которым необходим доступ к патентному контенту, после регистрации в сети обращаются к правообладателям. По результатам коммуникации между сторонами создается смарт-контракт с условиями использования патента, который вступает в силу после оплаты одним из доступных способов: фиатными деньгами, криптовалютой либо уникальными токенами. Дополнительно генерируется и сторонами подписывается соглашение о неразглашении (NDA – non-disclosure agreement). Механизм смарт-контракта контролирует согласие сторон с условиями сделки и его дальнейшее исполнение.

На прикладном уровне покупатель, согласный с открытыми условиями использования патента, которые заявлены его правообладателем, может произвести оплату и немедленно разблокировать права на его эксплуатацию без дополнительного взаимодействия сторон. В то время как патентные системы мира носят национальный либо региональный характер (например, Евразийская патентная система) токенизация патентов поможет устранить географические барьеры между ними через механизм поискового запроса в распределенном реестре. Простота и дешевизна поиска, автоматизация лицензирования, высокая скорость проведения транзакций для получения и оплаты прав на использование патентов, рассеянных по странам мира, поможет заинтересованным лицам ускорить применение инновационных решений. Предлагаемая система также может использоваться для отчуждения патентов и трекинга информации о правообладателях. Архитектура системы включает в себя арбитражный модуль для разрешения споров, функцию обработки претензий, поддержки обмена конфиденциальной информацией, проверки и доказательства авторства, трансфера прав, создания и размещения защитных публикаций.

Реализуемость и перспективность проекта токенизации патентных прав и прав на товарные знаки подтверждается партнерством IBM и корпорации IPwe, которое нацелено на стимулирование патентных транзакций с использованием блокчейн-платформы IBM. В IBM Services заявляют, что разрабатываемые ими патентные NFT представляют собой «упрощенные смарт-контракты на интеллектуальные активы с доступной

цепочкой поставок»²⁸. При этом токенизация патентов представляется все же делом будущего в отличие от токенизации объектов авторских и смежных прав, запустившей рыночный оборот соответствующих токенов в реальности наших дней.

9. Токенизация произведений науки

Выше мы говорили о NFT-тренде в отношении произведений искусства и решений технических задач, однако токенизация произведений науки нам также представляется вполне перспективным делом. Здесь нужно помнить о том, что объем передаваемых прав определяет автор как первоначальный правообладатель созданного произведения и потенциальный продавец токена на произведение науки. Согласно доктрине интеллектуальных прав автор полностью и навсегда сохраняет за собой личные права, включая право на имя, право называться автором произведения, право на защиту произведения от искажения и другие права данного типа, при этом имущественными правами или частью из них автор может распорядиться в собственных интересах и без ущерба для своей репутации посредством выпуска токена на произведение науки.

Мы считаем, что в современном обществе найдется немало желающих стать собственником токена на научное произведение, поскольку позитивный эффект результатов научных исследований мы наблюдаем в повседневной жизни, плюс популярность науки и инноваций непрерывно растет в развитых странах. По этой причине владение токеном на научное произведение будет повышать престиж и статус его правообладателя. Кроме того, токены на произведения науки имеют высокий потенциал в качестве средства измерения ценности в постэкономическом обществе и как инструмент для ее накопления. Научное сообщество вследствие глобальной интегрированности и включенности в отраслевые «научные клубы» находится в полной готовности к эффективному использованию механизмов выработки консенсуальной ценности произведений науки для их последующей токенизации и подключения таким образом к совершенно новому источнику средств на вознаграждение ученых и финансирование научных исследований.

Выводы

В настоящей статье осуществлен анализ гипотезы и совокупности поддерживающих ее аргументов о том, что невзаимозаменяемые токены на объекты цифрового искусства представляют собой технологию извлечения средств из активов, которые не имеют реальной стоимости, посредством введения в заблуждение их покупателей. В качестве обоснования данной позиции ее приверженцы называют отсутствие материальной составляющей товара; наличие неограниченных возможностей по созданию дополнительных цифровых копий произведения, обесценивающих оригинал произведения и его реплики; а также тот факт, что невзаимозаменяемые токены имеют ценность только в узкоспециализированных малочисленных сообществах, но не на широком рынке.

²⁸ Berman, B. (2021). IBM-IPwe Partnership Hopes to Increase Patent Efficiency, Propel Transactions. *IPWatchdog*. <https://www.ipwatchdog.com/2021/06/07/ibm-ipwe-partnership-hopes-increase-patent-efficiency-propel-transactions/id=134326>

В работе дано описание способов незаконного обогащения с использованием NFT через хищение чужого имущества, незаконное приобретение прав на него, нарушение авторских прав, а также причинение ущерба путем обмана или злоупотребления доверием. Предложены рекомендации по недопущению и обходу описанных рисков.

Позитивные перспективы токенизации творческих продуктов детально показаны на примере музыкальной индустрии. Подробно описаны одиннадцать моделей инновационного использования музыкальных композиций. Проанализированы положительные и отрицательные стороны реализации этих подходов, их влияние на общественные отношения в сфере создания и потребления музыки. Сделан вывод о том, что в реалиях ремикс-культуры, сложившихся в результате широкого проникновения технологий создания, использования и трансформации контента, те отношения и тенденции развития, что оформились в музыкальной индустрии, получат свое распространение в других областях науки и искусства.

В заключение мы рассмотрели умозаключения исследователей относительно токенизации других результатов интеллектуальной деятельности. В их число вошли артефакты компьютерного гейминга, результаты классического и цифрового изотворчества, патенты на изобретения, полезные модели и промышленные образцы, а также оригинальный взгляд на целесообразность токенизации результатов научной деятельности.

Список литературы

- Ayres, C. E. (1962). *The Theory of Economic Progress: a Study of the Fundamentals of Economic Development and Cultural Change*. Schocken Books.
- Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Sci Rep*, 12, 2178. <https://doi.org/10.1038/s41598-022-05920-6>
- Chey, H.-K. (2022). Cryptocurrencies and the IPE of money: an agenda for research. *Review of International Political Economy*, 1–16. <https://doi.org/10.1080/09692290.2022.2109188>
- Colicev, A. (2023). How can non-fungible tokens bring value to brands. *International Journal of Research in Marketing*, 40(1), 30–37. <https://doi.org/10.1016/j.ijresmar.2022.07.003>
- Commons, J. R. (1959). *Institutional economics: its place in political economy*. Madison: University of Wisconsin Press.
- Far, S. B., Bamakan, S. M. H., Qu, Q., & Jiang, Q. (2022). A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. *Procedia Computer Science*, 214, 755–762. <https://doi.org/10.1016/j.procs.2022.11.238>
- Gioia, T. (2019). *Music: a subversive history*. Basic Books.
- Goel, A. K., Bakshi, R., & Agrawal, K. K. (2022). Web 3.0 and decentralized applications. *Materials Proceedings*, 10(1), 8. <https://doi.org/10.3390/materproc2022010008>
- Hale, R. L. (1952). *Freedom Through Law. Public Control of Private Governing Power*. Columbia University Press.
- Henry, C. (Ed.). (2007). *Entrepreneurship in the creative industries: An international perspective*. Edward Elgar Publishing.
- Hilko, M. R. (2021). *Disrupting Copyright. How Disruptive Innovations and Social Norms are Challenging IP Law*. Taylor & Francis.
- Jelil, S. N. (2022). *Non-Fungible Tokens, Crypto-Assets and Web3: What's in It for Conservation Science?* <http://dx.doi.org/10.2139/ssrn.4282312>
- Kraizberg, E. (2023). Non-fungible tokens: a bubble or the end of an era of intellectual property rights. *Financial Innovation*, 9, 32.
- Michalski, R., Jankowski, J., & Kazienko, P. (2012, November). Negative effects of incentivised viral campaigns for activity in social networks. In *2012 Second International Conference on Cloud and Green Computing Xiangtan, China* (pp. 391–398). <https://doi.org/10.1109/CGC.2012.95>
- Momtaz, P. P. (2022). Some very simple economics of Web3 and the Metaverse. *FinTech*, 1(3), 225–234. <https://doi.org/10.3390/fintech1030018>

- Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons*, 66(2), 191–202. <https://doi.org/10.1016/j.bushor.2022.06.002>
- Okediji, R. L. (Ed.). (2017). *Copyright law in an age of limitations and exceptions*. Cambridge University Press.
- Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Applied Sciences*, 13(4), 2231. <https://doi.org/10.3390/app13042231>
- Santiago, J. M. (2017). The «Blurred Lines» of Copyright Law: Setting a New Standard for Copyright Infringement in Music. *Brooklyn Law Review*, 83(1). <https://brooklynworks.brooklaw.edu/blr/vol83/iss1/18/>
- Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Springer International Publishing.
- Walker, W. (2022). *The Definitive Guide to NFT Investing. Learn to Profit From the NFT, Metaverse, and Crypto Gaming Connection*. PublishDrive.
- Wilson, K. B., Karg, A., & Ghaderi, H. (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons*, 65(5), 657–670. <https://doi.org/10.1016/j.bushor.2021.10.007>
- Yue, Y., Li, X., Zhang, D., & Wang, S. (2021). How cryptocurrency affects economy? A network analysis using bibliometric methods. *International Review of Financial Analysis*, 77, 101869. <https://doi.org/10.1016/j.irfa.2021.101869>

Сведения об авторе



Будник Руслан Александрович – доктор юридических наук, профессор, заместитель директора Международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам», Национальный исследовательский университет «Высшая школа экономики»; профессор Российско-китайского центра сравнительного правоведения, Университет «МГУ-ППИ в Шэньчжэне».

Адрес: 101000, Российская Федерация, г. Москва, Большой Трёхсвятительский переулок 3, 436;

518172, Китайская Народная Республика, провинция Гуандун, г. Шэньчжэнь, район Лунган, Даюньсиньчэн, ул. Гоцзидасюэюань, 1

E-mail: rbudnik@hse.ru

ORCID ID: <https://orcid.org/0000-0001-8076-1560>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=43760909700>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/1299111>

Google Scholar ID: <https://scholar.google.com/citations?user=Z9tacXwAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=822805

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики:

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.41.26 / Личные неимущественные права авторов и исполнителей

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 16 февраля 2023 г.

Дата одобрения после рецензирования – 1 мая 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.25>

Risks and Prospects of Creativity Tokenization

Ruslan A. Budnik

National Research University "Higher School of Economics"
Moscow, Russian Federation;
Shenzhen MSU-BIT University
Shenzhen, China

Keywords

Art,
blockchain,
creativity,
digital technologies,
law,
music,
NFT,
token,
tokenization,
work of art

Abstract

Objective: tokenization of creativity, alongside with cryptoeconomy and Web3 network infrastructure, is a notable trend in the development of modern society in the third decade of the 21st century. The objective of this article is to explore the risks and prospects emerging in the process of disposition of the creative labor results in the form of non-fungible tokens.

Methods: the research methodology is based on analysis of varied viewpoints on the problem, including diametrically opposing concepts. The opposing views of the observers manifest their attitude to tokenization of creative products as a speculative scheme, on the one hand, and a promising tool of creative industries development, on the other.

Results: the probable negative consequences of tokenization of intellectual activity results are identified; author's recommendations on managing these risks are given. Another result of this publication is analysis of economic-legal prospects stemming from tokenization of the objects of copyright and neighboring rights by the example of musical pieces.

Scientific novelty: it consists in presenting and substantiating a hypothesis that the relations formed in the musical industry under the modern sociocultural and technological realities will be reproduced in other creative industries. Also, scientific novelty consists in the analysis of prospects of tokenization of such results of intellectual activity as gaming artifacts, works of traditional and digital visual arts, patents and scientific achievements. The use of non-fungible tokens the ecosystem of network computer games will allow gamers

© Budnik R. A., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

to buy and sell rights to game pieces autonomously from game publishers. Tokenization of industrial property objects and individualization means will ensure protection of intellectual rights of their authors while waiting for the issuance of a state protection document. In the modern society, there will be many of those wishing to become an owner of a token for a scientific work, as the popularity of science and innovations is constantly growing in developed countries. Ownership of a token for a scientific work will be regarded a moral investment, increasing the prestige and status of its owner. Tokens for scientific works have a high potential as a means of measuring value in a post-economic society.

Practical significance: it consists in the description of innovative means of using creative products and business models based on tokenization of the results of intellectual activity, ready to be implemented in practice.

For citation

Budnik, R. A. (2023). Risks and Prospects of Creativity Tokenization. *Journal of Digital Technologies and Law*, 1(3), 587–611. <https://doi.org/10.21202/jdtl.2023.25>

References

- Ayres, C. E. (1962). *The Theory of Economic Progress: a Study of the Fundamentals of Economic Development and Cultural Change*. Schocken Books.
- Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Sci Rep*, 12, 2178. <https://doi.org/10.1038/s41598-022-05920-6>
- Chey, H.-K. (2022). Cryptocurrencies and the IPE of money: an agenda for research. *Review of International Political Economy*, 1–16. <https://doi.org/10.1080/09692290.2022.2109188>
- Colicev, A. (2023). How can non-fungible tokens bring value to brands. *International Journal of Research in Marketing*, 40(1), 30–37. <https://doi.org/10.1016/j.ijresmar.2022.07.003>
- Commons, J. R. (1959). *Institutional economics: its place in political economy*. Madison: University of Wisconsin Press.
- Far, S. B., Bamakan, S. M. H., Qu, Q., & Jiang, Q. (2022). A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. *Procedia Computer Science*, 214, 755–762. <https://doi.org/10.1016/j.procs.2022.11.238>
- Gioia, T. (2019). *Music: a subversive history*. Basic Books.
- Goel, A. K., Bakshi, R., & Agrawal, K. K. (2022). Web 3.0 and decentralized applications. *Materials Proceedings*, 10(1), 8. <https://doi.org/10.3390/materproc2022010008>
- Hale, R. L. (1952). *Freedom Through Law. Public Control of Private Governing Power*. Columbia University Press.
- Henry, C. (Ed.). (2007). *Entrepreneurship in the creative industries: An international perspective*. Edward Elgar Publishing.
- Hilko, M. R. (2021). *Disrupting Copyright. How Disruptive Innovations and Social Norms are Challenging IP Law*. Taylor & Francis.
- Jelil, S. N. (2022). *Non-Fungible Tokens, Crypto-Assets and Web3: What's in It for Conservation Science?* <http://dx.doi.org/10.2139/ssrn.4282312>
- Kraizberg, E. (2023). Non-fungible tokens: a bubble or the end of an era of intellectual property rights. *Financial Innovation*, 9, 32.
- Michalski, R., Jankowski, J., & Kazienko, P. (2012, November). Negative effects of incentivised viral campaigns for activity in social networks. In *2012 Second International Conference on Cloud and Green Computing Xiangtan, China* (pp. 391–398). <https://doi.org/10.1109/CGC.2012.95>
- Momtaz, P. P. (2022). Some very simple economics of Web3 and the Metaverse. *FinTech*, 1(3), 225–234. <https://doi.org/10.3390/fintech1030018>

- Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons*, 66(2), 191–202. <https://doi.org/10.1016/j.bushor.2022.06.002>
- Okediji, R. L. (Ed.). (2017). *Copyright law in an age of limitations and exceptions*. Cambridge University Press.
- Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Applied Sciences*, 13(4), 2231. <https://doi.org/10.3390/app13042231>
- Santiago, J. M. (2017). The «Blurred Lines» of Copyright Law: Setting a New Standard for Copyright Infringement in Music. *Brooklyn Law Review*, 83(1). <https://brooklynworks.brooklaw.edu/blr/vol83/iss1/18/>
- Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Springer International Publishing.
- Walker, W. (2022). *The Definitive Guide to NFT Investing. Learn to Profit From the NFT, Metaverse, and Crypto Gaming Connection*. PublishDrive.
- Wilson, K. B., Karg, A., & Ghaderi, H. (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons*, 65(5), 657–670. <https://doi.org/10.1016/j.bushor.2021.10.007>
- Yue, Y., Li, X., Zhang, D., & Wang, S. (2021). How cryptocurrency affects economy? A network analysis using bibliometric methods. *International Review of Financial Analysis*, 77, 101869. <https://doi.org/10.1016/j.irfa.2021.101869>

Author information



Ruslan A. Budnik – Doctor of Juridical Sciences, Professor, Deputy Director of International scientific-educational center “UNESCO Chair of Copyright, Neighboring, Cultural and Information Rights”, National Research University “Higher School of Economics”; Professor at Russian-Chinese Center for comparative legal science, Shenzhen MSU-BIT University

Address: 3 Bolshoy Trekhsvyatitskiy pereulok, 436, 101000 Moscow, Russian Federation;

No. 1, International University Park Road, Dayun New Town, Longgang District, Shenzhen, Guangdong Province, PRC, 518172, China

E-mail: rbudnik@hse.ru

ORCID ID: <https://orcid.org/0000-0001-8076-1560>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=43760909700>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/1299111>

Google Scholar ID: <https://scholar.google.com/citations?user=Z9tacXwAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=822805

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – February 16, 2023

Date of approval – May 1, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:34.096:7.091.5:7.097:004

EDN: <https://elibrary.ru/xoftaw>

DOI: <https://doi.org/10.21202/jdtl.2023.26>

«Чисто крысиная страна» – размышления о решении по делу 2022-001-FB-UA Наблюдательного совета Фейсбука (Дело мультфильма о городе Книн)

Гергели Ференц Лендваи

Католический университет Петера Пазмания
г. Будапешт, Венгрия

Ключевые слова

Мета*,
мультфильм о городе Книн,
Наблюдательный совет,
права человека,
право,
регулирование,
свобода выражения мнения,
Фейсбук*,
цифровые технологии,
язык ненависти

Аннотация

Цель: в работе представлен анализ решения Наблюдательного совета Фейсбука* по делу 2022-001-FB-UA, известному как «Дело мультфильма о городе Книн». Цель исследования – определение места данного дела в историческом и культурном контексте и выработка критического подхода к проблеме модерирования контента в компании «Фейсбук»*.

Методы: основным методом, используемым в работе, является изучение источников. Исследование опирается на сравнительное изучение и анализ кейсов. Использованы положения различных дисциплин, таких как философия права, международное право, право в области средств массовой информации, регулирование деятельности платформ, история.

Результаты: в работе представлен контекст дела мультфильма о городе Книн и основные решения Наблюдательного совета Фейсбука* с их обоснованиями. Кроме того, отражена концепция языка ненависти в понимании Наблюдательного совета и сделана попытка показать контекст и описать основные проблемы и возможные решения в области модерирования контента в компании Мета* на примере данного дела.

Научная новизна: с момента опубликования решения по делу мультфильма о городе Книн в 2022 г. он не подвергался глубокому историческому и контекстуальному анализу. До настоящего времени вышли лишь несколько работ, анализирующих его с юридической точки зрения.

© Лендваи Г. Ф., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Практическая значимость: полученные результаты важны в трех основных аспектах: (1) они могут быть использованы для дальнейшего критического анализа модерирования контента в компании «Фейсбук»*, (2) они могут служить в качестве рекомендаций в области регулирования деятельности платформ и разработки инструкций и (3) они показывают исключительную актуальность и важность целостного подхода к определению языка ненависти. В рамках последнего аспекта работа доказывает, что историческая, культурная, общественная и символическая интерпретация и понимание проблемы определения языка ненависти является не только практически применимым, но и единственным целесообразным методом для распознавания, определения и вынесения суждения о предполагаемом использовании языка ненависти.

Для цитирования

Лендваи, Г. Ф. (2023). «Чисто крысиная страна» – размышления о решении по делу 2022-001-FB-UA Наблюдательного совета Фейсбука (Дело мультфильма о городе Книн). *Journal of Digital Technologies and Law*, 1(3), 612–628. <https://doi.org/10.21202/jdtl.2023.26>

Содержание

Введение

1. Детали дела о мультфильме о городе Книн

2. Решение Наблюдательного совета

Заключение

Список литературы

Введение

В конце 2018 г. профессор Гарвардской школы права Ноа Фельдман выдвинул идею квази Верховного суда¹, которую позднее подхватил глава компании «Мета»* (в то время «Фейсбук»*) Марк Цукерберг (Klonick, 2020; Douek, 2021). Несмотря на определенную критику относительно возможных проблем с надзором и объективностью (Sale, 2022), в компании был создан Совет, позиционировавшийся как независимый, законный и официальный (Bayer, 2022) институт саморегулирования (Bayer, 2022; Klonick, 2020), призванный обеспечить соблюдение компанией баланса между принципом свободы выражения мнений и соответствующими ценностями (такими как свобода слова, безопасность, защита неприкосновенности частной жизни) (Pickup, 2021). Что касается саморегулирования, Medzini предлагает использовать выражение «способствует саморегулированию», чтобы подчеркнуть факт делегирования обязанностей по регулированию в дополнение к классическим механизмам посредничества (Medzini, 2022). При этом определение Наблюдательного совета как

¹ Klonick, Kate: Inside the making of Facebook's Supreme Court. *The New Yorker*. <https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court>

Верховного суда (COWLS & DOMINIQUE-SCHRAMM, 2022) представляется преувеличением или даже наивностью (SCHULTZ, 2021), ведь этот независимый орган, учрежденный компанией «Мета»*, использует Стандарты сообщества «Фейсбук»* (PICKUP, 2021) наряду с международным законом о правах человека и относящимися к нему положениями (например, международными принципами в области прав человека) (VUKČEVIĆ, 2021; BENESCH, 2020; HELFER & LAND, 2022); поэтому актуальность и важность понимания, изучения и проверки решений Наблюдательного совета представляются более насущными, чем когда-либо ранее. Нужно учитывать, что, несмотря на договорной характер отношений между пользователями и «Фейсбуком»* (SCHULTZ, 2021; BAYER, 2022), структура власти в сфере свободы выражения мнений, как верно отмечает Schultz (SCHULTZ, 2021), кардинально изменилась после введения Наблюдательного совета. Хотя решения Наблюдательного совета направлены на поддержание ответственности компании «Мета»* за ее решения и осуществляемые меры (O'KANE, 2022), а значит, являются обязательными исключительно для «Фейсбука»* (WONG & FLORIDI, 2022), однако этот орган уникален в отношении степени своего воздействия, несмотря на критическую позицию «Фейсбука»* относительно выражения мнений в сети и коммуникации в целом (WONG & FLORIDI, 2022). Как признает Schultz (SCHULTZ, 2021), «члены Наблюдательного совета – не только 'судьи': они также частично ответственны за свое законодательство. Это уникальная концентрация власти над доступом к свободе выражения мнений для миллиардов людей. Никогда в истории человечества такой узкий круг людей не обладал такой властью над возможностью такого количества других людей быть услышанными». Такая гигантская власть над жизнями людей (CHANDER, 2012) и соблюдением прав человека неразрывно связана с ожиданиями публики: в частности, способен ли Наблюдательный совет разрешить спор, порожденный цифровизацией коммуникации, – например, относительно языка ненависти в сети или кибербуллинга (PONGÓ, 2020)²? Ответ на этот вопрос в настоящее время далеко не однозначен, ведь Наблюдательный совет склонен придерживаться более консервативного подхода в ситуациях, подобных вышеописанной: лишь мизерное количество дел вообще доходит до Совета (WONG & FLORIDI, 2022; NUNZIATO, 2022), а юридическое обоснование по ним зачастую является теоретическим. Такие дела основываются на абстрактных или общих принципах (KULICK, 2022). Хотя Совет часто принимает на рассмотрение основополагающие и неоднозначные дела (TAKHSHID, 2021) (см., например, решение о Черном Пите (Zwarte Piet) как квази фундаментальное решение по проблеме чернокожих³ или решение по делу о дезинформации относительно COVID-19⁴), большинство дел касается языка ненависти (WONG & FLORIDI, 2022) и реакции на него со стороны «Фейсбука»*. В данной статье мы обсудим так называемое дело мультфильма

² Klonick, Kate. (2019, October 28). Does Facebook's Oversight Board Finally Solve the Problem of Online Speech. *CIGI*. <https://www.cigionline.org/articles/does-facebooks-oversight-board-finally-solve-problem-online-speech/>

³ Oversight Board decision no. 2021-002-FB-UA. <https://oversightboard.com/sr/decision/2021/002/public-comments>

⁴ Oversight Board decision no. 2020-006-FB-FBR. <https://oversightboard.com/sr/decision/006/public-comments>

о городе Книн⁵, которое относительно недавно – в марте 2022 г. – было отобрано для рассмотрения в Наблюдательном совете⁶ в результате требования пользователя «Фейсбука»* удалить видеоролик, переделанный из диснеевского мультфильма, в котором сербы изображены в виде крыс⁷.

1. Детали дела мультфильма о городе Книн

Данное дело было отобрано для обсуждения в Наблюдательном совете в марте 2022 г. по обращению пользователя в соответствии с официальным порядком отбора трех дел для слушания в Наблюдательном совете. Вызвавший это обращение пост содержал видеоролик, опубликованный на странице «Фейсбука»* в Хорватии (pretjerivač). Поскольку ролик был на хорватском языке, компания Мета перевела содержание основного поста. В этом переводе ролик назывался «Дудочник из Чавоглаве и крысы из города Книн». Прежде чем рассматривать детали дела, необходимо дать контекстуальную интерпретацию основных его факторов. Чавоглаве – небольшая деревушка в далматинской провинции на юге Хорватии. По результатам хорватской переписи 2020 г., в ней жило 190 человек⁸.

Хорваты очень гордятся деревней Чавоглаве, так как группа «Томпсон» (хорватская рок-группа под управлением Марко Перковича) написала о ней патриотическую песню хорватских националистов (которую некоторые считают идеологическим призывом (Robionek, 2017))⁹. Эта песня стала символом для Хорватии (Robionek, 2017), и деревня приобрела широкую известность в стране (Melichárek, 2015). Книн – город с населением около 8 000–10 000 человек, расположенный недалеко от Чавоглаве на юге Хорватии. Он был крупнейшим городом в эпоху Средневековья, а также известен как крепость сербов во время вышеупомянутой войны. Кроме того, в 1991 г. Книн короткое время был столицей непризнанного сербского военного округа – Республики Сербская Краина (Leutloff-Grandits, 2008). Сербы исторически проживали в Книне. Перед войной около 80 % населения называли себя сербами. Эта ситуация резко изменилась после войны, и в 2021 г. всего 21,42 % населения стали именовать себя сербами (Leutloff-Grandits, 2008; Douek, 2020). В городе существует проблема национализма. 5 августа 2011 г. хорватское правительство отметило 16-ю годовщину операции «Буря», проведенной вооруженными силами Хорватии в августе–ноябре 1995 г. в регионе Краина и городе Книн¹⁰. Это была массированная наступательная военная операция против хорватских сербов (Banjeglav, 2015). Тысячи сербов были вынуждены бежать, и многие из них под-

⁵ Oversight Board decision no. 2022-001-FB-UA. <https://oversightboard.com/news/1629549600777906-oversight-board-overturms-meta-s-original-decision-in-knin-cartoon-case-2022-001-fb-ua/>

⁶ Oversight Board, Announcing the Board's next cases. <https://oversightboard.com/news/175638774325447-announcing-the-oversight-board-s-next-cases/>

⁷ Oversight Board Selects a Case Regarding a Video of an Edited Cartoon Depicting a Croatian City. Facebook Transparency Center. <https://transparency.fb.com/hu-hu/oversight/oversight-board-cases/cartoon-case/>

⁸ Opcina Ruzic. Čavoglave. <https://www.opcina-ruzic.hr/index.php/naselja/cavoglave>

⁹ Thompson-Cavoglave. <https://www.youtube.com/watch?v=tVaYgPBYNQQ>

¹⁰ Amnesty International Public Statement, Croatia: Praise for “Operation Storm” creates climate of impunity. Index: EUR 64/010/2011. <https://www.amnesty.eu/wp-content/uploads/2018/10/AIR12-Report-English.pdf>

вергались негуманному обращению со стороны хорватской армии (Banjeglav, 2015). Организация Amnesty International выразила озабоченность фактом прославления военных преступников и призвала Хорватию начать разбираться с последствиями войны (Banjeglav, 2015). Ситуация осложняется тем, что многие преступления так и не были расследованы, в том числе и совершенные в городе Книн, поскольку, по словам Vesna Terselic, главы Комитета Хорватии по правам человека, это не было приоритетом для судебной системы Хорватии¹¹. Хотя бывший мэр Marko Jelić попытался сгладить непростые отношения между сербами и хорватами¹², напряженность очевидна по сей день, служа основанием для многочисленных конфликтов (к примеру, недавно хорватское министерство иностранных дел потребовало публичных извинений от сербской делегации, посетившей Книн, за то, что они назвали город «сербским и оккупированным»¹³). Учитывая вышесказанное и в полном соответствии с Общими критериями отбора дел Наблюдательным советом¹⁴, мультфильм о городе Книн был обоснованно отобран для рассмотрения как содержащий язык ненависти в контексте давнего националистического конфликта между сербами и хорватами и проводящий историческую и культурную параллель между двумя городами.

Возвращаясь к делу мультфильма о городе Книн, необходимо изложить его детали¹⁵. Получившее печальную славу видео было переделано из диснеевского мультфильма «Гамельнский крысолов», основанного на известной германско-саксонской сказке. Ее главный герой – крысолов, который выманил крыс из города Хамельн, играя на своей волшебной дудочке. Исследователи полагают, что в этой сказке изображалась идея контроля над грызунами или борьбы с инфекциями (Singleton et al., 2003). В мультфильме показан город Хамельн, наводненный полчищами крыс. В видео на хорватском языке говорится, что крысы хотели жить в «чисто крысиной стране», поэтому они беспрестанно пытались выдавить людей из города. В первой части видео можно также увидеть явную провокацию – над воротами города хорошо читается надпись «Книн». Она наложена на оригинальное изображение. Поисковая система «Фейсбука»^{*} не находит мультфильм о городе Книн, однако оригинальный мультфильм можно посмотреть на «Ютубе»; описанная сцена открывает мультфильм¹⁶. Далее зрители видят множество крыс, бегающих по городу; люди пытаются отогнать их метлами и палками. Затем показана сцена,

¹¹ Operation Storm Anniversary Highlights Croatia and Serbia's Bitter Mistrust. <https://balkaninsight.com/2022/08/03/operation-storm-anniversary-highlights-croatia-and-serbias-bitter-mistrust/>

¹² Mayor of Knin: I will invite Serbs to return, this is their city too. RTRS. <https://dijasporars.com/en/gradonacelnik-knina-pozvacu-srbe-da-se-vrate-ovo-je-i-njihov-grad/>

¹³ Hina. (2021, January 29). Croatia demands apology from Serbia for calling Knin "Serbian occupied town". № 1. <https://rs.n1info.com/english/news/croatia-demands-apology-from-serbia-for-calling-knin-serbian-occupied-town/>

¹⁴ Oversight Board. *Overarching Criteria for Case Selection*, 2.

¹⁵ Decision no. 2022-001-FB-UA.

¹⁶ Nestanak Srba iz Knina. <https://www.youtube.com/watch?v=5nQjwH9vHTU>

где крысы мгновенно уничтожают огромное количество еды. Картина хаоса меняется при появлении дудочника из Чавоглаве. Сначала крысы не обращают на него внимания. Затем показано, как они высовывают языки, узнав о его появлении (рассказчик также сообщает о продолжении «великой крысиной агрессии»). В соответствии с первоначальным фольклорным сюжетом и видеорядом, крысолов начинает играть мелодию на своей волшебной дудочке. Крысы собираются огромными толпами, начинают танцевать на задних лапах, петь свою любимую песню и идут за крысоловом, который выводит их за пределы города.

Один из самых спорных моментов видео – это аудиосодержание, которое в качестве любимой песни крыс представляет песню в честь Момчило Джуича. Он был сербским православным священником и воеводой четников. Джуич сыграл решающую роль в организации сербского сопротивления во время Второй мировой войны. Однако с точки зрения хорватов его репутация не такая героическая, так как он и все четники были врагами хорватского государства (Ramet, 2011). Динарская четническая дивизия под руководством Момчило Джуича несет ответственность за тысячи кровавых преступлений против хорватских гражданских лиц в конце 1944 г. Среди них разграбление деревень, убийства, изнасилования, грабежи жителей¹⁷. Писатель и историк Михаэл Соболевски считает террористические действия четников в деревне Криви-Пут одной из самых страшных трагедий Второй мировой войны.

Когда последняя крыса покидает город Книн, люди выражают радость. Затем в мультфильме показан крысолов, ведущий крыс к трактору, появляющемуся на горизонте. Крысы садятся на трактор, и он исчезает. Крысолов радостно машет рукой вслед трактору (волшебному трактору, как саркастически замечает рассказчик), полному крыс, а рассказчик заканчивает видео, говоря, что крысы «навсегда исчезли из этих краев» и «все жили долго и счастливо». Трактор, на котором покидают город, – это также исторический символ. В 1995 г. во время операции «Буря» – спорной и неоднозначной военной акции хорватов – многие из 200 тысяч этнических сербов вынуждены были покинуть Хорватию на грузовиках и тракторах¹⁸. По словам журналистки Associated Press Юлианы Мойсилович, опубликованном в газете Los Angeles Times в 1995 г., это бегство было «эпичной сценой хаоса»¹⁹. Мойсилович в подробностях описала ее: «Растерянные люди с теми пожитками, что успели схватить, спасались на тракторах, автомобилях, телегах

¹⁷ Sobolevski, M. *Robbery and terror of Dinara Četnik division in the Krivi Put region on 28th and 29th December 1944*. <https://hrcak.srce.hr/clanak/27653>

¹⁸ McLaughlin, D. (2015, August 5). Croatia celebration of 1995 military victory alienates ethnic Serbs. *Al Jazeera*. <http://america.aljazeera.com/articles/2015/8/5/croatia-celebration-of-1995-military-victory-alienates-and-angers-serbs1.html>

¹⁹ Croatia Captures Rebel Serb City; Thousands Flee : Balkans: Takeover of Knin sends refugees on panicked flight to Serb-held areas of Bosnia. U.N. officer tells of bodies lying in the streets. Two more peacekeepers killed. <https://www.latimes.com/archives/la-xpm-1995-08-06-mn-32175-story.html>

с лошадьми, велосипедах – на всем, что могло двигаться»²⁰. Также сообщалось, что дороги были забиты испуганными людьми, пытавшимися уехать на тракторах. В общине Топуско сербы и мусульмане набивались в машины (в основном трактора, автобусы и грузовики), чтобы иметь возможность просто покинуть Хорватию²¹. Таким образом, трактор является исторической метафорой страданий, террора и бесчеловечности, которые выпали на долю сербов в конце войны.

Что касается масштабов популярности поста, в тот момент у страницы было более 50 тысяч подписчиков, пост просмотрели более 380 тысяч раз. Несмотря на 397 обращений пользователей, из которых в 362 сообщалось о языке ненависти, компания «Мета»* решила не удалять контент. Это решение²² было оспорено в Наблюдательном совете, после чего «Мета»* провела дополнительную проверку (людьми), чтобы определить, нарушает ли данный контент Стандарты сообщества или политику относительно языка ненависти. После этой проверки также было принято решение не удалять контент. Примечательно, что когда было объявлено о полном разборе дела Наблюдательным советом, компания внесла два существенных изменения в модерацию данного мультфильма. Нужно подчеркнуть, что решение о полном разборе дела было принято в январе 2022 г., так что к этому времени мультфильм был доступен на платформе уже много недель. Сначала компания постановила, что мультфильм не нарушает букву, но не дух политики относительно языка ненависти²³ (цитируем непосредственно из текста решения: «Компания “Мета” объяснила, что решение принято в соответствии с “духом политики”, так как раздел одного из Стандартов сообщества, содержащий обоснование данной политики, ясно дает понять, что данная политика направлена на определенный сценарий, тогда как формулировки данной политики не описывают его напрямую»). Позже было вынесено решение, что нарушение касалось также и буквы политики относительно языка ненависти²⁴. Компания также заключила, что все предыдущие проверки были ошибочными, имея в виду три решения не удалять контент. Путаницы в это дипломатически поспешное обсуждение добавило то, что компания не проинформировала пользователей об изменениях и исправлениях решений, хотя ранее сообщила о том, что контент не нарушает политику компании. Пользователь, представивший дело в Наблюдательный совет, аргументировал свое мнение таким образом: «Крысолов символизирует хорватскую армию, которая в 1995 г. изгнала хорватских сербов, показанных в виде крыс».

²⁰ Mojsilovic, J. (1995, August 6). Shelling of Knin Causes disbelief, panic, flight. <https://www.washingtonpost.com/archive/politics/1995/08/06/shelling-of-knin-causes-disbelief-panic-flight/5cdb41ed-39c1-4c7f-a8f5-ab012c097039/>

²¹ Pomfret, J. (1995, August 7). Thousands of Serb refugees flee Croatian army advance. *The Washington Post*. <https://www.washingtonpost.com/archive/politics/1995/08/07/thousands-of-serb-refugees-flee-croatian-army-advance/2912317d-a965-449e-9c97-62ca900dc6a6/>

²² Klonick, K. (2021, February 12). Inside the making of Facebook’s Supreme Court. <https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court>

²³ Oversight Board Case of Knin Cartoon. *Global Freedom of Expression*. <https://globalfreedomofexpression.columbia.edu/cases/oversight-board-case-of-knin-cartoon/>

²⁴ Oversight Board Selects a Case Regarding a Video of an Edited Cartoon Depicting a Croatian City. <https://transparency.fb.com/ru-ru/oversight/oversight-board-cases/cartoon-case/>

2. Решение Наблюдательного совета

Наблюдательный совет отменил решение компании «Мета»* оставить мультфильм о городе Книн на платформе. Проведя стандартную процедуру, Наблюдательный совет постановил, что ролик нарушает Стандарты сообщества «Фейсбука»* о языке ненависти и призывах к насилию. Цель этих Стандартов – предотвратить возможный вред вне сети, связанный с контентом «Фейсбука»*. С помощью данного документа «Фейсбук»* пытается обратить внимание на язык и контекст и определить важнейшие культурные, контекстуальные, лингвистические и иные точки зрения, которые могут помочь модераторам вмешаться в свободу выражения мнения, если публикуемый контент представляет реальную угрозу общественной или личной безопасности. Политика относительно языка ненависти также запрещает нападки на лиц, обладающих защищаемыми характеристиками, включая этническую принадлежность²⁵. Наблюдательный совет постановил, что изображение сербов в виде крыс является «дегуманизирующим и ненавистническим». Совет также заключил, что видео прославляет акты дискриминации, совершенные в прошлом.

Наблюдательный совет верно понял глубокие исторические и контекстуальные коннотации: замена названия «Хамельн» на название хорватского города «Книн», связь крысолова с хорватской деревней Чавоглаве (отсылка к антисербской песне «Вojна Čavoglave» группы «Thompson», чей лидер родом из Чавоглаве) и образ крыс, спасающихся на тракторах, являются отсылками к хорватской военной операции «Буря». Эта операция, проведенная в 1995 г., привела к изгнанию, убийствам и насильственному уничтожению гражданских лиц – этнических сербов. Комментарии к посту подтверждают, что эти отсылки были понятны лицам, просматривавшим контент²⁶.

На этих основаниях Наблюдательный совет постановил, что данный пост нарушил два ключевых внутренних стандарта компании «Мета»* – ценности достоинства и безопасности.

Как следует из решения Наблюдательного совета, в изучении вопроса приняли участие 40 модераторов, владеющих хорватским языком, и никто из них не счел данный контент нарушающим стандарты «Фейсбука»*. Однако это проблематично также с другой точки зрения – как верно предположил Наблюдательный совет, данное видео, содержащее многочисленные дискриминирующие символы и сравнения, может подстрекать к насилию. Следовательно, компания «Мета»* и ее модераторы не смогли соответствовать не только политике относительно языка ненависти, но и своим собственным Стандартам сообщества о языке ненависти и призывах к насилию.

В своем решении Наблюдательный совет поднял два ключевых вопроса. Во-первых, усиление модерации и работа специализированной команды модераторов не помогли осознать скрытые, но культурно неоспоримые смыслы видеоролика. Как уже упоминалось, в соответствии с собственной политикой относительно языка ненависти компании «Мета»*, при определении языка ненависти следует обращать особое внимание на контекстуальные и культурные различия. Во-вторых, Наблюдательный

²⁵ Oversight Board decision no. 2021-002-FB-UA. <https://oversightboard.com/sr/decision/2021/002/public-comments>

²⁶ Oversight Board overturns Meta's original decision in 'Knin cartoon' case (2022-001-FB-UA). <https://oversightboard.com/news/1629549600777906-oversight-board-overturns-meta-s-original-decision-in-knin-cartoon-case-2022-001-fb-ua/>

совет предложил компании две рекомендации: (1) прояснить Стандарт сообщества о языке ненависти путем создания особого руководства для понимания скрытых отсылок и (2) усовершенствовать систему модификации в соответствии с изменениями в решении компании «Мета»* по данному делу²⁷.

Заключение

Наблюдательный совет ставил своей целью привлечь общественное мнение к делу мультфильма о городе Книн. Таким образом, процесс принятия решения сопровождался созданием общественной платформы для обсуждения, где третьи стороны могли поделиться своим мнением по делу. В приложении «Комментарии общественности»²⁸ Наблюдательный совет опубликовал 13 комментариев без указания авторов. Примечательно, что только два из них поступили из Европы; это вызывает сомнения и вопросы относительно контекстуальной и культурной интерпретации. Что еще более странно, только два комментария в данном приложении доступны для прочтения.

Следует также критически отнестись к ответам компании «Мета»* на вопросы Наблюдательного совета о том, что обсуждаемый пост может быть классифицирован как форма подстрекательства к насилию. Компания заявила, что угроза насилия должна подкрепляться или сопровождаться угрозой исключения или изгнания – то есть какого-либо физически насильственного действия²⁹. Но тогда возникает вопрос о масштабах применимости Стандарта сообщества о языке ненависти и призывах к насилию. По мнению компании, ссылки на крыс и их «бегство» в мультфильме не могут быть безоговорочно и безошибочно расценены как отсылки к возможной угрозе изгнания сербов³⁰. Такое объяснение предполагает весьма высокий порог применимости этих стандартов. Разумеется, нельзя сказать, что данное дело является простым, однако угроза, несомненно, присутствует, так как упомянутые исторические отсылки явно и недвусмысленно указывают на сербов и содержат неприкрытую насмешку над болью, страданиями и утратами, постигшими их в 1995 г. В этом контексте следует также отметить, что рассказчик говорит о счастливой жизни города Книн после того, как все крысы покинули его, что легко можно расценить как призыв к действию.

При принятии данного решения Наблюдательный совет опирался на ряд международных правовых актов, таких как Международный пакт о гражданских и политических правах, Международная конвенция о ликвидации всех форм расовой дискриминации, Рабатский план Управления Верховного комиссара Организации Объединенных Наций по правам человека, комментарии Совета ООН по правам

²⁷ Oversight Board decision no. 2021-002-FB-UA. <https://oversightboard.com/sr/decision/2021/002/public-comments>

²⁸ Oversight Board Public Comment Appendix for Knin Cartoon. <https://oversightboard.com/news/1629549600777906-oversight-board-overturns-meta-s-original-decision-in-knin-cartoon-case-2022-001-fb-ua/>

²⁹ Oversight Board Case of Knin Cartoon. *Global Freedom of Expression*. <https://globalfreedomofexpression.columbia.edu/cases/oversight-board-case-of-knin-cartoon/>

³⁰ Там же.

человека (Общий комментарий № 34). Это достаточно характерно для Наблюдательного совета, который часто опирается на принципы, заложенные в этих документах (Bayer, 2021). Это еще раз подтверждает, что Наблюдательный совет серьезно намерен использовать и применять международно признанные принципы при рассмотрении дел (об этом свидетельствует и тот факт, что многие судьи имеют опыт работы в области международного права³¹). Используя положения статьи 19 Международного пакта о гражданских и политических правах для изучения влияния на свободу выражения мнения автора поста, Наблюдательный совет предложил более конкретную, научную и практическую правовую точку зрения. Наиболее важным аспектом данного дела является вопрос законности. По мнению Наблюдательного совета, концепция, использование, применение и даже в целом понимание положений о языке ненависти компании «Мета»^{*} недостаточно обоснованы, если 40 модераторов не смогли верно опознать в видеоролике признаки языка ненависти. Предложение о выпуске руководства нельзя расценивать как рекомендацию; это знак предупреждения компании о том, что доктрина и недостаток практических инструкций являются системной проблемой, допустившей наличие ненавистнического, оскорбительного, глубоко дискриминационного поста несмотря на почти 400 сообщений пользователей. Во-вторых, компании следует обратить внимание на более глубокую оценку и понимание языковых, этнических, исторических и культурных различий. Совет даже упомянул языковой аспект армяно-азербайджанского конфликта в 2020 г.³² Ответы компании «Мета»^{*} игнорируют эти аспекты, а модераторы явно не смогли опознать очевидные отсылки, что также указывает не на ряд индивидуальных ошибок, а на внутреннюю, скрытую, укоренившуюся и структурную порочность стандартов сообщества. До настоящего времени компания «Мета»^{*} так и не выпустила более четкого руководства по проблемам языка ненависти, призывов к насилию или распознавания таковых. Третье решение можно считать наиболее радикальным. В настоящее время Наблюдательный совет не имеет полномочий напрямую влиять на политику, устанавливаемую компанией «Мета»^{*}, а значит, «внутренние правила» (Goldman & Miers, 2021) могут оставаться неприкосновенными сколь угодно долго, включая спорные алгоритмы, зачастую неспособные распознать незаконный контент (Frazier, 2021). Хотя вопросы свободы высказываний регулируются на основе конституционной доктрины недопущения делегирования полномочий (Elkin-Koren & Perel, 2020; Cows & Dominiquo-Schramm, 2022), задача управления онлайн-пространствами и платформами не может полностью и эксклюзивно выполняться официальными властями, и инициатива «Фейсбука»^{*} по надзору за модерированием, несомненно, способствует выработке механизма совместных действий (Balkin, 2018; Arun 2021). К сожалению, мы пока не наблюдаем рекомендаций, имеющих правовую обязательность для развития политики компании «Мета»^{*}³³, которые служили бы «обоюдоострым мечом»: (1) бесспорно побуждали бы компанию улучшать свои

³¹ What Kind of Oversight Board Have You Given Us? *The University of Chicago Law Review Online*. <https://lawreviewblog.uchicago.edu/2020/05/11/fb-oversight-board-edouek/>

³² Oversight Board decision no. 2021-002-FB-UA. <https://oversightboard.com/sr/decision/2021/002/public-comments>

³³ Facebook Releases an Update on Its Oversight Board: Many Questions, Few Answers. <https://www.lawfareblog.com/facebook-releases-update-its-oversight-board-many-questions-few-answers>

стандарты, внедряя инструкции и в целом совершенствовать модерацию контента (Douek, 2019), задавая стандарты платформы (Bayer, 2021), (2) для усиления ориентации на пользователя обязывали бы компанию внедрять и создавать меры, стандарты и механизмы, полнее отвечающие интересам пользователя (Klonick, 2020) и позволяющие избежать «чрезмерного модерирования» (Rogoff, 2019), и (3) лучше и своевременнее учитывали бы международные принципы³⁴ в приложении к праву на свободу выражения мнений в «Фейсбуке»* (Dvoskin, 2022; Helfer & Land, 2022). В заключение отметим, что для выработки более гибких решений (Douek, 2022) таких проблем, как в случае с мультфильмом о городе Книн, рекомендуется применять более формализованную (Douek, 2022) и в то же время высоко контекстуализированную систему модерации контента. Решение, полнее отвечающее реалиям конкретной компании, подобное предложенному выше, могло бы побудить Наблюдательный совет взять на себя еще более значимую роль в отношении модерации «Фейсбука»* (Gorwa, 2019).

* Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

Список литературы

- Arun, Ch. (2021). Facebook's Faces. *Harvard Law Review Forum*, 135, 22–37.
- Balkin, J. M. (2018). Free Speech is a Triangle. *Columbia Law Review*, 118, 12–20.
- Banjeglav, T. (2015). A Storm of Memory in Post-War Croatia. *Cultures of History Forum*, 4, 34–39.
- Bayer, J. (2021). Rights and Duties of Online Platforms. In J. Bayer, B. Holznapel, P. Korpisaari, L. Woods (Eds.). *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos—Digitalization and the Law. <https://doi.org/10.1002/poi3.298>
- Bayer, J. (2022). A Facebook Ellenőrző Bizottság mint alternatív vitarendező szerv. *Fundamentum*, 3, 5–16.
- Benesch, S. (2020). But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies. *Yale Journal on Regulation Online Bulletin*, 38, 71–86.
- Chander, A. (2012). Facebookistan. *North Carolina Law Review*, 90(5), 56–61.
- Cowls, J-D., & Dominiquo-Schramm, M. (2022). Constitutional Metaphors: Facebook's 'Supreme Court' and the Legitimation of Platform Governance. *New Media & Society*, 3, 23346. <https://doi.org/10.1177/14614448221085559>
- Douek, E. (2019). Facebook's, Oversight Board: Move Fast with Stable Infrastructure and Humility. *North Carolina Journal of Law and Technology*, 21, 123–130.
- Douek, E. (2020). What Kind of Oversight Board Have You Given Us. *The University of Chicago Law Review Online*, 23, 45–59.
- Douek, E. (2021). Governing Online Speech. *Columbia Law Review*, 121(3), 34456.
- Douek, E. (2022). The Siren Call of Content Moderation Formalism. In L. Bollinger, G. Stone (Eds.). *Social Media, Freedom of Speech, and the Future of our Democracy*. Oxford, Oxford University Press. <https://doi.org/10.1093/oso/9780197621080.003.0009>
- Dvoskin, B. (2022). Expert Governance of Online Speech. *Harvard International Law Journal*, 63, forthcoming.
- Elkin-Koren, N., & Perel, M. (2020). Separation of Functions for AI: Restraining Speech Regulation by Online Platforms. *Lewis & Clark Law Review*, 24(3), n.pag. <https://doi.org/10.2139/SSRN.3439261>
- Frazier, K. (2021). Why Meta Users Need a Public Advocate: a Modest Means to Address the Shortcomings of the Oversight Board. *Richmond Journal of Law & Technology*, XXVIII(3), 596–622.
- Goldman, E., & Miers, J. (2021). Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules. *Journal of Free Speech Law*, 1, 192–225.

³⁴ The Oversight Board: Operationalizing the UN Guiding Principles on Business and Human Rights. <https://www.wbcsd.org/contentwbc/download/2248/28541>

- Gorwa, R. (2019). The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review*, 8, 1–22. <https://doi.org/10.14763/2019.2.1407>
- Helfer, L. R., & Land, M. K. (2022). The Facebook Oversight Board's Human Rights Future. *Cardozo Law Review*, 44(6), 1–70.
- Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *The Yale Law Journal*, 129, 2418.
- Kulick, A. (2022). Corporations as Interpreters and Adjudicators of International Human Rights Norms – Meta's Oversight Board and Beyond. *The Law and Practice of International Courts and Tribunals*, 5, 8–17.
- Leutloff-Grandits, C. (2008). Claiming in Postwar Croatia: The Dynamics of Property Relations and Ethnic Conflict in the Knin Region. *Journal of Refugee Studies*, 21(1), 34–45. <https://doi.org/10.1093/jrs/fen004>
- Medzini, R. (2022). Enhanced self-regulation: The case of Facebook's content governance. *New Media & Society*, 24(10), 1–29. <https://doi.org/10.1177/1461444821989352>
- Melichárek, M. (2015). Národná symbolika a mýtus v srbských vojenských piesňach z obdobia r. 1991–1995. *Porta Balkanica*, 7(2), 25–34.
- Nunziato, D. C. (2022). Protecting Free Speech and Due Process Values on Dominant Social Media Platforms. *Hastings Law Journal*, 73(5), 1255.
- O'Kane, R. (2022). Meta's Private Speech Governance and the Role of the Oversight Board: Lessons from the Board's First Decisions. *Stanford Technology Law Review*, 25(2), 167–209.
- Pickup, E. L. (2021). The Oversight Board's Dormant Power to Review Facebook's Algorithms. *Yale Journal on Regulation Bulletin*, 39(1), 2–21.
- Pongó, T. (2020). Új Korszak Az Online Véleménynyilvánítás Korlátozásában? Gondolatok a Facebook Oversight Board működéséről. *Iustum Aequum Salutare*, XVI(4), 147–162.
- Ramet, S. P. (2011). Serbia and the Serbs in World War Two. Berlin, Springer. <https://doi.org/10.1057/9780230347816>
- Robionek, B. (2017). Musik als Transportmittel für Ideologie. In K., Bozay, D. Borstel (Eds.). *Ungleichwertigkeitsideologien in der Einwanderungsgesellschaft*. Wiesbaden, Springer. https://doi.org/10.1007/978-3-658-14245-2_14
- Rogoff, Z. (2019). Five Free Expression Safeguards from a Facebook User's Perspective. *TPRC47: Research Conference on Communications, Information and Internet Policy*. <http://dx.doi.org/10.2139/ssrn.3428062>
- Sale, H. A. (2022). Monitoring Facebook. *Harvard Business Law Review*, 12. <https://ssrn.com/abstract=4213540>
- Schultz, M. (2021). Six Problems with Facebook's Oversight Board. In J. Bayer, B. Holznagel, P. Korpisaari, & L. Woods (Eds.), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos. <https://doi.org/10.5771/9783748929789-145>
- Singleton, F. Hinds, L. A., Krebs, Ch., & Spratt, D. M. (2003). *Rats, mice and people: rodent biology and management*. Canberra, Australian Centre for International Agricultural Research.
- Takhshid, Z. (2021). Regulating Social Media in the Global South. *Vanderbilt Journal of Entertainment & Technology Law*, 24(1), 1–55.
- Vukčević, I. (2021). Facebook Oversight Board's Decision on the Indefinite Suspension of Donald Trump's Account. *Pravni Zapisi*, 12(1), 295–311. <https://doi.org/10.5937/pravzap0-32521>
- Wong, D., & Floridi, L. (2022). Meta's Oversight Board: A Review and Critical Assessment, Minds and Machines. <https://doi.org/10.1007/s11023-022-09613-x>

Информация об авторе



Гергели Ференц Лендваи – доктор права, докторант, Католический университет Петера Пазманы

Адрес: Венгрия, г. Будапешт, улица Хаттью, 17

E-mail: lendvaigergely@me.com

ORCID ID: <https://orcid.org/0000-0003-3298-8087>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/ISU-4560-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=CVKzt1AAAAAJ>

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.19.65 / Правонарушения в области информатики. Ответственность в информационном праве

Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 20 декабря 2022 г.

Дата одобрения после рецензирования – 1 мая 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.26>

"Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case)

Gergely Ferenc Lendvai

Pázmány Péter Catholic University
Budapest, Hungary

Keywords

Digital technologies,
Facebook*,
freedom of expression,
hate speech,
human rights,
knin cartoon,
law,
Meta*,
oversight board,
regulation

Abstract

Objective: the present paper aims to analyse Case Decision 2022-001-FB-UA of Facebook* Oversight Board, also known as the Knin cartoon case and attempts to put the case as well as its procedure in a historical and cultural context to set out a critical approach concerning Facebook's* content moderation.

Methods: the paper uses desk research as the primary source of method. The paper's resource background builds upon comparative case studies and case analysis as well. The paper uses resources from various disciplines: legal philosophy, international law, media law, platform regulation, history.

Results: the paper presents the context of the Knin cartoon case as well as the key findings of the Oversight Board and the reasoning behind its decision. Furthermore, this paper aims to reflect on the idea of hate speech as interpreted by the Oversight Board and makes a tentative to contextualise and introduce the main problems and possible solutions regarding Meta's content moderation in the scope of the present case.

Scientific novelty: the Knin case has not been analysed in such historical and contextual depth before as the case decision was issued in 2022. Only a few analyses from merely legal standpoints were published thus far.

© Lendvai G. F., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Practical significance: the findings regarding the Knin case may be of importance of three main aspects: (1) it could be used for further critical analyses on Facebook's* content moderation, (2) it could serve as a recommendation regarding platform regulation and guideline development and (3) it presents the paramount relevance and significance of the holistic interpretational perspectives when determining hate speech. As for the latter the present paper argues that the historical, cultural, societal and symbolic interpretation and understanding of hate speech determination is not only instrumental, but the only viable method to understand, determine and judge upon alleged hate speech cases.

For citation

Lendvai, G. F. (2023). "Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case). *Journal of Digital Technologies and Law*, 1(3), 612–628. <https://doi.org/10.21202/jdtl.2023.26>

References

- Arun, Ch. (2021). Facebook's Faces. *Harvard Law Review Forum*, 135, 22–37.
- Balkin, J. M. (2018). Free Speech is a Triangle. *Columbia Law Review*, 118, 12–20.
- Banjeglav, T. (2015). A Storm of Memory in Post-War Croatia. *Cultures of History Forum*, 4, 34–39.
- Bayer, J. (2021). Rights and Duties of Online Platforms. In J. Bayer, B. Holznagel, P. Korpisaari, L. Woods (Eds.). *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos–Digitalization and the Law. <https://doi.org/10.1002/poi3.298>
- Bayer, J. (2022). A Facebook Ellenőrző Bizottság mint alternatív vitarendező szerv. *Fundamentum*, 3, 5–16.
- Benesch, S. (2020). But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies. *Yale Journal on Regulation Online Bulletin*, 38, 71–86.
- Chander, A. (2012). Facebookistan. *North Carolina Law Review*, 90(5), 56–61.
- Cowls, J-D., & Dominiquo-Schramm, M. (2022). Constitutional Metaphors: Facebook's 'Supreme Court' and the Legitimation of Platform Governance. *New Media & Society*, 3, 23346. <https://doi.org/10.1177/14614448221085559>
- Douek, E. (2019). Facebook's, Oversight Board: Move Fast with Stable Infrastructure and Humility. *North Carolina Journal of Law and Technology*, 21, 123–130.
- Douek, E. (2020). What Kind of Oversight Board Have You Given Us. *The University of Chicago Law Review Online*, 23, 45–59.
- Douek, E. (2021). Governing Online Speech. *Columbia Law Review*, 121(3), 34456.
- Douek, E. (2022). The Siren Call of Content Moderation Formalism. In L. Bollinger, G. Stone (Eds.). *Social Media, Freedom of Speech, and the Future of our Democracy*. Oxford, Oxford University Press. <https://doi.org/10.1093/oso/9780197621080.003.0009>
- Dvoskin, B. (2022). Expert Governance of Online Speech. *Harvard International Law Journal*, 63, forthcoming.
- Elkin-Koren, N., & Perel, M. (2020). Separation of Functions for AI: Restraining Speech Regulation by Online Platforms. *Lewis & Clark Law Review*, 24(3), n.pag. <https://doi.org/10.2139/SSRN.3439261>
- Frazier, K. (2021) Why Meta Users Need a Public Advocate: a Modest Means to Address the Shortcomings of the Oversight Board. *Richmond Journal of Law & Technology*, XXVIII(3), 596–622.
- Goldman, E., & Miers, J. (2021). Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules. *Journal of Free Speech Law*, 1, 192–225.
- Gorwa, R. (2019). The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review*, 8, 1–22. <https://doi.org/10.14763/2019.2.1407>
- Helfer, L. R., & Land, M. K. (2022). The Facebook Oversight Board's Human Rights Future. *Cardozo Law Review*, 44(6), 1–70.

- Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *The Yale Law Journal*, 129, 2418.
- Kulick, A. (2022). Corporations as Interpreters and Adjudicators of International Human Rights Norms – Meta’s Oversight Board and Beyond. *The Law and Practice of International Courts and Tribunals*, 5, 8–17.
- Leutloff-Grandits, C. (2008). Claiming in Postwar Croatia: The Dynamics of Property Relations and Ethnic Conflict in the Knin Region. *Journal of Refugee Studies*, 21(1), 34–45. <https://doi.org/10.1093/jrs/fen004>
- Medzini, R. (2022). Enhanced self-regulation: The case of Facebook’s content governance. *New Media & Society*, 24(10), 1–29. <https://doi.org/10.1177/1461444821989352>
- Melichárek, M. (2015). Národná symbolika a mýtus v srbských vojenských piesňach z obdobia r. 1991–1995. *Porta Balkanica*, 7(2), 25–34.
- Nunziato, D. C. (2022). Protecting Free Speech and Due Process Values on Dominant Social Media Platforms. *Hastings Law Journal*, 73(5), 1255.
- O’Kane, R. (2022). Meta’s Private Speech Governance and the Role of the Oversight Board: Lessons from the Board’s First Decisions. *Stanford Technology Law Review*, 25(2), 167–209.
- Pickup, E. L. (2021). The Oversight Board’s Dormant Power to Review Facebook’s Algorithms. *Yale Journal on Regulation Bulletin*, 39(1), 2–21.
- Pongó, T. (2020). Új Korszak Az Online Véleménynyilvánítás Korlátozásában? Gondolatok a Facebook Oversight Board működéséről. *Iustum Aequum Salutare*, XVI(4), 147–162.
- Ramet, S. P. (2011). *Serbia and the Serbs in World War Two*. Berlin, Springer. <https://doi.org/10.1057/9780230347816>
- Robionek, B. (2017). Musik als Transportmittel für Ideologie. In K., Bozay, D. Borstel (Eds.). *Ungleichwertigkeitsideologien in der Einwanderungsgesellschaft*. Wiesbaden, Springer. https://doi.org/10.1007/978-3-658-14245-2_14
- Rogoff, Z. (2019). Five Free Expression Safeguards from a Facebook User’s Perspective. *TPRC47: Research Conference on Communications, Information and Internet Policy*. <http://dx.doi.org/10.2139/ssrn.3428062>
- Sale, H. A. (2022). Monitoring Facebook. *Harvard Business Law Review*, 12. <https://ssrn.com/abstract=4213540>
- Schultz, M. (2021). Six Problems with Facebook’s Oversight Board. In J. Bayer, B. Holznagel, P. Korpisaari, & L. Woods (Eds.), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*. Baden-Baden, Nomos. <https://doi.org/10.5771/9783748929789-145>
- Singleton, F. Hinds, L. A., Krebs, Ch., & Spratt, D. M. (2003). *Rats, mice and people: rodent biology and management*. Canberra, Australian Centre for International Agricultural Research.
- Takshid, Z. (2021). Regulating Social Media in the Global South. *Vanderbilt Journal of Entertainment & Technology Law*, 24(1), 1–55.
- Vukčević, I. (2021). Facebook Oversight Board’s Decision on the Indefinite Suspension of Donald Trump’s Account. *Pravni Zapisi*, 12(1), 295–311. <https://doi.org/10.5937/pravzap0-32521>
- Wong, D., & Floridi, L. (2022). Meta’s Oversight Board: A Review and Critical Assessment, Minds and Machines. <https://doi.org/10.1007/s11023-022-09613-x>

Author information



Gergely Ferenc Lendvai – Juris Doctor, dr. and Pázmány Péter Catholic University (PhD candidate)

Address: Hattyú utca 17, Budapest, Hungary

E-mail: lendvaigergely@me.com

ORCID ID: <https://orcid.org/0000-0003-3298-8087>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/ISU-4560-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=CVKzt1AAAAAJ>

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – December 20, 2022

Date of approval – May 1, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 346.7:34.096

EDN: <https://elibrary.ru/vbowtb>

DOI: <https://doi.org/10.21202/jdtl.2023.27>

Интеллектуальные транспортные системы – основа de lege ferenda транспортной системы Российской Федерации

Мария Анатольевна Бажина

Уральский государственный юридический университет имени В. Ф. Яковлева
г. Екатеринбург, Российская Федерация

Ключевые слова

Безопасность,
беспилотное транспортное
средство,
высокоавтоматизированное
транспортное средство,
интеллектуальная
транспортная система,
искусственный интеллект,
право,
правовое регулирование,
транспортная
инфраструктура,
транспортное
законодательство,
цифровые технологии

Аннотация

Цель: исследование тенденций правового регулирования применения интеллектуальных транспортных систем в условиях цифровой трансформации транспортного сектора экономики, а именно нарастающего значения интеллектуальных транспортных систем в будущей транспортной системе Российской Федерации.

Методы: системно-структурный метод является основой изучения интеллектуальных транспортных систем. С помощью него представляется возможным изучить архитектуру интеллектуальных транспортных систем как сложного структурного единства. Наряду с указанным методом используются также сравнительно-правовой метод, направленный на иллюстрацию различий и сходных черт в правовом регулировании применения интеллектуальных транспортных систем. Методы правового моделирования и прогнозирования, а также формально-логический метод выступают второстепенными методами для полноценного изучения правового регулирования интеллектуальных транспортных систем.

Результаты: в статье представлены концептуальные подходы по определению понятия «интеллектуальные транспортные системы», выделению иерархии интеллектуальных транспортных систем, которым отводится основополагающее место в построении транспортной отрасли. На основе проведенного анализа делаются выводы о векторах формирования транспортного законодательства, направленного на регулирование применения интеллектуальных транспортных систем.

© Бажина М. А., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: в статье представлен концептуальный подход по формированию правового регулирования интеллектуальных транспортных систем. С этой целью рассмотрен вопрос о сущностном содержании понятия «интеллектуальные транспортные системы» на легальном и научном уровнях, показаны существующие терминологические проблемы для выстраивания правового регулирования. Анализ архитектуры интеллектуальных транспортных систем позволил впервые сформулировать основные подходы к формированию правового регулирования отдельных ее элементов (в том числе высокоавтоматизированных и полностью автоматизированных транспортных средств, «умной» инфраструктуры и т. д.) не обособленно, а как составных частей целого.

Практическая значимость: представленный в исследовании материал и сделанные на его основе выводы способствуют развитию правового регулирования транспортной отрасли в условиях цифровой трансформации. В статье делается акцент именно на правовом регулировании интеллектуальных транспортных систем с учетом их технических и технологических особенностей. Именно интеллектуальные транспортные системы являются *de lege ferenda* транспортной системы, которая предопределяет вектор трансформации транспортного законодательства. В свою очередь разработка правовых основ позволяет расширять географию внедрения технических новелл и делать их применение более масштабным.

Для цитирования

Бажина, М. А. (2023). Интеллектуальные транспортные системы – основа *de lege ferenda* транспортной системы Российской Федерации. *Journal of Digital Technologies and Law*, 1(3), 629–649. <https://doi.org/10.21202/jdtl.2023.27>

Содержание

Введение

1. Онтология понятия «интеллектуальные транспортные системы»
2. Архитектура (структура) интеллектуальных транспортных систем
3. Перспективы развития правового регулирования применения интеллектуальных транспортных систем

Выводы

Список литературы

Введение

Современная национальная и глобальная транспортные системы характеризуются постоянным увеличением количества транспортных средств, участвующих в перемещении грузов и пассажиров. Такая тенденция имеет следующие негативные последствия:

- 1) рост количества транспортных происшествий, в большинстве случаев непосредственной причиной которых становится человеческий фактор;
- 2) вредное воздействие на окружающую среду (Bagreeva et al., 2019);
- 3) перегруженность транспортных путей, что приводит к проблемам в координации логистических цепочек и снижению скорости доставки грузов (Du et al., 2023);

4) отсутствие прозрачности перевозочного процесса;

5) отсутствие «бесшовного» транспортного коридора для движения грузов и пассажиров (неразвитость мультимодальных транспортировок).

В то же время устойчивое развитие российской экономики (в частности, эффективное функционирование распределительных цепочек поставок и другие сегменты экономики) требует ускорения грузооборота при условии повышения безопасности транспортного процесса, качества выполняемых транспортных операций, обеспечения их надежности и прозрачности. Иными словами, необходимо создать интегрированную и бесперебойную мультимодальную систему устойчивой и интеллектуальной транспортной мобильности¹.

Для разрешения поставленных выше проблем на всех видах транспорта принимаются определенные шаги, связанные с увеличением автоматизированности отдельных транспортных операций, появлением цифровых сервисов для участников транспортного процесса, созданием интерфейсов, позволяющих реализовывать проекты по управлению парковками и стоянками, регулированием дорожного движения, автоматической идентификации транспортных средств и т. д. Происходящие изменения, затрагивающие все виды транспорта, требуют создания правовой основы, которая в настоящий момент формируется путем издания отдельных нормативных правовых актов. Приведем несколько примеров. Так, в авиационной отрасли принята Комплексная программа развития авиационной отрасли Российской Федерации до 2030 г.² В сфере морской деятельности утверждена Морская доктрина Российской Федерации³. В железнодорожной отрасли с сентября 2023 г. вступят в силу изменения по перевозке пассажиров, багажа, грузобагажа с использованием автоматизированных систем⁴.

Однако наибольшее количество изменений связано с правовой регламентацией автомобильных перевозок. Это обусловлено тем, что на основе проведенной в г. Женеве 25–29 марта 2019 г. 78-й сессии Глобального форума по безопасности дорожного движения была принята резолюция⁵, согласно которой в дорожное движение внедряются высоко- и полностью автоматизированные транспортные средства. Данный документ стал основой для дальнейшего развития правового регулирования применения автоматизированных транспортных средств в различных странах. Приведем несколько примеров. Так, в России была принята Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств

¹ Такая задача видится актуальной не только в рамках одного государства, но и на интернациональном уровне (решение Европейской комиссии от 3 декабря 2021 г. по учреждению Мультимодального форума мобильности пассажиров).

² Распоряжение Правительства Российской Федерации № 1693-р от 25.06.2022. (2022). *Собрание законодательства Российской Федерации*, 27, ст. 4877.

³ Указ Президента Российской Федерации № 512 от 31 июля 2022 г. (2022). *Собрание законодательства Российской Федерации*, 31, ст. 5699.

⁴ Приказ Министерства транспорта Российской Федерации № 352 от 5 сентября 2022 г. (2022). *Официальный интернет-портал правовой информации*. www.pravo.gov.ru, № 0001202210270033.

⁵ Доклад Глобального форума по безопасности дорожного движения о работе его Семьдесят восьмой сессии. <https://unece.org/DAM/trans/doc/2019/wp1/ECE-TRANS-WP1-167r.pdf>

на автомобильных дорогах общего пользования⁶ (далее – Концепция обеспечения безопасности дорожного движения). Кроме того, Правительством Российской Федерации были утверждены новые правила перевозки грузов автомобильным транспортом⁷, которые связаны с введением электронного документооборота при перевозке грузов на автомобильном транспорте.

В иностранных государствах также подобное развитие законодательства имеет место быть. Так, в Японии в 2018 г. была принята Дорожная карта публично-частной концепции интеллектуальных транспортных систем (Public-Private ITS Concept Roadmap 2018)⁸. 7 июня 2019 г. план был пересмотрен, но концептуальных изменений внесено не было (Public-Private ITS Concept Roadmap 2019)⁹.

Названные мероприятия – это серьезный шаг для создания и функционирования единой транспортной системы страны. Однако очевидно, что все вышеизложенное не представляется достаточным для реализации поставленной задачи. Обусловлено это тем, что предпринимаемые меры по цифровизации носят точечный характер. Такая локальность существует не только в техническом плане, но и в легальном. Обособленность технической составляющей заключается в том, что автоматизация осуществляется лишь в отдельных аспектах перевозочного процесса. Каждый сегмент функционирует изолированно, без требуемой взаимосвязи между собой. Кроме того, цифровизация транспортной отрасли осуществляется сепарированно по различным видам транспорта. С точки зрения правовой регламентации принимаемые нормативные правовые акты, направленные на регулирование транспортных отношений (в частности, применение интеллектуальных транспортных систем), имеют ярко выраженную проавтомобильную направленность. Отсутствие единого правового регулирования, устанавливающего единообразные правила в отношении всех видов транспорта¹⁰, является препятствием для создания указанной в Транспортной стратегии Российской Федерации до 2030 г. с прогнозом на период до 2035 г.¹¹ национальной интерактивной транспортной системы – основы для разрешения указанных выше проблем (Zhihan & Shang, 2022). Кроме того, локальность в правовом аспекте предполагает и отсутствие межгосударственного регулирования, а преобладание национального законодательства.

Сказанное выше свидетельствует о том, что в Российской Федерации еще не сформировано самой транспортной системы как целостной структуры, обеспечивающей одновременно транспортную доступность, мобильность, прозрачность,

⁶ Распоряжение Правительства Российской Федерации № 724-р от 25 марта 2020 г. (2020). *Собрание законодательства Российской Федерации*, 13, ст. 1995.

⁷ Постановление Правительства Российской Федерации № 2200 от 21 декабря 2020 г. (2020). *Собрание законодательства Российской Федерации*, 52 (ч. II), ст. 8877.

⁸ Public-Private ITS Concept Roadmap 2018. <https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20180615/siryou9.pdf>

⁹ Public-Private ITS Concept Roadmap 2019. <https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20190607/siryou9.pdf>

¹⁰ В данном случае возможны исключения из подхода о единообразии в правовом регулировании в силу технических особенностей конкретного вида транспорта и связанного с ними транспортного процесса.

¹¹ Распоряжение Правительства Российской Федерации № 3363-р от 27 ноября 2021 г. (2021). *Собрание законодательства Российской Федерации*, 50 (ч. IV), ст. 8613.

безопасность оказания транспортных услуг, а также единого правового регулирования транспортной системы. В условиях цифровизации такая разрозненность элементов транспортной системы становится еще более очевидной.

Таким образом, в транспортной отрасли назрела потребность в создании единого транспортного пространства, в котором осуществляется мультимодальное технологичное взаимодействие различных видов транспорта, участников транспортного процесса и инфраструктуры как в рамках одного государства, так и на межгосударственном уровне. Устойчивая и инклюзивная мобильность может быть обеспечена только путем повышения связанности и согласованности всех процессов, происходящих в рамках транспортной деятельности.

Появление сквозных цифровых технологий (искусственный интеллект, интернет вещей, облачные и туманные вычисления, робототехника, обработка больших объемов данных¹²) стало тем необходимым инструментом (Gromova & Ivanc, 2020), с помощью которого становится возможным разрешение поставленных задач в транспортной отрасли экономики. Применение цифровых технологий позволяет говорить о создании интеллектуальных транспортных систем, которые призваны обеспечить синхронизацию и координацию всех ее элементов, с одной стороны, а также интеграцию информационно-коммуникационных технологий в транспортный комплекс страны – с другой. Именно интеллектуальная транспортная система является потенциалом в развитии транспортной системы России. Такая важная роль интеллектуальных транспортных систем предопределена тем, что на основе сбора, обработки и анализа данных из всех источников информации формируется ценная информация, используемая для осуществления контроля и принятия управленческих решений на транспорте. В силу указанных характеристик интеллектуальные транспортные системы способны преодолеть вызовы, обозначенные в Стратегическом направлении в области цифровой трансформации транспортной отрасли Российской Федерации до 2030 г.¹³

Несмотря на всю значимость интеллектуальных транспортных систем, в настоящее время правовое регулирование их применения находится в режиме становления. Это обусловлено формированием сущностного наполнения понятия «интеллектуальные транспортные системы», выстраиванием структуры интеллектуальных транспортных систем.

1. Онтология понятия «интеллектуальные транспортные системы»

В основе выстраивания правового регулирования различных общественных отношений лежит понятийный аппарат (Бажина, 2022), синтагматической единицей (Фоменко, 1970) которого является понятие. Сущностное наполнение понятий предопределяет саму направленность правового регулирования. От четкости формулирования содержания понятий, выстраивания логических взаимосвязей между понятиями зависит эффективность правового регулирования. Именно поэтому первоочередным в изучении правового регулирования применения интеллектуальных транспортных систем видится установление содержания понятия «интеллектуальные транспортные системы».

¹² Пункт 36 Стратегии развития информационного общества в Российской Федерации, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

¹³ Распоряжение Правительства Российской Федерации № 3744-р от 21 декабря 2021 г. (2021). *Собрание законодательства Российской Федерации*, 1 (ч. IV), ст. 264.

В 1980–1990-е гг. в отдельных государствах получило развитие изучение вопросов координации транспортных потоков. В качестве примера можно назвать мюнхенский проект COMFORT, направленный на оптимизацию транспортного потока в центре города с учетом планирования сети автомагистралей в окрестных городах¹⁴.

В 1994 г. в Париже был впервые проведен международный конгресс, посвященный интеллектуальным транспортным системам, а именно интеллектуальным автомагистральным транспортным системам¹⁵. В 1995 г. местом проведения конгресса стал японский город Иокогама. Данное событие стало основополагающим для создания по инициативе пяти министерств проекта под названием «Большой план по развитию интеллектуальных транспортных систем». Именно поэтому местом происхождения интеллектуальных транспортных систем считается Япония.

В настоящее время во многих государствах мира ведутся разработки в этой сфере. В этой связи представляется важным определить сущностное содержание интеллектуальных транспортных систем.

В широком смысле интеллектуальная транспортная система понимается как система, обеспечивающая мобильность с помощью цифровых технологий. При этом в разных странах даются свои определения понятия «интеллектуальные транспортные системы», которые отличаются некоторыми особенностями. Примечательным является еще и то, что в некоторых документах дефиниции не содержатся, а акцентируется внимание на значимости интеллектуальных транспортных систем для транспортного сектора экономики.

Рассмотрим несколько подходов к определению понятия «интеллектуальные транспортные системы».

1. Сущностная составляющая понятия «Интеллектуальные транспортные системы» определяется путем указания на их прямое назначение.

Японское сообщество инженеров-автоматизаторов в специальном документе, который называется «Стандартизация интеллектуальных транспортных систем. Деятельность ИСО/ТС 204»¹⁶ (далее – Стандартизация ИТС, утвержденная Японским сообществом инженеров-автоматизаторов) указывает на то, что интеллектуальные транспортные системы созданы специально для быстрого повышения безопасности дорожного движения, эффективности и комфорта перевозок, обеспечения энергосбережения и охраны окружающей среды (Hasegawa, 2013).

2. Интеллектуальная транспортная система понимается как система транспорта.

В Дорожной карте ЕЭК ООН по интеллектуальным транспортным системам на 2021–2025 гг., изданной Европейской экономической комиссией ООН в декабре 2020 г.¹⁷ (далее – Дорожная карта ООН по интеллектуальным транспортным системам), интеллектуальная транспортная система понимается как система внутреннего

¹⁴ Жанказиева С. В., Воробьева Т. В. (17 июля, 2013). Мировой опыт становления и развития региональных ИТС. Вестник ГЛОНАСС. http://vestnik-glonass.ru/stati/mirovoy_opyt_stanovleniya_i_razvitiya_regionalnykh_its/

¹⁵ European Commission. (1995). "Towards an intelligent transport system". Community Research and Development Information Service.

¹⁶ https://www.jsae.or.jp/01info/org/its/its_2019_en.pdf

¹⁷ Проект пересмотренной «дорожной карты» ЕЭК ООН по интеллектуальным транспортным системам. ЕЭК ООН. <https://unece.org/sites/default/files/2021-01/ECE-TRANS-2021-15r.pdf>

транспорта, к которой в целях мобильности применяются информационно-коммуникационные технологии (далее – ИКТ).

3. Интеллектуальные транспортные системы – это совокупность приложений или технологий. Такой подход содержится в Преамбуле Директивы Европейского парламента и Совета № 2010/40/ЕС от 7 июля 2010 г. «О рамках развертывания интеллектуальных транспортных систем в области автомобильного транспорта и для интерфейсов с другими видами транспорта»¹⁸ (далее – Директива ЕС 2010 г.). Данные приложения направлены на обеспечение предоставления инновационных услуг, связанных с различными видами транспорта. С их помощью различные пользователи могут получать более полную информацию о состоянии транспортных сетей. Тем самым использование транспортных сетей становится более безопасным, скоординированным и «разумным». В законодательстве Канады интеллектуальная транспортная система определяется как передовая и новейшая технология (в том числе с использованием компьютеров, датчиков, систем управления, связи и электронных устройств) на транспорте для спасения жизней, экономии времени, денег, сохранения энергии и окружающей среды¹⁹.

В Стандартах Международной организации по стандартизации ISO/TS14812:2022 *Intelligent transport systems – Vocabulary* в п. 3.1.2.4 дефиниция интеллектуальных транспортных систем дается через перечисление составляющих их элементов. К таковым относятся различного рода технологии, а именно: информационные, коммуникационные, сенсорные, контрольные технологии, предназначенные для использования в интересах наземной транспортной системы.

4. Интеллектуальная транспортная система понимается как система управления транспортным комплексом. Такой подход лежит в основе регламентации интеллектуальных транспортных систем в России. Понятие «интеллектуальные транспортные системы» дано в одноименном отечественном национальном стандарте, под которым понимается «система управления, интегрирующая современные информационные и телематические технологии и предназначенная для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортно-дорожным комплексом региона, конкретным транспортным средством или группой транспортных средств с целью обеспечения заданной мобильности населения, максимизации показателей использования дорожной сети, повышения безопасности и эффективности транспортного процесса, комфортности для водителей и пользователей транспорта»²⁰.

Данное понятие полностью повторяется в нескольких нормативных правовых актах, а именно: в Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования²¹, а также в общих положениях Концепции создания и функциониро-

¹⁸ European Parliament. <https://www.europarl.europa.eu/legislative-train/theme-resilient-energy-union-with-a-climate-change-policy/file-electronic-freight-transport-information>

¹⁹ ITS Canada. <https://www.itscanada.ca/about>

²⁰ ГОСТ Р 56829-2015 «Национальный стандарт Российской Федерации. Интеллектуальные транспортные системы. Термины и определения». <https://docs.cntd.ru/document/1200128315?section=text>

²¹ Распоряжение Правительства Российской Федерации № 724-р от 25 марта 2020 г. (2020). *Собрание законодательства Российской Федерации*, 13, ст. 1995.

вания национальной сети интеллектуальных транспортных систем на автомобильных дорогах общего пользования²² (далее – Концепция создания интеллектуальных транспортных систем).

В научной литературе также поддерживается указанная выше концепция в отношении сущности интеллектуальных транспортных систем. Интеллектуальная транспортная система – это интеграция управления, информационных и коммуникационных технологий с транспортной инфраструктурой (Sladkowski & Pamula, 2016).

Представленные концепции иллюстрируют общую картину развития правового регулирования в отношении интеллектуальных транспортных систем. Как справедливо отмечено в дорожной карте ЕЭК ООН по интеллектуальным транспортным системам, ввиду различий в экономических приоритетах каждое государство может по-своему трактовать содержание понятия «интеллектуальные транспортные системы»²³. С точки зрения правовой регламентации применения интеллектуальных транспортных систем такие разночтения могут стать причиной «путаницы на межгосударственном уровне»²⁴. Сказанное видится своего рода препятствием для глобального внедрения и применения интеллектуальных транспортных систем. Соответственно, важным шагом на пути преодоления указанных выше сложностей может стать разработка общих, межгосударственных руководящих принципов и правил, позволяющих определить порядок технической и технологической совместимости интеллектуальных транспортных систем, применяемых в каждом государстве.

Представленные определения в той или иной степени имеют определенные общие черты, которые можно выделить.

Во-первых, интеллектуальные транспортные системы являются основой современной транспортной системы.

Во-вторых, интеллектуальные транспортные системы имеют прямую связь с цифровыми технологиями, с помощью которых они функционируют.

В-третьих, основная задача применения интеллектуальных транспортных систем заключается в автоматизации транспортных операций с целью создания конкурентоспособной транспортной системы.

Однако ни один из указанных детерминистских подходов не является комплексным. Связано это с тем, что элементы интеллектуальной транспортной системы в полной мере не рассмотрены ни в одной из представленных дефиниций. При этом структурные элементы имеют важное значение для определения сущностного наполнения понятия, а также для выстраивания логических связей с другими понятиями и тем самым формированием понятийного аппарата, лежащего в основе любого правового регулирования. Именно этот аспект послужил основанием для рассмотрения архитектуры (структуры) интеллектуальных транспортных систем.

²² Распоряжение Минтранса России № АК-247-р от 30.09.2022. (2022). *Транспорт России*, 49, 05.12.2022–11.12.2022.

²³ Ход осуществления дорожной карты ЕЭК по интеллектуальным транспортным системам. Европейская экономическая комиссия ООН. https://unece.org/sites/default/files/2023-01/ECE_TRANS_2023_19_Rev1R.docx

²⁴ Там же.

2. Архитектура (структура) интеллектуальных транспортных систем

При раскрытии вопроса архитектуры интеллектуальных транспортных систем следует указать на несколько концептуальных моментов.

Во-первых, рассмотрение вопроса об архитектуре интеллектуальных транспортных систем представляется стратегически важным для отображения сущности интеллектуальных транспортных систем, их определенного предназначения в эволюции транспортной деятельности. Именно через архитектуру интеллектуальных транспортных систем происходит интеграция в саму идею создания интеллектуальных транспортных систем, определения ее эмерджентности. Выстраивание архитектуры интеллектуальных транспортных систем является ключевым для разработки адекватного правового регулирования применения интеллектуальных транспортных систем.

Во-вторых, в настоящее время архитектура интеллектуальных транспортных систем разрабатывается применительно к дорожной транспортной сети. Остальные компоненты транспортной системы (иные виды транспорта) в документах, посвященных автомобильному транспорту, не учитываются. Именно этим обусловлены выделяемые элементы архитектуры интеллектуальных транспортных систем.

Во многих документах, в том числе и нормативных правовых актах, используется понятие «архитектура интеллектуальных транспортных систем». Согласно отечественному предварительному национальному стандарту по интеллектуальным транспортным системам, под «архитектурой понимаются фундаментальные концепции или свойства системы в ее среде, воплощенные в элементах, отношениях и структуре»²⁵. Иными словами, понятие «архитектура» означает определенную структуру, формирующую интеллектуальную транспортную систему как систему, состоящую из различных элементов. Оно используется с целью подчеркнуть сложность и многофункциональность интеллектуальных транспортных систем.

В разных источниках, как нормативных, так и научных, эти составные части называются по-разному, а именно: уровни, подсистемы и т. д. При этом основания для выделения таких элементов различаются.

В Концепции создания интеллектуальных транспортных систем указано, что их архитектура должна состоять из определенных уровней, а именно: интеграционной платформы, комплексной подсистемы, инструментальной подсистемы, периферийного оборудования, телекоммуникационной инфраструктуры, решений (в том числе аппаратно-программных) в части информационной безопасности и отказоустойчивости.

Иной подход в отношении определения уровней указан в книге, посвященной интеллектуальным транспортным системам в дорожном движении, изданной Радиокommunikationным бюро (Швейцария)²⁶. Критерием выделения уровней в комплексе интеллектуальных транспортных систем в данном документе выступают их пользователи, которые делятся на три группы. Первая группа пользователей – это дорожный оператор, т. е. организация, которая управляет дорогами для достижения мест-

²⁵ ПНСТ РФ 636-2022 «Интеллектуальные транспортные системы. Коммерческие перевозки. Контроль автомобильных перевозок в цепочке поставок. Часть 1. Архитектура и определения данных». (2022). Москва: ФГБУ «РСТ».

²⁶ *Intelligent transport systems: Handbook on Land Mobile (including Wireless Access)* (Vol. 4. 2021 edition). https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-49-2021-PDF-E.pdf

ных целей, как правило, для поддержания транспортного потока и реагирования на дорожные инциденты. Дорожный оператор контролирует дорожную ситуацию и предоставляет информацию участникам дорожного движения. Дорожный оператор играет значительную роль в осуществлении различных сервисов интеллектуальных транспортных систем. Исключением являются системы обеспечения безопасности между транспортными средствами. Вторая группа пользователей состоит из водителей транспортных средств. Эта группа является конечным пользователем многих сервисов интеллектуальных транспортных систем и косвенным поставщиком большого количества данных о дорожных характеристиках (либо через дистанционное зондирование, либо с помощью сбора информации транспортным средством и предоставления третьей стороне). Третья группа пользователей – это путешественники или пешеходы, которые используют интеллектуальные транспортные системы для получения информации о дорожной обстановке, планирования поездок, использования транзитных услуг или запроса экстренной помощи.

Согласно определению «интеллектуальные транспортные системы»²⁷ подразделения Министерства транспорта США (Research and Innovative Technology Administration, RITA)²⁸, она состоит из 26 типов систем, основанных на технологиях. Эти системы могут быть разделены на две большие категории: умная инфраструктура и умные транспортные средства.

Также есть точка зрения, что интеллектуальные транспортные системы состоят из следующих элементов: системы управления дорожными сигналами, системы управления дорожным движением, системы управления автомагистралями, системы управления транзитом, системы управления дорожными происшествиями, услуг по информированию путешественников, услуг аварийного управления, расширенная аналитика дорожного движения, системы электронной оплаты проезда, системы управления общественным транспортом, инфраструктуры подключенных автомобилей, мониторинга производительности дорожной сети, систем безопасности на железнодорожных переездах, систем управления коммерческим транспортом (Abduljabbar et al, 2019).

Схожей с предыдущей является концепция, согласно которой интеллектуальные транспортные системы включают в себя умную систему публичного транспорта, умную систему дорожной инфраструктуры, умную систему управления парковками, умную систему дорожного управления и контроля, управления безопасностью и чрезвычайными ситуациями, умными системами управления тротуарами (Lakshmi Shankar Iyer, 2021).

Иерархический анализ интеллектуальных транспортных систем свидетельствует об отсутствии единого подхода по выделению компонентов интеллектуальных транспортных систем. Соответственно, те компоненты, которые указаны в системе, отличаются друг от друга в зависимости от оснований их выделения. Данная особенность предопределяет формирование правового регулирования применения интеллектуальных транспортных систем.

²⁷ Intelligent Transportation Systems Joint Program Office. Strategic Plan 2020–2025. www.ITS.DOT.GOV/STRATPLAN2020

²⁸ Данное подразделение Минтранса США создано в 2005 г. с целью совершенствования координации транспортных исследований, развития транспортной науки, технологий и анализа.

3. Перспективы развития правового регулирования применения интеллектуальных транспортных систем

Проведенный выше анализ сущностного наполнения понятия «интеллектуальные транспортные системы», иерархической структуры интеллектуальных транспортных систем позволяет сделать некоторые выводы о развитии правового регулирования применения интеллектуальных транспортных систем. Рассмотрим их более детально.

1. Сложившаяся в настоящее время тенденция по формированию национального законодательства в отношении применения интеллектуальных транспортных систем не в полной мере отражает потребности современной экономики. Связано это с тем, что развитие всех сфер деятельности ориентировано на интернациональный обмен различными благами. Кроме того, развитие интеллектуальных транспортных систем свидетельствует о возникновении межнациональных вопросов, связанных с обеспечением кибербезопасности. Тем самым информационно-коммуникационные технологии как бы размывают существующие территориальные границы между государствами, и возникает угроза цифровой безопасности государства (Кутюр, Тоупин, 2020). Решение указанных проблем на замкнутом национальном уровне не может быть эффективным. Требуется межгосударственный подход к разработке правового регулирования применения интеллектуальных транспортных систем.

2. Выделение указанных элементов как компонентов целостного образования ориентировано только на автомобильный транспорт. Это обстоятельство не соответствует концептуальному подходу, представленному в программных документах, посвященных реформированию транспортной отрасли. Мобильность в транспортной сфере означает не только возможность бесшовного движения грузов из одного пункта в другой (в том числе с использованием разных видов транспорта), но и создание прозрачности всего транспортного процесса (в том числе и документооборота).

3. Иерархия интеллектуальной транспортной системы предопределяет направления развития правового регулирования в транспортной сфере. Представленные выше подходы по выделению структурных компонентов интеллектуальной транспортной системы выстроены исходя из задач, стоящих перед транспортной отраслью экономики. К ним можно отнести: управление транспортом, обеспечение безопасности, наличие «умных» транспортных средств и транспортной инфраструктуры. Правовое регулирование этих направлений в настоящее время несовершенно (Землин, 2022). Оно носит фрагментарный характер, что не позволяет выстроить системный подход в правовом регулировании. Приведем несколько примеров. Рассмотрим такую сферу, как управление в сфере транспорта.

Управление в сфере транспорта является ключевым в силу того, что именно через управление реализуется «процесс упорядоченного воздействия субъекта на объект» (Харитонов, 2011). Не вдаваясь в изучение подходов по исследованию категории «управление» (Ананьева, 2015), следует указать на то, что в транспортной отрасли управление понимается в нескольких значениях. С одной стороны, государство осуществляет управление различными транспортными процессами посредством внедрения цифровых технологий (например, применение технологий искусственного интеллекта²⁹). Тем самым между государством в лице его органов и субъектами

²⁹ Паспорт Стратегии цифровой трансформации транспортной отрасли Российской Федерации. СПС «КонсультантПлюс».

транспортной деятельности возникают публичные отношения по соблюдению установленных правил и требований. С другой стороны, управление в сфере транспорта осуществляется и самими субъектами транспортной деятельности. Оно возникает в гражданско-правовых отношениях при оказании субъектами транспортной деятельности транспортных услуг своим клиентам. В качестве примера можно привести отношения по обслуживанию высокоавтоматизированных транспортных средств, в том числе и осуществление контроля за выполнением таким транспортным средством функции движения. Наиболее подходящей фигурой является оператор. Однако в подготовленном законопроекте и в некоторых положениях действующего законодательства, посвященных правовому регулированию применения высокоавтоматизированных транспортных средств, оператор рассматривается как физическое лицо, которое осуществляет определенные действия.

Так, в проекте закона «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации»³⁰ вводится понятие «оператор высокоавтоматизированного транспортного средства», под которым понимается физическое лицо, находящееся вне высокоавтоматизированного транспортного средства, осуществляющее мониторинг за его движением посредством удаленного доступа, имеющее возможность дистанционного вмешательства в стратегическое управление высокоавтоматизированным транспортным средством, а также обладающее знаниями по дистанционному вмешательству в функционирование указанных транспортных средств. В Постановлении Правительства Российской Федерации от 29 декабря 2022 г. № 2495 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по предоставлению транспортных услуг с использованием высокоавтоматизированных транспортных средств на территориях отдельных субъектов Российской Федерации»³¹ используется понятие «оператор», которым выступает физическое лицо, не являющееся водителем-испытателем и находящееся вне высокоавтоматизированного транспортного средства 2-й категории, осуществляющее маршрутизацию и диспетчеризацию высокоавтоматизированного транспортного средства 2-й категории (определение и изменение маршрута движения, активацию и деактивацию).

В представленных выдержках закона оператор не является субъектом транспортной деятельности. Исходя из анализа норм, можно предположить, что его статус в большей степени схож со статусом подрядчика – физического лица в гражданско-правовом договоре подряда или работника в трудовых отношениях, когда у физического лица фиксируется трудовая функция в виде определенного перечня действий или бездействий.

Такой подход видится фрагментарным, не подходящим с точки зрения иерархии интеллектуальной транспортной системы, где управление является ключевым элементом для функционирования всей интеллектуальной транспортной системы. Думается, что такая деятельность должна быть лицензируемой и подконтрольна государству с целью возможности регулирования.

³⁰ Проект федерального закона «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» от 8 июня 2021 г. № 02/04/06-21/00116763. <http://regulation.gov.ru/p/116763>

³¹ Постановление Правительства Российской Федерации № 2495 от 29 декабря 2022 г. (2022). *Собрание законодательства Российской Федерации*, 1 (ч. II), ст. 300.

Учитывая уже существующий опыт закрепления такого рода фигур в действующем законодательстве, посвященном цифровизации, можно провести аналогию с оператором информационной системы (статья 5 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»³²), а также с оператором инвестиционной платформы (гл. 2 Федерального закона от 2 августа 2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ о внесении изменений в отдельные законодательные акты Российской Федерации»³³).

Другим примером точечного правового регулирования является разработка законодательства об «умных» транспортных средствах как одном из элементов интеллектуальной транспортной системы. Под «умным» транспортным средством следует понимать высокоавтоматизированное или полностью автоматизированное транспортное средство. Здесь представляется важным указать на терминологическую путаницу, связанную с отсутствием признаваемого в научном сообществе, в национальном и межнациональном законодательствах единого понятия, обозначающего транспортное средство, управление которым осуществляется им самим с помощью автоматизированной системы вождения, встроенной в транспортное средство.

Так, в Концепции безопасности дорожного движения есть некий терминологический парадокс. С одной стороны, в названии документа используется понятие «беспилотное транспортное средство». С другой – в данном акте указывается на приоритет применения понятий «высокоавтоматизированное транспортное средство», «полностью автоматизированное транспортное средство». Эти понятия также были рекомендованы Резолюцией Глобального форума по безопасности дорожного движения. В ином акте – Программе экспериментального правового режима по применению высокоавтоматизированных транспортных средств – используется только понятие «высокоавтоматизированное транспортное средство». При этом эти высокоавтоматизированные транспортные средства подразделяются на две категории.

В связи с тем, что на легальном уровне нет терминологической четкости, в научной литературе также используются разные понятия. Каждый автор обозначает рассматриваемые объекты с помощью того термина, который представляется наиболее верным с его точки зрения. Так, ряд авторов используют понятие «беспилотное транспортное средство» (Ананенко, 2020; Бегишев, 2021; Коробеев, Чучаев 2019; Степанян, 2019; Begishev, Bersei, Sherbakova et al., 2022). Другие авторы считают более правильным термин «высокоавтоматизированное транспортное средство» (Юдкина, 2022, Евстигнеев, 2019; Takeyoshi, 2019; Begishev, Bersei, Amvrosova et al., 2022).

Каждая из представленных точек зрения по наименованию такого рода умных транспортных средств представляется заслуживающей внимания. Однако для того, чтобы избежать в будущем разночтений в правовом регулировании, необходимо выработать единый подход к наименованию такого рода транспортных средств. В этой связи думается правильным обратить внимание на следующее.

³² Федеральный закон № 259-ФЗ от 31 июля 2020 г. (2020). *Собрание законодательства Российской Федерации*, 31 (ч. I), ст. 5018.

³³ Федеральный закон № 259-ФЗ от 2 августа 2019 г. (2019). *Собрание законодательства Российской Федерации*, 31, ст. 4418.

Во-первых, понятие «беспилотный» в различных актах используется для обозначения такого транспортного средства, которое может управлять движением без присутствия внутри него человека. В большей степени это понятие используется в актах, посвященных воздушному транспорту. Так, в ГОСТ Р 56122-2014 «Национальный стандарт Российской Федерации. Воздушный транспорт. Беспилотные авиационные системы. Общие требования»³⁴ и в Регламенте № 428/2009 Совета Европейского союза³⁵ применяется термин «беспилотный летательный аппарат». В пункте 5 ст. 32 Воздушного кодекса Российской Федерации³⁶ под беспилотным транспортным воздушным судном понимается судно, которым управляет или которое контролирует внешний пилот, т. е. лицо, находящееся вне борта самого этого судна.

Таким образом, термин «беспилотный» означает лишь то, что самого лица, осуществляющего управление, в транспортном средстве нет (Sipetas et al, 2023; O'Hern & St. Louis, 2023).

Во-вторых, понятие «автоматизированное транспортное средство» в нормативном правовом регулировании, в том числе и в международном, используется в отношении дорожного транспорта. Так, в разработанной Обществом автомобильных инженеров (Society of automotive engineers – SAE) классификации уровней автоматизации³⁷ (далее – Классификация SAE) в объем понятия «автоматизированное транспортное средство» входят те транспортные средства, которые в соответствии с Классификацией SAE относятся к уровням 3–5:

- уровень 3 – условно автоматизированное (Conditional automation), т. е. управление транспортным средством требует наличия водителя, который хотя и не всегда может следить за дорожной обстановкой, должен быть готов в любой момент принять управление транспортным средством на себя;

- уровень 4 – высокоавтоматизированное (High automation), т. е. транспортное средство оснащено всем необходимым, чтобы осуществлять движение без участия водителя при определенных условиях;

- уровень 5 – полностью автоматизированное (Full automation), т. е. наличия водителя для осуществления управления транспортным средством не требуется (Schubert, 2015).

Кроме того, в других национальных системах также используется понятие «высокоавтоматизированное транспортное средство» и «полностью автоматизированное транспортное средство». Так, в Германии в законе, посвященном регулированию дорожных перевозок (Straßenverkehrsgesetz (StVG)), одна из первых статей (пар. 1a) называется “Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion”, что в переводе означает «транспортное средство с высоко- или полностью автоматизированной функцией управления»³⁸.

³⁴ ГОСТ Р 56122-2014 «Национальный стандарт Российской Федерации. Воздушный транспорт. Беспилотные авиационные системы. Общие требования». Москва: Стандартинформ, 2020.

³⁵ Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428>

³⁶ Воздушный кодекс Российской Федерации № 60-ФЗ от 19 марта 1997 г. (1997). Собрание законодательства Российской Федерации, 12, ст. 1383.

³⁷ Automated Vehicles for Safety. <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>

³⁸ <https://www.gesetze-im-internet.de>

Представленные выводы свидетельствуют об отсутствии единого подхода в наименовании новых объектов реального мира и определении их сущностных характеристик, а также системного подхода в разработке правового регулирования, общего для всех видов транспорта с учетом требований современного транспортного процесса.

Выводы

Представленная работа является начальным этапом развития правовых исследований в сфере применения интеллектуальных транспортных систем. Исходя из изложенного выше, можно сделать следующие выводы.

1. Формирование правового регулирования применения интеллектуальных транспортных систем носит фрагментарный характер. Это связано с тем, что нормативное регулирование создается обособленно по различным видам транспорта как на национальном уровне, так и на международном. Кроме того, создание нормативного регулирования в большей степени носит замкнутый национальный характер.

2. В настоящее время нет четкой детерминации сущностного наполнения понятия «интеллектуальные транспортные системы». Таким образом, требуется совершенствование нормативного понятия «интеллектуальные транспортные системы». Такая необходимость обусловлена тем, что в основе любого правового регулирования лежит понятийный аппарат, состоящий из согласованных, взаимосвязанных друг с другом понятий.

3. Структурные элементы, образующие архитектуру интеллектуальных транспортных систем, имеют важное значение для выстраивания взаимосвязей внутри системы. При этом сама архитектура интеллектуальных транспортных систем не является «закостенелой», а трансформируется в связи с изменением отдельных ее элементов под влиянием цифровых технологий.

Список литературы

- Ананенко, А. О. (2020). Основные направления совершенствования гражданско-правового законодательства в области регулирования беспилотных транспортных средств. *Транспортное право и безопасность*, 2(34), 76–83. <https://elibrary.ru/zxiivh>
- Ананьева, А. А. (2015). Система нормативных юридических конструкций гражданско-правовых договоров оперативного управления транспортной деятельностью. Саратов: Издательский центр «Наука». <https://elibrary.ru/zxiivh/uruyjt>
- Бажина, М. А. (2022). De lege ferende система понятийного аппарата транспортного права. *Транспортное право*, 4, 34–39. EDN: <https://elibrary.ru/jxkuko>. DOI: <https://doi.org/10.18572/1812-3937-2022-4-34-39>
- Бегишев, И. Р. (2021). Правовое регулирование беспилотных транспортных средств. *Транспортное право*, 3, 7–10. EDN: <https://elibrary.ru/bffk kj>. DOI: <https://doi.org/10.18572/1812-3937-2021-3-7-10>
- Евстигнеев, И. А. (2019). Дорожная инфраструктура и высокоавтоматизированные транспортные средства. *САПР и ГИС автомобильных дорог*, 2(13), 44–50. EDN: <https://elibrary.ru/elxrzr>. DOI: <https://doi.org/10.17273/CADGIS.2019.2.7>
- Землин, А. И. (2022). Проблемные вопросы правового регулирования отношений, связанных с использованием высокоавтоматизированных транспортных средств. *Журнал российского права*, 12. EDN: <https://elibrary.ru/bsmkwa>. DOI: <https://doi.org/10.12737/jrl.2022.128>
- Коробеев, А. И., Чучаев, А. И. (2019). Беспилотные транспортные средства: новые вызовы общественной безопасности. *Lex Russica (Русский закон)*, 2(147), 9–28. EDN: <https://elibrary.ru/swhgup>. DOI: <https://doi.org/10.17803/1729-5920.2019.147.2.009-028>
- Кутюр, С., Тоупин, С. (2020). Что означает «суверенитет» в цифровом мире? *Вестник международных организаций: образование, наука, новая экономика*, 15(4), 7. EDN: <https://elibrary.ru/zcvyrh>. DOI: <https://doi.org/10.17323/1996-7845-2020-04-03>

- Степанян, А. Ж. (2019). Проблемы регулирования беспилотных транспортных средств. *Вестник Университета имени О. Е. Кутафина*, 4(56), 169–174. EDN: <https://elibrary.ru/qkxcsc>. DOI: <https://doi.org/10.17803/2311-5998.2019.56.4.169-174>
- Харитонов, Ю. С. (2011). *Управление в гражданском праве: проблемы теории и практики*. Москва: Норма.
- Фоменко, Ю. В. (1970). Является ли словосочетание единицей языка. *Филологические науки*, 5, 60–65. <https://elibrary.ru/xnfdfb>
- Юдкина, В. В. (2022). Высокоавтоматизированные транспортные средства как субъект общественной безопасности. *Административное право и процесс*, 10. EDN: <https://elibrary.ru/xhbcrb>. DOI: <https://doi.org/10.18572/2071-1166-2022-10-49-53>
- Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. *Sustainability*, 11 (1), 189. <https://doi.org/10.3390/su11010189>
- Bagreeva, E. G., Zemlin, A. I., & Shamsunov, S. K. (2019). Does Environmental safety Depend Upon the Legal Culture of Transport Specialists? *Ekoloji*, 28(107). <https://elibrary.ru/isipid>
- Begishev, I., Bersei, D., Amvrosova, O., Dolgoplov, K., & Zhiron, R. (2022). Regulation of highly automated vehicles in the Russian Federation: problems, state and development prospects. In *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 648–655). <https://doi.org/10.1016/j.trpro.2022.06.058>
- Begishev, I., Bersei, D., Sherbakova, L. et al. (2022). Problems of legal regulation of unmanned vehicles. *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 1321–1327). <https://doi.org/10.1016/j.trpro.2022.06.142>
- Du, Y-L., Yi, T-H., Li, X-J., Rong, X-L, Dong, L-J., Wang, D-W., Gao, Y. & Leng, Z. (2023). *Advances in Intellectualization of Transportation Infrastructures. Engineering*. <https://doi.org/10.1016/j.eng.2023.01.011>
- Gromova, E., & Ivanc, T. (2020). Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS. *BRICS LAW Journal*, 7(2), 10–36. <https://doi.org/10.21684/2412-2343-2020-7-2-10-36>
- Hasegawa, Takaaki. (2013). A Design Theory for New Transportation System. *IATSS Review*, 37(3), 224–232.
- Lakshmi Shankar Iyer. (2021). AI enabled applications towards intelligent transportation. *Transportation Engineering*, 5. <https://doi.org/10.1016/j.treng.2021.100083>
- O'Hern, S., & St. Louis, R. (2023, February 8). Technology readiness and intentions to use conditionally automated vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour*, 1–8. <https://doi.org/10.1016/j.trf.2023.02.001>
- Schubert, M. (2015). *Autonomous Cars – Initial Thoughts About Reforming the Liability Regime*. Phi., 46–51.
- Sipetas, Ch., Roncoli, C., & Mladenovich, M. (2023). Mixed fleets of automated and human-driven vehicles in public transport systems: An evaluation of feeder line services. *Transportation Research Interdisciplinary Tendency*, 18, 100791. <https://doi.org/10.1016/j.trip.2023.100791>
- Sladkowski, A., & Pamula, W. (2016). *Intelligent transport systems – problems and perspectives* (Vol. 32). Springer, Switzerland.
- Takeyoshi, Imai. (2019). Legal regulation of autonomous driving technology: Current conditions and issues in Japan. *IATSS Research*, 43(4), 263–267. <https://doi.org/10.1016/j.iatssr.2019.11.009>
- Zhihan, Lv., & Wenlong, Shang. (2023). Impacts of intelligent transportation systems of energy conservation and emission reduction of transport systems: a comprehensive review. *Green Technologies and Sustainability*, 1(1) <https://doi.org/10.1016/j.grets.2022.100002>

Сведения об авторе



Бажина Мария Анатольевна – доктор юридических наук, доцент, доцент кафедры предпринимательского права, Уральский государственный юридический университет имени В. Ф. Яковлева

Адрес: 620137, Российская Федерация, г. Екатеринбург, ул. Комсомольская, д. 21

E-mail: mashsol@mail.ru

ORCID ID: <https://orcid.org/0000-0003-1237-0052>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57807831200>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/32495219>

Google Scholar ID: <https://scholar.google.ru/citations?user=m5W9vIYAAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=974423

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.23.51 / Правовое регулирование отдельных отраслей экономики

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 29 апреля 2023 г.

Дата одобрения после рецензирования – 30 мая 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.27>

Intelligent Transport Systems as the Basis of de Lege Ferenda of the Transport System of the Russian Federation

Maria A. Bazhina

V. F. Yakovlev Ural State Law University
Yekaterinburg, Russian Federation

Keywords

Artificial intelligence,
digital technologies,
highly automated vehicle,
intelligent transport system,
law,
legal regulation,
Safety,
transport infrastructure,
transport legislation,
unmanned vehicle

Abstract

Objective: to research the trends of legal regulation of using intelligent transport systems under digital transformation of the transport sector of economy, namely, the growing importance of intelligent transport systems in the future transport system of the Russian Federation.

Methods: systemic-structural method is the basis for researching intelligent transport systems. It enables to study the architecture of intelligent transport systems as a complex structural unity. Also, comparative-legal method was used, aimed at illustrating the differences and similarities in the legal regulation of intelligent transport systems. Methods of legal modeling and forecasting, as well as formal-logic method, served as secondary methods to comprehensively study the legal regulation of intelligent transport systems.

Results: the article presents conceptual approaches to defining the notion of “intelligent transport systems” and outlining the hierarchy of intelligent transport systems, which play a fundamental role in building the transport sector. Based on the analysis, conclusions are made about the vectors of forming transport legislation, aimed at regulating the use of intelligent transport systems.

Scientific novelty: the article provides a conceptual approach to forming the legal regulation of intelligent transport systems. To this end, the issue is considered about the essential content of the notion

© Bazhina M. A., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

of “intelligent transport systems” at legal and scientific levels; the current terminological problems in building the legal regulation are shown. Analysis of the architecture of intelligent transport systems allowed for the first time to formulate the basic approaches to shaping the legal regulation of its individual elements (including highly automated and fully automated transport means, “smart” infrastructure, etc.) not in isolation but as constituent parts of the whole matter.

Practical significance: the presented materials and conclusions facilitate the development of legal regulation of transport industry under digital transformation. The article accentuates the legal regulation of intelligent transport systems taking into account their technical and technological features. It is the intelligent transport systems that are *de lege ferenda* of the transport system, which determines the vector of transformation of transport legislation. In turn, development of the legal bases allows broadening the geography of introducing technical novelties and making their application much more large-scale.

For citation

Bazhina, M. A. (2023). Intelligent Transport Systems as the Basis of *de Lege Ferenda* of the Transport System of the Russian Federation. *Journal of Digital Technologies and Law*, 1(3), 629–649. <https://doi.org/10.21202/jdtl.2023.27>

References

- Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. *Sustainability*, 11 (1), 189. <https://doi.org/10.3390/su11010189>
- Ananenko, A. O. (2020). Key directions of improving civil-legal legislation in the sphere of unmanned vehicles regulation. *Transportnoye pravo i bezopasnost*, 2(34), 76–83.
- Ananyeva, A. A. (2015). *System of normative legal constructions of civil-legal contracts of operative management in transport activity*. Saratov: Izdatelskiy tsentr “Nauka”.
- Bagreeva, E. G., Zemlin, A. I., & Shamsunov, S. K. (2019). Does Environmental safety Depend Upon the Legal Culture of Transport Specialists? *Ekoloji*, 28(107).
- Bazhina, M. A. (2022). *De lege ferende system of conceptual apparatus of transport law*. *Transportnoye pravo*, 4, 34–39. <https://doi.org/10.18572/1812-3937-2022-4-34-39>
- Begishev, I. R. (2021). Legal regulation of unmanned vehicles. *Transportnoye pravo*, 3, 7–10. <https://doi.org/10.18572/1812-3937-2021-3-7-10>
- Begishev, I., Bersei, D., Amvrosova, O., Dolgoplov, K., & Zhiron, R. (2022). Regulation of highly automated vehicles in the Russian Federation: problems, state and development prospects. In *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 648–655). <https://doi.org/10.1016/j.trpro.2022.06.058>
- Begishev, I., Bersei, D., Sherbakova, L. et al. (2022). Problems of legal regulation of unmanned vehicles. In *X International Scientific Siberian Transport Forum. TransSiberia* (pp. 1321–1327). <https://doi.org/10.1016/j.trpro.2022.06.142>
- Du, Y-L., Yi, T-H., Li, X-J., Rong, X-L, Dong, L-J., Wang, D-W., Gao, Y., & Leng, Z. (2023). *Advances in Intelligentization of Transportation Infrastructures. Engineering*. <https://doi.org/10.1016/j.eng.2023.01.011>
- Evstigneev, I. A. (2019). Road infrastructure and highly automated vehicles. *SAPR i GIS avtomobilnykh dorog*, 2(13), 44–50. <https://doi.org/10.17273/CADGIS.2019.2.7>
- Fomenko, Yu. V. (1970). Is a word combination a language unit? *Filologicheskiye nauki*, 5, 60–65.
- Gromova, E., & Ivanc, T. (2020). Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS. *BRICS LAW Journal*, 7(2), 10–36. <https://doi.org/10.21684/2412-2343-2020-7-2-10-36>

- Hasegawa, Takaaki. (2013). A Design Theory for New Transportation System. *IATSS Review*, 37(3), 224–232.
- Kharitonova, Yu. S. (2011). *Management in civil law: problems of theory and practice*. Moscow: Norma.
- Korobeev, A. I., & Chuchaev, A. I. (2019). Unmanned vehicles: new challenges to public safety. *LexRussica (Russkiy zakon)*, 2(147), 9–28. <https://doi.org/10.17803/1729-5920.2019.147.2.009-028>
- Kutyur, S., & Toupin, S. (2020). What does “sovereignty” mean in the digital world? *Vestnik mezhdunarodnykh organizatsiy: obrazovaniye, nauka, novaya ekonomika*, 15(4), 7. <https://doi.org/10.17323/1996-7845-2020-04-03>
- Lakshmi Shankar Iyer. (2021). AI enabled applications towards intelligent transportation. *Transportation Engineering*, 5. <https://doi.org/10.1016/j.treng.2021.100083>
- O’Hern, S., & St. Louis, R. (2023, February 8). Technology readiness and intentions to use conditionally automated vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour*, 1–8. <https://doi.org/10.1016/j.trf.2023.02.001>
- Schubert, M. (2015). *Autonomous Cars – Initial Thoughts about Reforming the Liability Regime*. Phi., 46–51.
- Sipetas, Ch., Roncoli, C., & Mladenovich, M. (2023). Mixed fleets of automated and human-driven vehicles in public transport systems: An evaluation of feeder line services. *Transportation Research Interdisciplinary Tendency*, 18, 100791. <https://doi.org/10.1016/j.trip.2023.100791>
- Sladkowski, A., & Pamula, W. (2016). *Intelligent transport systems – problems and perspectives* (Vol. 32). Springer, Switzerland.
- Stepanyan, A. Zh. (2019). Problems of regulation of unmanned vehicles. *Vestnik Universiteta imeni O. E. Kutafina*, 4(56), 169–174. <https://doi.org/10.17803/2311-5998.2019.56.4.169-174>
- Takeyoshi, Imai. (2019). Legal regulation of autonomous driving technology: Current conditions and issues in Japan. *IATSS Research*, 43(4), 263–267. <https://doi.org/10.1016/j.iatssr.2019.11.009>
- Yudkina, V. V. (2022). Highly automated vehicles as a subject of public safety. *Administrativnoye pravo i protsess*, 10. <https://doi.org/10.18572/2071-1166-2022-10-49-5>
- Zemlin, A. I. (2022). Problem issues of the legal regulation of relations associated with using highly automated vehicles. *Zhurnal rossiyskogo prava*, 12. <https://doi.org/10.12737/jrl.2022.128>
- Zhihan, Lv., & Wenlong, Shang. (2023). Impacts of intelligent transportation systems of energy conservation and emission reduction of transport systems: a comprehensive review. *Green Technologies and Sustainability*, 1(1). <https://doi.org/10.1016/j.grets.2022.100002>

Author information



Maria A. Bazhina – Doctor of Juridical Sciences, Associate Professor, Department of Entrepreneurial Law, V. F. Yakovlev Ural State Law University

Address: 21 Komsomolskaya Str., 620137 Yekaterinburg, Russian Federation

E-mail: mashsol@mail.ru

ORCID ID: <https://orcid.org/0000-0003-1237-0052>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57807831200>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/32495219>

Google Scholar ID: <https://scholar.google.ru/citations?user=m5W9vIYAAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=974423

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – April 29, 2023

Date of approval – May 30, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:343.3/.7:004:654.1

EDN: <https://elibrary.ru/fiseet>

DOI: <https://doi.org/10.21202/jdtl.2023.28>

Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности

Евгений Александрович Русскевич

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Ключевые слова

Законодательство,
Интернет,
информационная
безопасность,
киберпреступление,
киберустойчивость,
оператор связи,
право,
сеть связи,
уголовная ответственность,
цифровые технологии

Аннотация

Цель: получение нового знания об ответственности за нарушение правил управления техническими средствами противодействия угрозам информационной безопасности, разработка теоретических рекомендаций и предложений по совершенствованию законодательства и правоприменения.

Методы: методологическую основу исследования составляет совокупность методов научного познания, в том числе абстрактно-логический, догматический, сравнения и др.

Результаты: на основе изучения документов, изданий сделаны следующие выводы: 1) предпринятые на национальном уровне меры по регулированию отношений, связанных с внедрением технических средств противодействия угрозам, в целом соответствуют положениям Доктрины информационной безопасности Российской Федерации; 2) одним из основных направлений развития зарубежного законодательства о телекоммуникациях является построение системы государственно-частного взаимодействия, при котором операторы связи стали бы воспринимать проблему информационной безопасности не как их внутреннюю задачу, а как элемент общей безопасности государства. В этом отношении предельно четко прослеживается констатация необходимости эффективного контроля за деятельностью операторов связи, прежде всего в сфере вводимых технических стандартов обеспечения киберустойчивости; 3) регулирование отношений в сфере управления техническими средствами противодействия угрозам в России характеризуется многочисленностью, многоуровневостью и, соответственно, вполне

© Русскевич Е. А., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

предсказуемой сложностью; 4) реализованная в ст. 274.2 Уголовного кодекса Российской Федерации модель ответственности представителей операторов связи за нарушения в области эксплуатации технических средств противодействия угрозам не представляется оптимальной. Довольно уязвимым является подход к описанию административно преюдициальных признаков состава. Несмотря на значимость отношений, возможность уголовно-правовой реакции на конкретный инцидент возникает не в связи с наступлением тех или иных общественно опасных последствий и даже не при традиционной повторности, а лишь при третьем задокументированном нарушении. Более предпочтительной представляется модель криминализации нарушения управления техническими средствами противодействия угрозам в зависимости от причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

Научная новизна: во многом определяется фактической неразработанностью вопросов, связанных с законодательным определением и реализацией уголовной ответственности за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования.

Практическая значимость: основные положения и выводы исследования могут быть использованы для совершенствования механизма уголовно-правовой охраны информационной безопасности, дальнейшего развития отечественной доктрины уголовного права об ответственности за преступления в сфере компьютерной информации.

Для цитирования

Русскевич, Е. А. (2023). Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности. *Journal of Digital Technologies and Law*, 1(3), 650–672. <https://doi.org/10.21202/jdtl.2023.28>

Содержание

Введение

1. Методика исследования нарушения правил централизованного управления техническими средствами противодействия угрозам информационной безопасности
2. Информационная безопасность и технические средства противодействия угрозам
3. Регулирование в сфере централизованного управления техническими средствами противодействия угрозам информационной безопасности
4. Уголовная ответственность за нарушение централизованного управления техническими средствами противодействия угрозам информационной безопасности

Выводы

Список литературы

Введение

Цифровой мир является как настоящим, так и перспективным будущим человека. Его повседневная деятельность с неизбежностью предполагает взаимодействие с устройствами и технологиями, которые стремительно меняют представление о реальности. Через аккаунты, свои цифровые alter ego, человек коммуницирует, осуществляет трудовую деятельность, получает услуги, приобретает товары. В результате современный человек оказывается в положении параллельного бытия – физического и виртуального. Устраниться от этого, замедлить цифровизацию в известном смысле можно, но неизбежность и необратимость этого процесса заставляет задаться вопросом: а зачем это делать? Отвечая на него, отдельные исследователи указывают на негативные последствия внедрения телекоммуникационных технологий с точки зрения состояния и динамики преступности, изменения ее характеристик. Здесь, как правило, демонстрируется виртуализация механизма криминального оборота запрещенных предметов, существенно осложняющая деятельность правоохранительных органов. Кроме того, довольно обстоятельно раскрывается, что развитие отдельных направлений исследований (например, в сфере искусственного интеллекта и робототехники) обладает вполне конкретной угрозой для человечества в целом.

Пожалуй, все приведенное выше в известном смысле справедливо. Однако верно и то, что дискурс этот в целом не выходит за рамки традиционного для человека замешательства перед чем-то новым, неизведанным, природа которого и возможное влияние представляются не до конца ясными. Любая технология имеет перспективу своей эксплуатации в преступных целях. Это, однако же, не может отменить прогресса как такового, т. е. стремления человека к устройству своей жизни наиболее разумным образом. По этой причине надо говорить не о защите человека от технологий, а о построении модели защиты технологий, или, если точнее, модели правового обеспечения информационно-телекоммуникационного развития, которая позволила бы упреждать и адекватно реагировать на совершение конкретных преступных посягательств. В этом смысле вполне закономерно в центре внимания оказываются вопросы качественного обеспечения устойчивости цифровых сетей по отношению к негативному воздействию или их киберустойчивости.

Федеральным законом от 14 июля 2022 г. № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» глава 28 Уголовного кодекса Российской Федерации¹ (далее – УК РФ) была дополнена новой нормой, устанавливающей ответственность за нарушение специальных правил управления техническими средствами, обеспечивающими нормальное функционирование на территории государства сети Интернет и сетей связи общего пользования (ст. 274.2 УК РФ). Изучение паспорта законопроекта не позволяет ознакомиться с обоснованием реализованной законодательной инициативы – в первоначальной редакции выделение ст. 274.2 УК РФ не планировалось. Соответствующие дополнения появились только ко второму

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. (1996, 17 июня). *Собрание законодательства Российской Федерации*, 25, ст. 2954.

чению законопроекта². Вместе с тем крайне важно не только разобраться в причинах, побудивших к решению о криминализации отдельных нарушений, связанных с управлением техническими средствами противодействия угрозам (далее – ТСПУ), но и проанализировать юридико-технические особенности ст. 274.2 УК РФ, выявить ее достоинства и возможные недостатки.

1. Методика исследования нарушения правил централизованного управления техническими средствами противодействия угрозам информационной безопасности

Методологический инструментарий исследования представлен комплексным сочетанием философских, общенаучных и частнонаучных средств познания. Из общенаучных методов научного познания были использованы такие, как анализ, синтез, дедукция, индукция, классификация, структурно-функциональный метод и др. Особое значение в методологии проведенного исследования было отведено системному методу, который выступал исходной посылкой при решении всех поставленных исследовательских задач.

Эмпирические методы (анализ документов, печатных и электронных изданий) были задействованы при накоплении и изучении материалов исследования. В процессе подготовки статьи было направлено письмо в федеральное государственное унитарное предприятие «Главный радиочастотный центр»³ (далее – ФГУП «ГРЧЦ») в целях получения разъяснений о ТСПУ (получен официальный ответ на обращение от 25 декабря 2022 г.).

В ряду частнонаучных методов познания были использованы сравнительно-правовой, формально-юридический (догматический) и др. Формально-юридический метод применялся при непосредственном изучении нормативных правовых актов Российской Федерации в сфере регулирования и охраны информационных отношений, отечественного и зарубежного уголовного законодательства. Использование догматического метода позволило решить целый ряд исследовательских задач, связанных, например, с выявлением юридико-технической определенности признаков ст. 274.2 УК РФ.

2. Информационная безопасность и технические средства противодействия угрозам

Для понимания процессов, приведших к появлению в отечественном уголовном законодательстве специальной нормы об ответственности за нарушение централизованного управления ТСПУ (ст. 274.2 УК РФ), следует прежде всего обратиться к категории информационной безопасности и документам стратегического планирования в этой сфере.

² Законопроект № 130406-8 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (в целях совершенствования уголовно-правовой охраны национальных интересов Российской Федерации, прав и свобод граждан от новых форм преступной деятельности и угроз государственной безопасности). <https://sozd.duma.gov.ru/bill/130406-8>

³ ФГУП «ГРЧЦ» представляет собой отраслевой экспертный центр, обеспечивающий выполнение задач и функций, возложенных на радиочастотную службу, а также сопровождение контрольно-надзорных и регуляторных функций Роскомнадзора по основным направлениям его деятельности в области связи и в сфере средств массовой информации и массовых коммуникаций. <https://grfc.ru>

В отечественной литературе информационная безопасность разработана обстоятельно⁴. М. А. Ефремова справедливо подчеркивает, что информационная безопасность являет собой динамическую систему общественных отношений. Открытость этой системы обусловлена тем, что информационная безопасность не может иметь постоянный, неизменный характер (Ефремова, 2018).

Категория информационной безопасности (в более узком смысле – киберустойчивости) хорошо исследована и в зарубежной литературе (Colding et al., 2020; Espinoza-Zelaya & Moon, 2022; Hausken, 2020; Li et al., 2020; Prasad & Moon, 2022; Tonhauser & Ristvej, 2019; Tsao et al., 2022).

Как известно, информационная безопасность имеет нормативное определение в Доктрине информационной безопасности Российской Федерации⁵. В соответствии с данным документом «информационная безопасность представляет собой состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»⁶.

Задача обеспечения информационной безопасности, в том числе посредством действенного контроля за деятельностью операторов связи, в некотором смысле является понятной ровно настолько, чтобы можно было предположить отсутствие необходимости это отдельно обосновывать. Все отечественные операторы связи составляют единую сеть связи государства и обеспечивают целостность, доступность, в отдельных случаях конфиденциальность данных, устойчивость и безопасность информационно-коммуникационной инфраструктуры в целом. Как справедливо пишет по этому поводу А. К. Жарова, сеть Интернет, сети связи общего пользования, локальные сети, функционирующие на территории Российской Федерации, хотя и не являются государственными информационными системами, но обеспечивают доступ к информации, содержащейся в государственных информационных системах. Соответственно, безопасность функционирования таких технологий и каналов доступа должна быть обеспечена правовыми инструментами (Жарова, 2022).

Национальная безопасность больше не определяется исключительно военной составляющей и границами государства. Киберугрозы носят спорадический и многомерный характер, создают риски причинения колоссального ущерба. При этом эти угрозы нельзя предупредить только традиционными средствами, такими как применение военной силы или правоохранительного механизма, – требуется эффективное двустороннее сотрудничество между правительствами и частным сектором (Li & Liu, 2021).

⁴ См., например: Калмыков, Д. А. (2005). *Информационная безопасность: понятие, место в системе уголовного законодательства Российской Федерации, проблемы правовой охраны*: дис. ... канд. юрид. наук. Ярославль. <https://elibrary.ru/nnomvb>; Кубышкин, А. В. (2002). *Международно-правовые проблемы обеспечения информационной безопасности государства*: дис. ... канд. юрид. наук. Москва; Лопатин, В. Н. (2000). *Информационная безопасность России*: дис. ... д-ра юрид. наук. Санкт-Петербург.

⁵ Указ Президента РФ № 646 от 05.12.2016. (2016, 12 декабря). *Собрание законодательства Российской Федерации*, 50, ст. 7074.

⁶ Там же.

Несмотря на это, в России выстраивание архитектуры регулирования государственно-частного взаимодействия в этой области долгое время не реализовывалось. Соответственно, не ставился вопрос и об ответственности операторов связи за несоблюдение необходимых стандартов информационной безопасности. Нельзя сказать, что такие решения не вызревали в общественном сознании и не обсуждались как перспективные в профессиональном сообществе. Дискуссия велась довольно активно, но, как это часто бывает, для непосредственной реализации потребовались изменение социальных условий и формирование актуального запроса в векторе обеспечения государственной безопасности.

Нетрудно понять, почему соответствующие изменения российского уголовного законодательства о введении ответственности за нарушение использования ТСПУ появились именно на этом этапе. За последнее время кибератаки на информационную инфраструктуру возросли многократно (Ельчанинова, 2020; Трунцевский, 2019; Красинский, Машко, 2023; Бокшицкий, Мельцева, 2017), в том числе в условиях пандемии коронавируса (Lallie et al., 2021; Hoheisel et al., 2023; Хисамова, Бегишев, 2022). При этом они имеют сложный характер, свидетельствующий о тщательной подготовке таких действий, наличии у злоумышленников высоких компетенций и дорогостоящего оборудования (Horsman, 2021; Kouloufakos, 2023; Boughton, 2019). Роскомнадзор сослался на это в своих комментариях относительно рассматриваемых законодательных новелл. В частности, было отдельно отмечено, что «в условиях гибридной войны, включающей элементы информационного противостояния, а также регулярные кибератаки, защита информационного пространства России является критически важной для государства и общества. В связи с этим необходимо безусловное выполнение операторами связи требований к установке, эксплуатации и модернизации ТСПУ и требований к пропуску всего трафика через них. Все технические средства противодействия угрозам находятся под управлением Центра мониторинга и управления сетью связи общего пользования (далее – ЦМУ ССОП), обеспечивающего отражение информационных атак»⁷.

Другим обстоятельством является то, что в условиях нарастающей международной напряженности и информационного противоборства особую значимость приобрело соблюдение вводимых ограничений по доступу к отдельным сетевым ресурсам. Иными словами, потребовалось не только поставить поток информации под технологический контроль (фильтрацию), выстроить барьеры, препятствующие доступу пользователей к конкретному трафику и мобильным приложениям, но и действенным образом обеспечить ответственность представителей операторов связи за уклонение от исполнения этих стандартов. В этом ключе были даны и пояснения Роскомнадзора: «Нередки случаи, когда операторы пропускают трафик в обход ТСПУ, по тем или иным причинам допускают отключение такого оборудования. Это может представлять угрозу устойчивому функционированию Интернета в России, привести к сбою в работе информационных ресурсов государственных органов. При отключении ТСПУ или пропуске трафика в обход российские пользователи получают доступ к информации, представляющей опасность: детской порнографии, пронаркотическому контенту, пропаганде самоубийства, фейкам, экстремистской информации»⁸.

⁷ В РКН заявили, что отказ операторов от использования ТСПУ представляет угрозу для граждан. (2022, 15 июля). <https://tass.ru/obschestvo/15228891>

⁸ Там же.

Принятие решения о построении системы мониторинга с использованием ТСПУ в целом соответствует положениям Доктрины информационной безопасности Российской Федерации, которая основными направлениями ее обеспечения определяет: противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации; пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами и др.

Немаловажно отметить, что предпринятые на национальном уровне меры по регулированию отношений, связанных с внедрением ТСПУ, в целом соответствуют тенденциям ряда зарубежных стран (Bitzer et al., 2023; Cascavilla et al., 2021; Mohamed, 2013; Nguyen & Golman, 2021; Broadhead, 2018; Qamar et al., 2023). В настоящей работе нет задачи дать развернутую характеристику тем процессам, которые происходят во всем мире. Вместе с тем сформировать некое общее представление о них все же необходимо хотя бы потому, чтобы лучше понимать ситуацию с обеспечением функционирования ТСПУ в России.

В определенном смысле российская модель регулирования и охраны отношений, связанных с внедрением и эксплуатацией ТСПУ, повторяет опыт Китайской Народной Республики (далее – КНР). Как совершенно справедливо отмечается в литературе, миллиардное количество пользователей сети Интернет в КНР предоставило государству большие экономические преимущества, но вместе с тем создает реальные угрозы для его экономической и политической безопасности (Дремлюга и др., 2017). Китай одним из первых столкнулся с рисками и оценил те «достоинства», которые возникают при сохранении курса на невмешательство в деятельность операторов телекоммуникационной связи на национальном уровне (Ye & Zhao, 2023). В настоящее время многие популярные зарубежные интернет-ресурсы в КНР заблокированы по причине того, что они осуществляют распространение информации, противоречащей идеологии Китая, морально-нравственным устоям общества, имеют признаки террористической либо экстремистской пропаганды. Более того, Закон КНР о безопасности сети Интернет 2016 г.⁹ обязывает провайдеров требовать от пользователей регистрироваться под своими реальными именами, осуществлять фильтрацию контента и реализацию запретов на блокирование ресурсов, использовать только сертифицированное оборудование, исполнять требование о локализации данных пользователей, предоставлять техническую поддержку и содействие органам общественной и государственной безопасности и др. Нарушение соответствующих правил, обеспечивающих безопасность сетевого пространства КНР, может повлечь принудительное прекращение деятельности оператора связи, а равно привлечение ее сотрудников к ответственности, в том числе уголовной.

В отечественной литературе небезосновательно признается, что репрессивное китайское законодательство в интернет-сфере, кроме очевидного для западной

⁹ В Китае вступает в силу резонансный Закон о кибербезопасности. <https://ria.ru/20170601/1495523455.html>

общественности нарушения прав и свобод, все же серьезным образом способствует «фильтрации» попадающего в китайский сегмент противоправного контента, защищая государственность и своих граждан от терроризма, экстремизма, сект, порнографии, насилия, подрывной деятельности иностранных разведок и т. п. (Лузянин, Трошинский, 2018).

В рамках Содружества Независимых Государств (далее – СНГ) подход, связанный с определением ответственности за нарушение правил использования ТСПУ, не получил своего распространения. В Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий¹⁰ соответствующие рекомендации также отсутствуют. Пожалуй, наиболее близкими по содержанию являются положения ст. 2781 «Нарушение правил информатизации» Уголовного кодекса Республики Узбекистан¹¹.

20 декабря 2018 г. вступила в силу Директива (ЕС) 2018/1972 Европейского парламента и Совета от 11.12.2018 о Европейском кодексе электронных коммуникаций¹². В соответствии с Директивой государства-члены должны обеспечить, чтобы поставщики общедоступных сетей электронной связи или общедоступных услуг электронной связи принимали надлежащие и пропорциональные технические и организационные меры для надлежащего управления рисками, связанными с безопасностью сетей и услуг. Принимая во внимание уровень техники, эти меры должны обеспечивать уровень безопасности, соответствующий существующему риску. Агентство Европейского союза по сетевой и информационной безопасности (ENISA) должно способствовать координации действий государств-членов во избежание расхождений в национальных требованиях, которые могут создавать риски безопасности и барьеры для внутреннего рынка. Государства-члены также должны обеспечить, чтобы поставщики общедоступных сетей электронной связи или общедоступных услуг электронной связи уведомляли без неоправданной задержки компетентный орган об инциденте безопасности, который оказал значительное влияние на работу сетей или услуг.

Государства-члены должны обеспечить, чтобы компетентные органы имели право издавать обязательные инструкции, в том числе касающиеся мер, необходимых для устранения инцидента безопасности или предотвращения его возникновения, поставщикам сетей электронной связи общего пользования или общедоступных услуг электронной связи. Государства-члены должны обеспечить, чтобы компетентные органы имели право требовать от поставщиков сетей электронной связи общего пользования или общедоступных услуг электронной связи: предоставлять информацию, необходимую для оценки безопасности своих сетей и услуг, включая документированные политики безопасности; подвергаться аудиту безопасности, проводимому квалифицированным независимым органом или компетентным органом, и предоставлять его результаты компетентному органу; стоимость аудита оплачивается поставщиком¹³.

¹⁰ Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий. (2022, 15 августа). *Собрание законодательства Российской Федерации*, 33, ст. 5883

¹¹ <https://lex.uz/docs/111457#111470>

¹² Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02018L1972-20181217>

¹³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972#d1e4938-36-1>

Директива обусловила изменение законодательств стран Европейского союза о телекоммуникационных технологиях и защите данных. Так, например, в Германии 22 апреля 2021 г. был принят Telecommunications Modernization Act (TKMG). Кроме того, был принят Telecommunications Telemedia Data Protection Act (TTDSG) – Закон о защите данных в телекоммуникациях Германии, который сопровождается новым техническим руководством по осуществлению установленных законом мер по мониторингу телекоммуникаций. Новые требования безопасности к телекоммуникационной отрасли вводят категорию «критических компонентов телекоммуникаций». Эти компоненты могут использоваться только в том случае, если они были протестированы и сертифицированы официально признанным органом по сертификации и если производитель компонентов представил оператору сети «декларацию о надежности». В соответствии с новым регулирующим режимом операторы с повышенным потенциалом риска должны использовать соответствующие системы обнаружения вторжений (IDS) и/или обнаружения атак (ADS). Кроме того, соответствующие операторы должны проходить внешний аудит безопасности каждые два года¹⁴.

В Великобритании 17 ноября 2021 г. был принят Закон о телекоммуникационной безопасности (Telecommunications (Security) Act 2021)¹⁵. Этим законом были внесены изменения в Закон о связи 2003 г.¹⁶ В ряду наиболее значимых положений следует назвать прямое определение в ст. 105A обязанностей операторов связи выявлять угрозы киберустойчивости и предпринимать меры, направленные на их преодоление и предупреждение. Кроме того, в ст. 105B предусмотрена обязанность операторов связи исполнять предписания государственного регулятора. В ст. 105E закреплено, что орган государственного контроля обладает полномочиями по подготовке и принятию правил обеспечения киберустойчивости. Соответствующие правила, закрепляющие технические стандарты безопасности и конкретные практики, являются обязательными для исполнения провайдерами. Функциями по непосредственному контролю и надзору за исполнением правил наделено Управление связи OFCOM.

За нарушения правил и стандартов телекоммуникационной безопасности, уклонение от исполнения предписаний OFCOM предусмотрены значительные штрафы, в том числе оборотные. Закон о связи Великобритании только в ст. 404 оговаривает вопрос о возможном привлечении к уголовной ответственности руководителя компании, «если деяние совершено юридическим лицом и доказано, что оно было совершено с согласия или при попустительстве, или было связано с каким-либо пренебрежением со стороны директора, менеджера, секретаря или другого лица, выполняющего управленческие функции».

14 июня 2022 г. в Канаде было инициировано обсуждение законопроекта (Bill C-26), направленного на внесение изменений в Закон о телекоммуникациях¹⁷. Его целью является укрепление безопасности государства, а также обеспечение киберустойчивости телекоммуникационной инфраструктуры посредством предоставления соответствующим государственным структурам новых полномочий

¹⁴ <https://www.gesetze-im-internet.de/ttdsg/>

¹⁵ <https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted>

¹⁶ <https://www.legislation.gov.uk/ukpga/2003/21/contents>

¹⁷ <https://www.parl.ca/legisinfo/en/bill/44-1/C-26>

относительно контроля за деятельностью операторов связи. Изучение законопроекта позволяет сделать вывод, что перечень таких полномочий крайне широк и предполагает не только надзор за соблюдением принятых стандартов безопасности, но и возможность налагать запреты на использование отдельного оборудования, предоставлять услуги связи отдельным пользователям и др. Надо сказать, что законопроект вызвал активное обсуждение. Так, было опубликовано открытое письмо министру общественной безопасности, в котором отмечалось, что законопроект С-26 уполномочивает правительство тайно приказывать операторам связи «делать что-либо или воздерживаться от чего-либо». Это открывает дверь для наложения обязательств по надзору на частные компании и на другие риски, такие как ослабление стандартов шифрования – то, что общественность уже давно отвергает как несовместимое с нашими правами на неприкосновенность частной жизни»¹⁸. Профессиональное сообщество заявило о существенном и неоправданном ограничении свободы экономической деятельности, а также о том, что предлагаемые стандарты попросту разорят малых участников рынка телекоммуникационных услуг. До настоящего времени законопроект не принят.

Таким образом, если попытаться в самом общем виде определить направление развития зарубежного законодательства о телекоммуникациях, то можно сделать вывод, что оно заключается в попытке выстроить систему государственно-частного взаимодействия, при котором операторы связи стали бы воспринимать проблему информационной безопасности не как их внутреннюю задачу, а как элемент общей безопасности государства. В этом отношении предельно четко прослеживается констатация необходимости эффективного контроля за деятельностью операторов связи, прежде всего в сфере вводимых технических стандартов обеспечения киберустойчивости.

3. Регулирование в сфере централизованного управления техническими средствами противодействия угрозам информационной безопасности

Обязанность оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети Интернет, обеспечивать установку в своей сети ТСПУ предусмотрена п. 5.1 ст. 46 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»¹⁹. Соответствующее положение впервые появилось в отечественном законодательстве с принятием Федерального закона от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”»²⁰.

Важно отметить, что сама законодательная инициатива явилась ответом на Стратегию национальной кибербезопасности США, принятую в сентябре 2018 г. Как отмечается в пояснительной записке к законопроекту: «В подписанном Президентом США документе декларируется принцип “сохранения мира силой”. Россия же напрямую и бездоказательно обвиняется в совершении хакерских атак, откровенно

¹⁸ <https://ccla.org/privacy/joint-letter-of-concern-regarding-bill-c-26/>

¹⁹ (2003, 14 июля). *Собрание законодательства Российской Федерации*, 28, ст. 2895.

²⁰ <http://publication.pravo.gov.ru/Document/View/0001201905010025>

говорится о наказании: “Россия, Иран, Северная Корея провели ряд безответственных кибератак, которые нанесли ущерб американским и международным компаниям, нашим союзникам и партнерам и не понесли соответствующего наказания, что могло бы сдерживать кибератаки в будущем”. В этих условиях необходимы защитные меры для обеспечения долгосрочной и устойчивой работы сети Интернет в России, повышения надежности работы российских интернет-ресурсов. Определяются необходимые правила маршрутизации трафика, организуется контроль их соблюдения. Создается возможность для минимизации передачи за рубеж данных, которыми обмениваются между собой российские пользователи. Определяются трансграничные линии связи и точки обмена трафиком. Предусматривается возможность установки на сетях связи технических средств, определяющих источник передаваемого трафика. Технические средства должны будут обладать возможностью ограничить доступ к ресурсам с запрещенной информацией не только по сетевым адресам, но и путем запрета пропуска проходящего трафика»²¹.

Закон от 1 мая 2019 г. № 90-ФЗ, также известный как Закон «О суверенном Рунете», вызвал принципиальные споры и даже протесты среди отдельных представителей отрасли и гражданского общества. Отмечалось, что его реализация создает неоправданные риски для конституционных прав и свобод граждан, потребует миллиардных затрат, угрожает конкуренции на рынке услуг связи и будет способствовать коррупционному поведению²². Ситуация, во многом аналогичная той, которая сложилась в связи с обсуждением законопроекта (Bill C-26) в Канаде, о чем уже было сказано ранее. Сейчас уже можно вполне уверенно заявить о том, что другого возможного решения для России по большому счету не оставалось. Конечно, создание единого контура защиты информационной инфраструктуры государства требует значительного финансирования. Нельзя не согласиться и с тезисом о принципиальном расширении контроля со стороны государства за активностью граждан в виртуальном пространстве. Вместе с тем здесь важен тот баланс, который и определяет состояние информационной безопасности как динамической системы, меняющейся под влиянием внешних условий.

Основным документом, определяющим в настоящее время регулирование в сфере управления техническими средствами обеспечения киберустойчивости цифровых сетей, является Постановление Правительства Российской Федерации от 12 февраля 2020 г. № 126 «Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования»²³.

Изучение данного нормативного акта позволяет сделать вывод, что механизм взаимодействия между радиочастотной службой и оператором связи имеет

²¹ Пояснительная записка «К проекту Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации». СПС «КонсультантПлюс».

²² См.: Бизнес раскритиковал детали перехода к «суверенному рунету». (2019, 26 июня). *Коммерсант*. <https://www.kommersant.ru/doc/4012730?ysclid=ldkccj43i272099969>; Глава РСПП заявил о коррупционных рисках закона о «суверенном Рунете». (2019, 30 июля). *РБК*. https://www.rbc.ru/technology_and_media/30/07/2019/5d3f08389a7947ada3baf05b

²³ (2020, 24 февраля). *Собрание законодательства Российской Федерации*, 8, ст. 1001.

многоэтапный характер. Правила предусматривают, что не позднее 90 календарных дней до планируемой даты установки ТСПУ оператору связи направляется запрос о предоставлении информации, включающей в себя: схемы построения сети связи оператора связи; технические характеристики средств связи оператора связи; места планируемой установки ТСПУ; количество каналов передачи данных с указанием физических свойств таких каналов, их технологии и пропускной способности; сведения о среднестатистической и максимальной загрузке каналов; сведения о структуре узла связи в месте планируемой установки ТСПУ; сведения о планах модернизации, реконструкции узла связи, ликвидации фрагмента сети связи; техническую информацию и технологические параметры средств связи операторов связи, необходимые для разработки проектной документации по установке и подключению ТСПУ.

Оператор связи обязан подготовить ответ на соответствующий запрос в течение 15 рабочих дней с момента его получения. При этом постановлением предусмотрено направление оператору связи уточняющего запроса в течение семи рабочих дней после получения ответа. В таком случае оператор связи должен подготовить ответ в течение трех рабочих дней со дня получения запроса.

Соответствующая процедура обмена информацией в целом призвана обеспечить необходимую подготовку к реализации согласованного плана мероприятий по установке и (или) модернизации ТСПУ. С уголовно-правовой точки зрения интерес представляет квалификация действий должностных лиц оператора связи, которые сознательно уклоняются от предоставления соответствующей информации либо заведомо указывают недостоверные данные. Полагаем, что при наличии на то фактических оснований следует рассматривать возможность применения ст. 201 УК РФ и 327 УК РФ соответственно. И если в ситуации использования заведомо подложного документа все относительно ясно, то применительно к злоупотреблению полномочиями необходимо установить не только бездействие лица, но и наступление негативных последствий, например, связанных с масштабным сбоем в работе объектов информационно-коммуникационной инфраструктуры и т. п. При этом важным и очевидно непростым моментом реализации механизма уголовной ответственности будет установление наличия причинно-следственной связи между уклонением от предоставления данных, отсутствием ТСПУ на конкретных каналах связи и наступившими общественно опасными последствиями.

Важнейшее значение для применения положений административного и уголовного законодательства имеет п. 10 Правил, определяющий обязанности оператора связи при эксплуатации технических средств противодействия угрозам: обеспечить ТСПУ электропитанием; обеспечить техническую поддержку функционирования ТСПУ в части их подключения к своей сети связи, организации технологического канала связи для управления указанными средствами, в том числе в соответствии с техническими условиями установки ТСПУ; обеспечивать не позднее 48 часов с момента поступления требования радиочастотной службы доступ к ТСПУ представителям радиочастотной службы; не препятствовать радиочастотной службе осуществлять посредством использования специальных программных средств дистанционное управление ТСПУ; соблюдать требования к обеспечению функционирования ТСПУ, содержащиеся в эксплуатационной документации; обеспечить выполнение комплекса мер, направленных на безопасную эксплуатацию ТСПУ, в том числе предусматривающих исключение возникновения аппаратного, программного и физического воздействия неуполномоченных лиц на функционирование ТСПУ и др.

Изучение приведенных выше положений Правил позволяет сделать вывод, что в отдельных случаях привлечение представителей оператора связи к ответственности будет предполагать необходимость непосредственного указания на нарушение конкретных положений и требований, предусмотренных другими документами (например, инструкцией по взаимодействию уполномоченных лиц оператора связи с радиочастотной службой, эксплуатационной документацией оборудования и др.).

Технические условия установки, а также требования к сетям при использовании ТСПУ определены Приказом Роскомнадзора от 31 июля 2019 г. № 228 «Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам»²⁴.

В дополнение надо указать, что регулирование в части управления ТСПУ приведенными нормативными актами не исчерпывается и в настоящее время характеризуется многочисленностью, многоуровневостью и соответственно вполне предсказуемой сложностью. В ряду таковых следует отдельно отметить: Постановление Правительства Российской Федерации от 3 ноября 2022 г. № 1978 «Об утверждении требований к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и Правил функционирования и взаимодействия системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования с информационными системами и иными системами, в том числе с системами операторов связи»²⁵, Приказ Минкомсвязи России от 7 октября 2019 г. № 572 «Об утверждении требований к обеспечению функционирования точек обмена трафиком, включая требования к обеспечению устойчивого функционирования технических и программных средств связи, сооружений связи, а также порядка соблюдения требований, предусмотренных п. 4 ст. 56.2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»²⁶ и др.

4. Уголовная ответственность за нарушение централизованного управления техническими средствами противодействия угрозам информационной безопасности

Следует предположить, что объектом преступления, предусмотренного ст. 274.2 УК РФ, выступают общественные отношения, связанные с эксплуатацией ТСПУ, и обеспечением устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования. Возникновение этих отношений между государством и операторами связи, как было показано выше, состоялось сравнительно недавно и имело соответствующие социально-правовые предпосылки.

²⁴ <http://publication.pravo.gov.ru/Document/View/0001201909120028>

²⁵ (2022, 14 ноября). *Собрание законодательства Российской Федерации*, 46, ст. 7995.

²⁶ <https://minjust.consultant.ru/documents/45269>

Интересным представляется подход, согласно которому в современных условиях объектом преступлений в сфере компьютерной информации являются общественные отношения в сфере цифровой экономики и информационного общества (Дремлюга, 2022). В определенном смысле, опираясь на стратегические документы в сфере развития цифровой экономики России, с такой трактовкой можно согласиться. Пожалуй, его недостатком является лишь вполне очевидная обширность используемой терминологии, которая при определенных обстоятельствах не позволяет выделить специфику именно конкретной группы общественно опасных посягательств в рамках Особенной части УК РФ.

Предметом являются сами технические средства противодействия угрозам (ТСПУ). Следует отметить, что какой-либо перечень соответствующего оборудования в открытом доступе отсутствует. Согласно разъяснениям радиочастотной службы, сведения о данных устройствах составляют коммерческую тайну.

Часть 1 ст. 274.2 УК РФ предусматривает ответственность за нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости функционирования сети Интернет и сети связи общего пользования либо несоблюдение технических условий их установки или требований при использовании. Диспозиция является бланкетной и отсылает к Постановлению Правительства Российской Федерации от 12 февраля 2020 г. № 126²⁷.

Объективная сторона данного преступления предполагает как активное, так и пассивное поведение субъекта и может заключаться в воспрепятствовании дистанционному управлению радиочастотной службой техническими средствами противодействия угрозам; нарушении требований, содержащихся в эксплуатационной документации; отключении технических средств противодействия угрозам от электропитания; в блокировании доступа к соответствующему оборудованию представителям радиочастотной службы и др.

В ч. 2 ст. 274.2 УК РФ объективная сторона заключается в нарушении требований к пропуску трафика через технические средства противодействия угрозам. Соответствующие требования определены Приказом Минцифры России от 26 января 2022 г. № 44 «Об утверждении Требований к порядку пропуска трафика в сетях передачи данных»²⁸.

В соответствии с Постановлением Правительства Российской Федерации от 12 февраля 2020 г. № 127 «Об утверждении Правил централизованного управления сетью связи общего пользования»²⁹ оператор связи имеет право не направлять трафик через технические средства противодействия угрозам в следующих случаях: а) нарушение функционирования технического средства противодействия угрозам, при котором прекращается пропуск трафика через данное техническое средство, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам; б) нарушение функционирования технического средства противодействия угрозам, при котором параметры пропуска трафика не соответствуют параметрам, указанным в проектной документации на установку и функционирование

²⁷ Постановление Правительства РФ № 126 от 12.02.2020. *Собрание законодательства Российской Федерации*, 8, ст. 1001.

²⁸ <http://publication.pravo.gov.ru/Document/View/0001202203010002>

²⁹ (2020, 24 февраля). *Собрание законодательства Российской Федерации*, 8, ст. 1002.

технических средств противодействия угрозам, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам; в) выявление информации или информационных ресурсов, доступ к которым не подлежит ограничению в соответствии с законодательством Российской Федерации, но доступ к которым ограничивается. Направление трафика помимо технических средств противодействия угрозам в иных случаях, не предусмотренных Постановлением № 127, может быть квалифицировано как нарушение требований к пропуску трафика по смыслу ч. 2 ст. 274.2 УК РФ.

Оба состава преступления сконструированы с использованием административной преюдиции и предполагают, что соответствующее нарушение правил должно быть допущено в период, когда лицо считается подвергнутым административному наказанию за правонарушения, предусмотренные квалифицированными видами ст. 13.42 Кодекса Российской Федерации об административных правонарушениях³⁰ (далее – КоАП РФ) и 13.421 КоАП РФ. Отягчающим признаком в обоих случаях выступает повторность административного правонарушения. Таким образом, по смыслу ст. 274.2 УК РФ признаки уголовно наказуемого деяния будут иметь место лишь при третьем нарушении правил централизованного управления ТСПУ.

С точки зрения законодательного описания деяние, предусмотренное ст. 274.2 УК РФ, относится к весьма многочисленной группе преступлений, связанных с нарушением специальных правил, двойственная природа которых, по меткому определению Н. И. Пикурова, характеризуется сочетанием проступка и преступления (как бы формат «юридической матрешки») (Пикуров, 2009).

Предложенная законодательная модель ответственности представителей операторов связи за нарушения в области эксплуатации ТСПУ не представляется оптимальной. Во-первых, довольно уязвимым является подход к описанию административно-преюдициальных признаков состава. Несмотря на значимость отношений, обеспечиваемых системой централизованного управления ТСПУ, возможность уголовно-правовой реакции на конкретный инцидент появляется не в связи с наступлением тех или иных общественно опасных последствий и даже не при традиционной повторности, а лишь при третьем задокументированном нарушении.

В продолжение данной мысли следует предположить, что напрасно законодатель отказался от модели криминализации нарушения управления ТСПУ в зависимости от причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства. Это в некотором смысле уже сейчас ставит вопрос о квалификации действий представителя оператора связи, который, используя свои управленческие полномочия, вмешался в функционирование ТСПУ, что в результате привело к наступлению значимых общественно опасных последствий (например, в результате кибератаки были утеряны персональные данные нескольких тысяч пользователей, выведена из строя информационная инфраструктура крупных хозяйствующих субъектов, похищены денежные средства в особо крупных размерах и т. п.). Полагаем, что при наличии признаков специального субъекта, предусмотренного ст. 201 УК РФ, предпочтение должно быть отдано в пользу применения именно данной нормы. На это, в частности, указывает и соотношение санкций ст. 274.2 УК РФ и 201 УК РФ.

³⁰ (2002, 7 января). *Собрание законодательства Российской Федерации*, 1 (ч. I), ст. 1.

Субъект обоих преступлений специальный – должностное лицо, понятие которого сформулировано в примечании к ст. 274.2 УК РФ, – лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации, а равно индивидуальный предприниматель, подвергнутые административному наказанию за соответствующие деяния, предусмотренные Кодексом об административных правонарушениях Российской Федерации.

В исследуемой норме законодатель допускает не вполне удачное использование терминологии. Должностными лицами названы субъекты, обладающие управленческими функциями в коммерческой или иной организации (см. примечание к ст. 201 УК РФ). Таким образом, как бы утверждается два вида должностных лиц – в коммерческих и иных организациях, а также в государственных органах, органах местного самоуправления и т. д. (см. примечание к ст. 285 УК РФ).

Субъективная сторона напрямую не раскрыта в ст. 274.2 УК РФ. Принимая во внимание формальную конструкцию составов, следует сделать вывод, что субъективная сторона нарушения специальных правил по смыслу ч. 1 ст. 274.2 УК РФ и нарушения требований к пропуску трафика по ч. 2 ст. 274.2 УК РФ выражается виной в виде прямого умысла. При этом содержание мотивов и целей не влияет на квалификацию преступления.

В случае, когда соответствующие нарушения были допущены по неосторожности, вследствие небрежного отношения к соблюдению эксплуатационных требований и иных правил, содеянное в зависимости от обстоятельств дела может быть квалифицировано по ст. 274 УК РФ либо по ч. 3 ст. 274.1 УК РФ.

Выводы

Подводя итог, следовало бы еще раз подчеркнуть, что само решение о создании в России замкнутого контура защиты информационной безопасности посредством внедрения ТСПУ и выстраивания соответствующей системы отношений между государством и операторами связи, можно только приветствовать. По большому счету неважно, какие конкретно внешние или внутренние причины приблизили реализацию реформы в сфере телекоммуникаций. Полагать, что «суверенный Рунет» есть сугубо российская история, экстраординарная реакция на экстраординарные обстоятельства, пожалуй, неверно. Этому способствовали гораздо более сложные и глубинные процессы. Подтверждением данной мысли является опыт ряда зарубежных стран, которые либо уже реализовали соответствующие реформы, либо активно продвигаются в этом направлении.

Вместе с тем модель уголовно-правового обеспечения отношений в сфере централизованного управления ТСПУ, получившую свое оформление в ст. 274.2 УК РФ, вряд ли можно признать свободной от недостатков и противоречий. И дело не только в продолжении весьма спорной ветки развития отечественного уголовного законодательства, связанной с расширением в Особенной части УК РФ составов с административной преюдицией. Хотя данный подход во многом исключил саму возможность дифференциации ответственности за данное преступление. Проблема в самом условии предварительного двукратного привлечения к административной ответственности за соответствующее деяние в течение года. Весьма уязвимым также является решение об использовании категории должностного лица, которому

законодатель решил придать свое «автономное» значение исключительно к ст. 274.2 УК РФ.

Востребованность и качество нормы довольно скоро будут верифицированы практикой. И в этом отношении стоит только полагаться на время. Доктрина же традиционно, надеясь на лучшее, должна готовиться к худшему, обсуждая и вырабатывая возможные перспективные шаги по изменению закона и преодолению проблем правоприменения.

Список литературы

- Бокшицкий, В. И., Мельцева, И. С. (2017). Совершенствование защиты общественно значимых информационных ресурсов. *Вопросы кибербезопасности*, S2(20), 11–14. <https://www.elibrary.ru/vzvzgg>
- Дремлюга, Р. И. (2022). *Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение*: монография. Москва: Юрлитинформ. <https://www.elibrary.ru/hsbxrm>
- Дремлюга, Р. И., Коробеев, А. И., Федоров, А. В. (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. *Всероссийский криминологический журнал*, 11(3), 607–614. EDN: <https://www.elibrary.ru/zhnbdp>. DOI: [https://doi.org/10.17150/2500-4255.2017.11\(3\).607-614](https://doi.org/10.17150/2500-4255.2017.11(3).607-614)
- Ельчанинова, Н. Б. (2020). Защита критической информационной инфраструктуры как новый институт правового обеспечения информационной безопасности. *Информационное общество*, 2, 58–65.
- Ефремова, М. А. (2018). *Уголовно-правовая охрана информационной безопасности*: монография. Москва: Юрлитинформ. <https://www.elibrary.ru/zihcgl>
- Жарова, А. К. (2022). Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях. *Безопасность бизнеса*, 1, 19–26. EDN: <https://www.elibrary.ru/mnaski>. DOI: <https://doi.org/10.18572/2072-3644-2022-1-19-26>
- Красинский, В. В., Машко, В. В. (2023). Кибертерроризм: криминологическая характеристика и квалификация. *Государство и право*, 1, 79–91. EDN: <https://www.elibrary.ru/omupsq>. DOI: <https://doi.org/10.31857/S102694520024122-5>
- Лузянин, С. Г., Трошинский, П. В. (2018). Обеспечение национальной безопасности Китая на современном этапе (нормативно-правовой аспект). *Журнал зарубежного законодательства и сравнительного правоведения*, 1, 60–69. EDN: <https://www.elibrary.ru/yshope>. DOI: <https://doi.org/10.12737/art.2018.1.8>
- Пикуров, Н. И. (2009). *Квалификация преступлений с бланкетными признаками состава*: монография. Москва: Российская академия правосудия.
- Трунцевский, Ю. В. (2019). Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов. *Журнал российского права*, 5(269), 99–106. EDN: <https://www.elibrary.ru/krnllwx>. DOI: https://doi.org/10.12737/art_2019_5_9
- Хисамова, З. И., Бегишев И. Р. (2022). Цифровая преступность в условиях пандемии: основные тренды. *Всероссийский криминологический журнал*, 16(2), 185–198. [https://doi.org/10.17150/2500-4255.2022.16\(2\).185-198](https://doi.org/10.17150/2500-4255.2022.16(2).185-198)
- Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, 125, 103050. <https://doi.org/10.1016/j.cose.2022.103050>
- Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, 4, 18–19. [https://doi.org/10.1016/S1353-4858\(19\)30051-0](https://doi.org/10.1016/S1353-4858(19)30051-0)
- Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, 34(6), 1180–1196. <https://doi.org/10.1016/j.clsr.2018.08.005>
- Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, 105, 102258. <https://doi.org/10.1016/j.cose.2021.102258>
- Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, 103, 102761. <https://doi.org/10.1016/j.cities.2020.102761>
- Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, 55(10), 2252–2257. <https://doi.org/10.1016/j.ifacol.2022.10.043>

- Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, 11, 100204. <https://doi.org/10.1016/j.iot.2020.100204>
- Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, 128, 103158. <https://doi.org/10.1016/j.cose.2023.103158>
- Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, 61 (6), 761–770. <https://doi.org/10.1016/j.scijus.2021.10.003>
- Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, 49, 105809. <https://doi.org/10.1016/j.clsr.2023.105809>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egy.2021.08.126>
- Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, 53(4), 7–13. <https://doi.org/10.1016/j.ifacol.2021.04.001>
- Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, 29(1), 66–76. <https://doi.org/10.1016/j.clsr.2012.11.005>
- Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: ‘Law on the books’ vs ‘law in action’. *Computer Law & Security Review*, 40, 105521. <https://doi.org/10.1016/j.clsr.2020.105521>
- Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, 55(10), 2246–2251. <https://doi.org/10.1016/j.ifacol.2022.10.042>
- Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, 128, 103127. <https://doi.org/10.1016/j.cose.2023.103127>
- Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, 40, 1591–1596. <https://doi.org/10.1016/j.trpro.2019.07.220>
- Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, 133, 102894. <https://doi.org/10.1016/j.adhoc.2022.102894>
- Ye, W., & Zhao, L. (2023). “I know it’s sensitive”: Internet censorship, recoding, and the sensitive word culture in China. *Discourse, Context & Media*, 51, 100666. <https://doi.org/10.1016/j.dcm.2022.100666>

Сведения об авторе



Русскевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)

Адрес: 125993, Российская Федерация, г. Москва, ул. Садовая-Кудринская, 9

E-mail: russkevich@mail.ru

ORCID ID: <https://orcid.org/0000-0003-4587-8258>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57919310600>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/2510065>

Google Scholar ID: <https://scholar.google.ru/citations?user=rwKPImlAAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование выполнено в рамках государственного задания «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023-0006)». Регистрационный номер: 1022040700002-6-5.5.1.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.77.51 / Отдельные виды преступлений

Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 6 февраля 2023 г.

Дата одобрения после рецензирования – 13 апреля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.28>

Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security

Evgeniy A. Russkevich

Kutafin Moscow State Law University
Moscow, Russian Federation

Keywords

Communication network,
communication operator,
criminal liability,
cyber resilience,
cybercrime,
digital technologies,
information security,
Internet,
law,
legislation

Abstract

Objective: to acquire new knowledge about the liability for violating the rules of managing technical means of counteracting the threats to information security; to elaborate theoretical recommendations and proposals for improving legislation and law enforcement.

Methods: the methodological basis of the research is a set of scientific cognition methods, including abstract-logic, dogmatic, comparison, etc.

Results: based on studying documents and publications, the following conclusions were made: 1) the measures taken at the national level for regulating the relations associated with introduction of technical means of counteracting the threats generally comply with the provisions of the Doctrine on information security of the Russian Federation; 2) one of the main directions of development of the foreign legislation on telecommunications is building a system of public-private interaction, in which communication operators would perceive the information security problem not as their internal task but as an element of the overall security of the state. In this regard, one may clearly trace the statement of the need to efficiently control the activities of communication operators, first of all, in the sphere of the newly introduced standards providing cyber resilience; 3) regulation of relations in the sphere of managing the technical means of counteracting threats in Russia is characterized by their multiplicity, multi-leveledness,

© Russkevich E. A., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

hence, rather predictable complexity; 4) the model of communication operators' liability for violations in the field of exploitation of technical means of counteracting threats, implemented in Article 274.2 Of the Russian Criminal Code, is not optimal. Rather disputable is the approach to describing the administratively prejudicial elements of crime. Despite the significance of the relations, the possibility of a criminal-legal reaction to a particular incident appears not in connection with the occurrence of certain publicly dangerous consequences and not even with the traditional recurrence, but only with the third documented violation. We consider more preferable the model of criminalization of violating the management of technical means of counteracting threats depending on infliction of substantial harm to the rights and legal interests of citizens or organizations, or the legally protected interests of the society or the state.

Scientific novelty: the novelty of the research is mainly due to the actual underdevelopment of the issues related to the legal definition and implementation of criminal liability for violating the rules of centralized management of technical means of counteracting the threats to sustainability, security and integrity of functioning of the telecommunication network Internet and the general purpose communication network in the territory of the Russian Federation.

Practical significance: the main provisions and conclusions of the research can be used for improving the mechanism of criminal-legal protection of information security, further development of the Russian doctrine of criminal law on liability for crimes in the sphere of computer information.

For citation

Ruskevich, E. A. (2023). Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security. *Journal of Digital Technologies and Law*, 1(3), 650–672. <https://doi.org/10.21202/jdtl.2023.28>

References

- Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, 125, 103050. <https://doi.org/10.1016/j.cose.2022.103050>
- Bokshitskii, V., & Meltseva, I. (2017). Improving the protection of socially significant information resources. *Voprosy Kiberbezopasnosti*, S2(20), 11–14. (In Russ.).
- Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, 2019(4), 18–19. [https://doi.org/10.1016/S1353-4858\(19\)30051-0](https://doi.org/10.1016/S1353-4858(19)30051-0)
- Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, 34(6), 1180–1196. <https://doi.org/10.1016/j.clsr.2018.08.005>
- Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, 105, 102258. <https://doi.org/10.1016/j.cose.2021.102258>
- Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, 103, 102761. <https://doi.org/10.1016/j.cities.2020.102761>
- Dremliuga, R. I. (2022). *Criminal-legal protection of digital economy and information society against cybercriminal infringements: doctrine, law, law enforcement*: monograph. Moscow: Yurlitinform. (In Russ.).

- Dremliuga, R. I., Korobeev, A. I., & Fedorov, A. V. (2017). Cyberterrorism in China: Criminal Law and Criminological Aspects. *Russian Journal of Criminology*, 11(3), 607–614. (In Russ.). [https://doi.org/10.17150/2500-4255.2017.11\(3\).607-614](https://doi.org/10.17150/2500-4255.2017.11(3).607-614)
- Efremova, M. A. (2018). *Criminal-legal protection of information security*: monograph. Moscow: Yurlitinform. (In Russ.).
- Elchaninova, N. B. (2020). Protection of critical information infrastructure as a new institute of legally enforcing information security. *Information Society*, 2, 58–65. (In Russ.).
- Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, 55(10), 2252–2257. <https://doi.org/10.1016/j.ifacol.2022.10.043>
- Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, 11, 100204. <https://doi.org/10.1016/j.iot.2020.100204>
- Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, 128, 103158. <https://doi.org/10.1016/j.cose.2023.103158>
- Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, 61(6), 761–770. <https://doi.org/10.1016/j.scijus.2021.10.003>
- Khisamova, Z. I., & Begishev, I. R. (2022). Digital crime in the context of a pandemic: main trends. *Russian Journal of Criminology*, 16(2), 185–198. (In Russ.). [https://doi.org/10.17150/2500-4255.2022.16\(2\).185-198](https://doi.org/10.17150/2500-4255.2022.16(2).185-198)
- Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, 49, 105809. <https://doi.org/10.1016/j.clsr.2023.105809>
- Krasinsky, V. V., & Mashko, V. (2023). Cyberterrorism: criminological characteristics and qualification. *State and Law*, 1, 79–91. (In Russ.). <https://doi.org/10.31857/S102694520024122-5>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egyr.2021.08.126>
- Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, 53(4), 7–13. <https://doi.org/10.1016/j.ifacol.2021.04.001>
- Luzyanin, S. G., & Troshchinsky, P. V. (2018). Ensuring China's national security at the present stage (normative and legal aspect). *Journal of Foreign Legislation and Comparative Law*, 1, 60–69. (In Russ.). <https://doi.org/10.12737/art.2018.1.8>
- Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, 29(1), 66–76. <https://doi.org/10.1016/j.clsr.2012.11.005>
- Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, 40, 105521. <https://doi.org/10.1016/j.clsr.2020.105521>
- Pikurov, N. I. (2009). *Qualification of crimes with blanket characteristics of the components of crime*: monograph. Moscow: Russian State Academy of Justice. (In Russ.).
- Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, 55(10), 2246–2251. <https://doi.org/10.1016/j.ifacol.2022.10.042>
- Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, 128, 103127. <https://doi.org/10.1016/j.cose.2023.103127>
- Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, 40, 1591–1596. <https://doi.org/10.1016/j.trpro.2019.07.220>
- Truntsevsky, Yu. V. (2019). Unlawful impact on critical information infrastructure: the criminal liability of its owners and operators. *Journal of Russian Law*, 5(269), 99–106. (In Russ.). https://doi.org/10.12737/art_2019_5_9
- Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, 133, 102894. <https://doi.org/10.1016/j.adhoc.2022.102894>
- Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. *Discourse, Context & Media*, 51, 100666. <https://doi.org/10.1016/j.dcm.2022.100666>
- Zharova, A. K. (2022). The legal regulation of relations in the sphere of prevention of possible information technology vulnerabilities. *Bezopasnost biznesa*, 1, 19–26. (In Russ.). <https://doi.org/10.18572/2072-3644-2022-1-19-26>

Author information



Evgeniy A. Russkevich – Doctor of Juridical Sciences, Associate Professor, Professor of the Department of Criminal Law, Kutafin Moscow State Law University

Address: 9 Sadovaya-Kudrinskaya Str., 125993 Moscow, Russian Federation

E-mail: russkevich@mail.ru

ORCID ID: <https://orcid.org/0000-0003-4587-8258>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57919310600>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/2510065>

Google Scholar ID: <https://scholar.google.ru/citations?user=rwKPImlAAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research was performed as part of a state order «Russian legal system under the realities of digital transformation of the society and state: adaptation and prospects of reacting to the modern challenges and threats (FSMW-2023-0006)». Registration number: 1022040700002-6-5.5.1.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – February 6, 2023

Date of approval – April 13, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:342.3:004

EDN: <https://elibrary.ru/nfwlyf>

DOI: <https://doi.org/10.21202/jdtl.2023.29>

Суверенитет и цифровой суверенитет

Маргарита Роблес-Каррильо

Гранадский университет

г. Гранада, Королевство Испания

Ключевые слова

Безопасность,
государственная власть,
защищенность,
контекст,
концепция,
право,
суверенитет,
функции,
цифровая трансформация,
цифровой суверенитет,
цифровые технологии

Аннотация

Цель: анализ взаимоотношений между суверенитетом и цифровым суверенитетом и определение того, являются ли они взаимосвязанными или независимыми понятиями, а также в каких случаях и в какой степени прослеживается связь между данными категориями.

Методы: методология основана на анализе международной, европейской и государственной практики и научного дискурса, рассматривающего суверенитет и цифровой суверенитет с трех точек зрения: контекстуальной, концептуальной и функциональной.

Результаты: 1) анализ корреляции между суверенитетом и цифровым суверенитетом показал, что эти понятия взаимосвязаны; 2) определены важные следствия цифрового суверенитета для государств и Евросоюза в целом, а именно: а) между суверенитетом и цифровым суверенитетом существуют значительные отличия, поскольку первый относится только к государствам, тогда как второе понятие используется также по отношению к Евросоюзу; б) цифровой суверенитет не обязательно является следствием или продолжением обычного суверенитета; в) в случае отдельных государств цифровой суверенитет оправдан в качестве гарантии традиционного суверенитета, тогда как в случае Евросоюза его функция должна быть иной, поскольку Евросоюз не обладает суверенитетом.

Научная новизна: анализ данных взаимоотношений дает объективную научную базу для глубокого понимания концепции цифрового суверенитета. С точки зрения контекста, в котором действуют суверенитет и цифровой суверенитет, а также их концепций и функций эти категории представляются независимыми и в некоторых случаях взаимодополняющими.

© Роблес-Каррильо М., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Практическая значимость: дуальная функциональность цифрового суверенитета как понятия, тесно связанного с государственным суверенитетом, и как независимого понятия помогает объяснить использование этой категории по отношению к отдельным государствам и по отношению к такой организации, как Европейский союз, а также различия в масштабах и значении каждого из этих сценариев.

Для цитирования

Роблес-Каррильо, М. (2023). Суверенитет и цифровой суверенитет. *Journal of Digital Technologies and Law*, 1(3), 673–690. <https://doi.org/10.21202/jdtl.2023.29>

Содержание

Введение

1. Понятия суверенитета и цифрового суверенитета
2. Контекстуальный подход к определению корреляций между суверенитетом и цифровым суверенитетом
3. Концептуальный подход к определению корреляций между суверенитетом и цифровым суверенитетом
4. Функциональный подход к определению корреляций между суверенитетом и цифровым суверенитетом

Заключение

Список литературы

Введение

По ряду причин правовая и политическая категории суверенитета всегда были противоречивыми понятиями. В последнее время процессы глобализации и технификации бросают серьезный вызов суверенитету. Прежде всего, цифровая сфера оказывается средой, плохо пригодной для реализации суверенитета. В ней не существует границ, и она пересекается с другими физическими областями, размывая эффект географических границ. Хотя прошло уже немало времени после появления цифровой реальности, вопрос суверенитета в ней продолжает оставаться противоречивым. В 2020 г. вышла статья Мюллера «Против суверенитета в киберпространстве» (Muller, 2020), а в 2021 г. – статья К. Дж. Хеллера «В защиту чистого суверенитета в киберпространстве» (Heller, 2021). В ходе этих дискуссий возникло новое понятие: «цифровой суверенитет».

Идея цифрового суверенитета появилась в рамках политических, институциональных и научных дебатов на международном, национальном и общеевропейском уровнях. Несмотря на множество высококачественных научных работ по этому вопросу, до сих пор не достигнуто согласие относительно данной концепции, ее масштаба и значения, сущности и даже ее взаимоотношений с физическим суверенитетом. Действительно, цифровой суверенитет провозглашается как на уровне государств, так и на уровне Евросоюза, который не обладает свойством суверенности.

Цифровой суверенитет представляется не просто онлайн-версией принципа суверенитета (Chander & Sun, 2021; Franzese, 2009). Взаимоотношения между обычным и цифровым суверенитетом еще далеки от устоявшихся. Однако эта проблема требует решения; необходимо установить, являются ли данные понятия эквивалентными, дополняющими друг друга, независимыми друг от друга или это вообще разные понятия. Это станет первым шагом к пониманию концепции цифрового суверенитета.

В настоящей статье анализируются взаимоотношения между обычным и цифровым суверенитетом с трех взаимодополняющих точек зрения: контекстуальной, концептуальной и функциональной. Цель первого, контекстуального, подхода состоит в том, чтобы проанализировать, являются ли понятия обычного и цифрового суверенитетов эквивалентными, дополняющими друг друга, различными или независимыми друг от друга категориями цифровой сферы. Контекст играет значимую роль, потому что именно в нем выполняется принцип суверенитета и рождается идея цифрового суверенитета. С точки зрения второго подхода – концептуального – необходимо определить, существуют ли концептуальные сходства или различия между данными категориями. Цель третьего подхода – функционального – также определить, существуют ли сходства или различия между данными категориями в аспекте их функций и, более точно, почему необходим цифровой суверенитет, если существует обычный, и почему в отсутствие обычного суверенитета используется цифровой. Таким образом, вопрос в том, какую функцию выполняет цифровой суверенитет при наличии обычного и какая функция ему придается при отсутствии обычного суверенитета.

Вопросы цифрового суверенитета ставятся при анализе политических и институциональных разногласий и в научных исследованиях, главным образом в странах Евросоюза, где эти вопросы стали особенно актуальны в последнее время.

1. Понятия суверенитета и цифрового суверенитета

Суверенитет считается важнейшим принципом международного права, на котором основывается архитектура существующего правопорядка. Помимо того, что это важнейший структурный принцип международного права, это также максимальное выражение идентичности государства. Более того, государство и суверенитет – это два неразделимых понятия, закрепленных в Уставе Организации Объединенных Наций¹ и в ряде международных норм.

Во многих отношениях цифровой мир стал крупным вызовом принципу суверенитета. Он стал также вызовом государствам, которые испытывают негативное влияние процессов глобализации и приватизации. Более того, в экосистеме, где другие участники получили значительные преимущества, государства сохраняют и усиливают свою идентичность путем укрепления своего суверенитета. Суверенитет является эксклюзивным атрибутом государства и определяется как абсолютная, ограничительная и эксклюзивная власть. Это символ государства.

В данном контексте появление концепции цифрового суверенитета ставит различные новые вопросы. Эта концепция соблюдается различными странами с разнообразными целями и мотивами. Поддерживает ее и Евросоюз. Эта концепция

¹ Устав Организации Объединенных Наций. <https://www.un.org/en/about-us/un-charter/full-text>

провозглашается как Евросоюзом в целом, так и отдельными его членами без каких-либо противоречий и споров относительно ее использования в отношении Евросоюза, в отличие от обычного положения дел с принципом национального суверенитета. Между этими категориями прослеживаются как сходства, так и существенные различия. Значение выражения «цифровой суверенитет» представляется более широким, чем обычно передает сочетание прилагательного и существительного. Для понимания этой концепции необходимо проанализировать ее взаимоотношения с принципом суверенитета.

Проблема суверенитета обычно не оспаривается, но цифровой суверенитет рассматривается как отдельное, оригинальное и значимое понятие. Статус этих двух категорий и взаимоотношения между ними анализируются с контекстуальной, концептуальной и функциональной точек зрения.

2. Контекстуальный подход к определению корреляций между суверенитетом и цифровым суверенитетом

Почти три десятилетия назад, в 1996 г., Джон Перри Барлоу выпустил Декларацию независимости киберпространства, в которой провозглашалось отсутствие суверенитета в данной сфере². С тех пор в политических, институциональных и научных кругах не прекращаются дискуссии о суверенитете в киберпространстве. Однако в международной практике нет свидетельств существенных изменений понятия суверенитета, за исключением того факта, что ряд стран и организаций продвигают управленческие подходы с точки зрения множественных субъектов. По словам Mainwaring, «суверенитет и государственная власть изменены, но не уничтожены» (Mainwaring, 2020).

Задолго до прокламации Барлоу концепция суверенитета не исчезла, но была в большей или меньшей степени пересмотрена государствами. Кроме того, идея цифрового суверенитета стала главной темой политического, институционального и научного дискурсов.

Анализ этих дискурсов позволяет выдвинуть ряд предварительных соображений. Во-первых, цифровой суверенитет – это не просто онлайн-версия обычного суверенитета. Во-вторых, цифровой суверенитет не заменяет и не отменяет эту политико-правовую категорию. В-третьих, он не является ни следствием, ни расширением принципа суверенитета. На самом деле цифровой суверенитет составляет основу специфических правового, политического и научного дискурсов, далеко не всегда и не обязательно связанных с понятием физического суверенитета. Фактически аргументация этих концепций не всегда связана или родственна друг другу.

Следуя нарративу, отличному от нарратива цифрового суверенитета, принцип суверенитета выражается через утверждение себя в киберпространстве несколькими различными способами.

Во-первых, принцип киберсуверенитета утвердился в качестве модели управления, продвигаемой рядом стран и международных организаций, в первую очередь Китаем (Jiangyu & Huaer, 2022), Россией (Budnitsky & Jia, 2018) и Шанхайской

² Barlow, J. P. (1996). *Declaration on the Independence of Cyberspace*. <https://www.eff.org/cyberspace-independence>

организацией сотрудничества, а также в качестве альтернативы модели был поддержан Соединенными Штатами, странами Большой семерки и Евросоюзом³. По замечанию Flonk et al., это конфликт между суверенитаристами и либералами (Flonk et al., 2020).

Во-вторых, принцип суверенитета в отношении инфраструктур, сетей и систем, расположенных на территории государства, принят огромным большинством стран, а также согласован в рамках работы Групп правительственных экспертов и Рабочей группы открытого состава, утвержденных Генеральной Ассамблеей ООН для обсуждения прогресса в сфере ИКТ и международной безопасности (Christakis, 2020).

В-третьих, ряд государств ввели принцип киберсуверенитета при создании своего собственного цифрового пространства с целью обособиться и отделиться от общего цифрового пространства. Так, Китай создал так называемую Цифровую стену (Zeng et al., 2017), а Российская Федерация запустила Яндекс и Рунет (Budnitsky & Jia, 2018).

Фактически за этим процессом последовательного утверждения суверенитета в киберпространстве стоит несколько уровней мотивации (Kaloudis, 2021). Государства провозглашают его разными способами и с разной степенью интенсивности.

Нечто подобное происходит и с цифровым суверенитетом, поскольку не все государства, и даже не большинство из них преследуют одни и те же цели или стремятся достичь их одинаковым способом. Для защиты цифрового суверенитета существуют конкретные основания. Три главные из них определили Chander и Sun: «...во-первых, правительства выступают за цифровой суверенитет в целях защиты своего населения – например, стремясь удалить материалы, считающиеся незаконными в данной стране, или защитить права своих граждан в цифровом пространстве. <...> Во-вторых, правительства выступают за цифровой суверенитет в попытке развить собственную цифровую экономику, иногда вытесняя зарубежные корпорации, от финтеха до социальных сетей. В-третьих, правительства выступают за цифровой суверенитет в стремлении контролировать своих граждан – ограничивая то, что те могут говорить, читать или делать» (Chander & Sun, 2021). Не все страны преследуют одни и те же цели и не все делают это с одинаковой силой и последовательностью.

Более того, в данном контексте нет полного совпадения между теми, кто поддерживает принцип суверенитета в киберпространстве, и теми, кто выступает за цифровой суверенитет. Принцип киберсуверенитета поддерживают главным образом Китай, Российская Федерация и Шанхайская организация сотрудничества, тогда как концепцию цифрового суверенитета в основном продвигает Евросоюз среди стран Европы. При этом в любом случае, когда автократичные страны заявляют о цифровом суверенитете, их мотивация отличается от таковой демократических стран. По мнению Pohle, между ними существует фундаментальное отличие, поскольку «поддержание и усиление цифрового суверенитета в демократических странах является

³ Khawly, N., Arias-Oliva, M., & De Andrés, J. (2021). Technology and Geoeconomics: Emerging Conflicts in the Digital World. In Pelegrín Borondo, J. (coord.). *Moving technology ethics at the forefront of society, organisations and governments*. Universidad Complutense de Madrid and Universidad Rovira i Virgili. <https://repository.ukim.mk/bitstream/20.500.12188/14702/1/Dialnet-MovingTechnologyEthicsAtTheForefrontOfSocietyOrgan-829454.pdf>

эффективным средством сохранения либеральных ценностей и идей порядка в русле цифровой трансформации. Напротив, концепция суверенитета в авторитарных странах служит сохранению государственной власти и использует новые средства для поддержания авторитарных структур, подавляющих потенциальные демократические эффекты в цифровой сфере»⁴. Как отмечает Kaloudis, концепция суверенитета в авторитарных странах «также подкрепляется цифровым суверенитетом с целью обосновать авторитарно мотивированный суверенитет внутри страны и твердую экономическую и регулятивную политику вовне. Примерами таких стран являются Россия и Китай. Они характеризуются наличием цифровой автаркии, технологической изоляции и контроля над своими гражданами» (Kaloudis, 2021). Исследователь Ruohonen отмечает, что цифровой суверенитет давно стал «дубинкой геополитики, когда некоторые страны используют это понятие в своей политической риторике, стремясь оправдать усиление государственного контроля над Интернетом» (Ruohonen, 2021). По словам Crespi et al., цифровой, или технологический, суверенитет «воспринимается как националистическое понятие» (Crespi et al., 2021). Pohle и Thiel считают, что укрепление цифрового суверенитета предполагает «не только активное преодоление зависимости, но и создание инфраструктур для контроля и (возможно) манипулирования» (Pohle & Thiel, 2020). По мнению Fabiano, понятие цифрового суверенитета «имеет междисциплинарные коннотации и может принимать различные значения или описывать несколько аспектов, в зависимости от контекста, в котором о нем говорится» (Fabiano, 2020).

С контекстуальной точки зрения, суверенитет и цифровой суверенитет имеют различные сферы применения и подходы. Кроме того, суверенитет – это общий принцип, обладающий равным объемом и значением повсюду и для всех государств, тогда как цифровой суверенитет может пониматься по-разному. В соответствии с доктриной и практикой, особенно при сравнении демократических и авторитарных стран, различные контексты применения цифрового суверенитета изменяют его функции и содержание данного понятия.

3. Концептуальный подход к определению корреляций между суверенитетом и цифровым суверенитетом

Хотя принцип суверенитета определяется по-разному (Brack et al., 2019), в целом все согласны, что это понятие подразумевает абсолютную, ограничительную и эксклюзивную власть государства. В случае цифрового суверенитета ситуация иная. По словам Prokscha, «из-за повсеместного использования понятия цифрового суверенитета оно часто концептуализируется вне научного сообщества, что приводит к смешению терминологии. В результате понятие цифрового суверенитета ассоциируется с различными чертами, от регулирования данных, сервисов и алгоритмов до контроля над аппаратными устройствами и инфраструктурой, и различается в зависимости от контекста, смысла и назначения... Таким образом, понятие цифрового суверенитета является подвижным, его коннотации и предполагаемые

⁴ Pohle, J. (2020). *Digital sovereignty. A new key concept of digital policy in Germany and Europe*. Konrad Adenauer-Stiftung. <https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf>

эффекты часто меняются»⁵. Как отмечает Elms, понятие цифрового суверенитета «нечеткое по своей природе» (Elms, 2021). В этом смысле Allen выражал озабоченность тем, что это понятие «используется для прикрытия других политических целей: ряд критиков описывают его как призрак, что бродит по Европе, и Троянского коня протекционизма»⁶.

С концептуальной точки зрения возникают две различные, хотя и взаимосвязанные проблемы: определение цифрового суверенитета и необходимость различения его с аналогичными концепциями, такими как технологический или стратегический суверенитет.

Что касается первого вопроса, цифровой суверенитет определяется как власть, как способность, как простая автономия или с аксиологической точки зрения. Первой позиции придерживаются Chander и Sun, для которых цифровой суверенитет «должен быть определен широко, объединяя суверенную власть государства, регулирующего не только трансграничные потоки данных с помощью ограничивающих технологий Интернета и мандатов на локализацию данных, но также самовыражение и доступ к технологиям» (Chander & Sun, 2021). Эти авторы считают цифровой суверенитет продолжением традиционного. Сторонник второй позиции Posch определяет цифровой суверенитет как «способность человека или общества обладать полным знанием и контролем над тем, куда передаются данные и кто имеет к ним доступ» (Posch, 2015). К третьей группе принадлежат такие авторы, как Crespi et al., которые признают, что понятие суверенитета много раз переформулировалось, но «все больше используется для описания различных форм независимости, автономии и контроля над цифровыми технологиями и содержанием» (Crespi et al., 2021). Наконец в рамках аксиологического подхода термин «цифровой суверенитет» «используется по отношению к упорядоченной, ценностной, регулируемой и безопасной цифровой сфере, отвечающей требованиям индивидуальных прав и свобод, равенства и справедливой экономической конкуренции»⁷. Как можно видеть, лишь одно направление научной литературы, а именно первое из упомянутых, связывает понятие цифрового суверенитета с классическим принципом суверенитета.

Более того, согласно докладу, опубликованному во время председательства Германии в Европейском союзе, цифровой суверенитет «представляет собой не четко определенную концепцию, а скорее политическое видение соответствующего социально-экономического порядка. Оно в основном направлено на сокращение существующих и будущих зависимостей в цифровизированном мире»⁸.

⁵ Prokscha, A. (2021, June). *Digital Sovereignty for the European Union - Analysing Frames and Claims for Digital Sovereignty in the European Union's Digital Strategy*. https://www.researchgate.net/publication/354888060_Digital_Sovereignty_for_the_European_Union_-_Analysing_Frames_and_Claims_for_Digital_Sovereignty_in_the_European_Union%27s_Digital_Strategy

⁶ *European Sovereignty In the Digital Age*. (2021, July 19). https://www.iiea.com/images/uploads/resources/European_Sovereignty_in_the_Digital_Age.pdf

⁷ *European Digital Sovereignty*. Institute of European Democrats. <https://www.iedonline.eu/download/2021/IED-Research-Paper-Innerarity.pdf>

⁸ *Report of German Presidency on Digital Sovereignty*. https://erstelesung.de/wp-content/uploads/2020/10/20-10-14_Germany_EU_Digital-Sovereignty.pdf

Фактически не существует единого или превалирующего определения цифрового суверенитета, нет и консенсуса по поводу самого термина. Наряду с термином «цифровой суверенитет», говорят также о технологическом или стратегическом суверенитете; эти термины часто используются как альтернативные, объединяющие или взаимозаменяющие.

Существует мнение, что их нельзя использовать как синонимы, так как каждый представляет «один из аспектов единой, более широкой концепции цифрового суверенитета»⁹. По словам Pohle и Thiel, понятие цифрового суверенитета «стало гораздо более всеохватывающим, относящимся не только к вопросам коммуникации в Интернете и связи, но и к более широким вопросам цифровой трансформации обществ» (Pohle & Thiel, 2020). Burwell и Propp также признают, что концепция цифрового суверенитета значительно расширилась, «включив в себя сильную инновационную промышленную базу и достаточные меры кибербезопасности»¹⁰. Поддерживая эту идею, Edler et al. определяют технологический суверенитет как «способность государства или федерации государств обеспечить технологии, которые оно считает необходимыми для своего благополучия, конкурентоспособности и дееспособности, а также способность развивать их или получать их из других экономических областей без возникновения односторонней структурной зависимости»¹¹. Напротив, Csernatonì считает, что «цифровой суверенитет по большому счету является лишь очередным вариантом технологического суверенитета от внешних игроков в киберпространстве», основанным на трех неразделимых столпах: вычислительные мощности, контроль над данными и безопасные соединения»¹².

Как показывает практика, различные определения используются в целом как взаимозаменяемые, особенно в Евросоюзе. Однако с точки зрения логики и согласно мнению большинства ученых, цифровой суверенитет должен пониматься как более широкое и общее понятие, а технологический суверенитет – как его компонент, нацеленный на сущностные аспекты; при этом понятие стратегического суверенитета должно передавать конкретный политический аспект цифрового суверенитета как целого.

В настоящее время, как можно видеть, в науке цифровой суверенитет в основном определяется как понятие, отличное от традиционного суверенитета. Однако ни относительно самой концепции, ни относительно терминологии консенсус пока не достигнут. Кроме того, в отличие от принципа суверенитета, не достигнут консенсус и по поводу функций и назначения цифрового суверенитета.

⁹ *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study*. Istituto Affari Internazionali (IAI), Roma. <https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study>

¹⁰ Burwell, F. G., & Propp, K. (2020). *The European Union and the Search for Building "Fortress Europe" or Preparing for a New World?* <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>

¹¹ Edler, J., Blind, K., Frietsch, R., Kimpeler, S., Kroll, H., Lerch, Ch., Reiss, T., Roth, F., Schubert, T., Schuler, J., & Walz, R. (2020). *Technology sovereignty from demand to concept*. Fraunhofer Institute for Systems and Innovation Research. https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technology_sovereignty.pdf

¹² Csernatonì, R. (2021). *The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty*. Carnegie Europe Program. <https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134>

4. Функциональный подход к определению корреляций между суверенитетом и цифровым суверенитетом

Суверенитет является абсолютным, ограничительным и эксклюзивным принципом, выделяющим верховную власть среди других видов власти. В таком качестве суверенитет – это власть, которая может осуществляться независимо от окружения, физического или виртуального, и ее нет необходимости дополнять цифровой версией или цифровым измерением. Следовательно, необходимо поставить вопросы «как» и «почему» относительно цифрового суверенитета. Действительно, зачем нужен цифровой суверенитет, если уже существует обычный суверенитет? Что добавляет цифровой суверенитет и для чего он нужен, если обычный суверенитет отсутствует? На эти вопросы нет простого ответа. Два различных примера использования цифрового суверенитета при наличии и при отсутствии обычного суверенитета представляют Франция и Евросоюз.

Франция утверждает принцип цифрового суверенитета в качестве базового принципа своей политики как на внутригосударственном, так и на европейском уровне. На первом уровне цифровой суверенитет воспринимается как необходимая предпосылка гарантии государственного суверенитета¹³. В контексте Евросоюза смысл понятия становится совершенно иным, поскольку оно не связано с государственным суверенитетом в истинном и традиционном смыслах, что подтверждают многогранность и функциональность данной категории.

На совместном заседании министров 7 апреля 2016 г. Франция и Германия обосновали необходимость укрепления европейского цифрового суверенитета на основе трех главных принципов:

1. Укрепление способности стран – членов ЕС защищать свои сети и усиливать цифровую устойчивость.
2. Развитие независимой, инновационной, эффективной и диверсифицированной промышленности на общеевропейском уровне, в особенности в областях кибербезопасности и надежности цифровых продуктов.
3. Способность европейцев независимо определять уровень безопасности своих данных, в особенности в контексте переговоров по торговым соглашениям¹⁴.

В октябре 2020 г. Европейский совет постановил, что «для достижения цифрового суверенитета ЕС должен выстроить по-настоящему единый цифровой рынок, укрепить свою способность определять собственные нормы, принимать независимые технологические решения, развивать и применять стратегические цифровые возможности и инфраструктуру. На международном уровне ЕС будет активизировать свои нормативные инструменты и компетенции с целью способствовать выработке глобальных норм и стандартов»¹⁵. В заявлении членов Европейского совета

¹³ Aktoudianakis, A. (2020, December). *Digital sovereignty for growth, rules and cooperation*. European Policy Centre. Konrad Adenauer Stiftung. https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

¹⁴ *The European digital sovereignty: a common objective for France and Germany*. <https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany>

¹⁵ *European Council Conclusions*. <https://www.consilium.europa.eu/en/press/press-releases/2021/10/22/european-council-conclusions-21-22-october-2021>

от 21 марта 2021 г. была непосредственно выражена «необходимость решительно и открыто усилить цифровой суверенитет Европы, опираясь на ее сильные стороны и сокращая недостатки, а также используя разумные и выверенные меры для сохранения открытых рынков и глобального сотрудничества»¹⁶. Согласно совместному заявлению по политике ЕС в области киберобороны, опубликованному в декабре 2022 г., ЕС должен обеспечить «свой технологический и цифровой суверенитет в киберпространстве. Дееспособность ЕС будет зависеть от его способности осваивать и развивать новейшие технологии кибербезопасности и киберобороны на территории Евросоюза»¹⁷. Как отмечает Christakis, сам факт того, что Евросоюз говорит о суверенитете, «довольно загадочен <...>. В наши дни политики Европы и Евросоюза удивительно много выступают за цифровой или технологический суверенитет» (Christakis, 2020).

Эти примеры показывают, что идея цифрового суверенитета стала частью европейского дискурса, хотя, как хорошо известно, ЕС не обладает признаком суверенитета, который сохраняется за его членами. Очевидный вывод – цифровой суверенитет не зависит от обладания суверенитетом и не влияет на суверенитет государства.

Установлено, что цифровой суверенитет ЕС основывается на трех потребностях: «1. ЕС должен вкладывать средства в создание ценностей путем разработки технологий и важнейшей инфраструктуры. 2. ЕС должен разработать конкретный список долгосрочных руководящих принципов цифровой политики на основе демократических ценностей и прав человека, определить направление и цель существующим правовым нормам и проектам. 3. ЕС должен выработать стратегии, опирающиеся на глобальное сотрудничество, а не пытаться оградить Европу от внешнего мира»¹⁸. Как считают Burwell и Propp, нынешняя сосредоточенность Европы на проблеме цифрового суверенитета «коренится в более общей дискуссии о способности Европы защитить своих граждан от все более враждебного и сложного окружения»¹⁹. По словам Siebert, «разговор о цифровом суверенитете имеет также геополитическое измерение. Зависимость от США и Китая в области цифровых технологий долгое время не воспринималась в Европе как проблема. Однако в период правления Трампа отношения между США и Китаем стали более напряженными, и Европа рискует оказаться между двух огней»²⁰. Цифровой суверенитет стал пониматься как «средство продвижения понятия о лидерстве и стратегической независимости Европы в цифровой об-

¹⁶ Statement of the members of the European Council. <https://www.consilium.europa.eu/en/press/press-releases/2021/03/25/statement-of-the-members-of-the-european-council-25-march-2021>

¹⁷ EU Policy on Cyber Defense. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

¹⁸ Obendiek, A. (2021, May 11). *Take back control? Digital sovereignty and a vision for Europe*. Policy Paper. Hertie School. Jacques Delors Center. https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/6_Jacques_Delors_Centre/Publications/20210511_Policy-Paper_Obendiek_Digital-Sovereignty__1_.pdf

¹⁹ Burwell, F. G., & Propp, K. (2020). *The European Union and the Search for Building "Fortress Europe" or Preparing for a New World?* <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>

²⁰ *Digital Sovereignty – The EU in a Contest for Influence and Leadership*. The Green Political Foundation, <https://www.boell.de/en/2021/02/10/digital-sovereignty-eu-contest-influence-and-leadership>

ласти»²¹. Как писали Irion et al., «стремясь к цифровому суверенитету, ЕС использует новую решительную риторику, сопоставляя свой ценностный подход с более рыночно ориентированным подходом США и государственно ориентированной иерархией Китая» (Irion et al., 2021). Аналогичным образом цифровой суверенитет ЕС увязывается с глобальной борьбой за модель цифровизации. Китай, США, Россия и Евросоюз оказались сегодня на поле битвы за различные модели цифровизации, в которой определяются будущие глобальные рынки и законодательные нормы. Речь идет о концепциях защиты частной жизни, прав человека, платформенной экономики и в конечном итоге взаимоотношений рынков, государств и обществ. Кратко говоря, существуют различные толкования европейского цифрового суверенитета, но ни одно из них не связано с традиционным суверенитетом.

Более того, использование термина «цифровой суверенитет» как взаимозаменяемого в государственном и общеевропейском контекстах показывает, во-первых, что существует значительная разница между концепциями суверенитета и цифрового суверенитета. Первый может применяться только к государствам, тогда как второй также используется по отношению к ЕС, следовательно, он не является ограничительной или эксклюзивной категорией. Во-вторых, в той мере, в какой понятие цифрового суверенитета применяется к отдельным государствам, обладающим суверенитетом, и к международной организации, не обладающей таковым, оно не обязано быть ни следствием, ни расширением суверенитета в традиционном смысле. В-третьих, если в случае отдельных государств цифровой суверенитет оправдан в качестве гарантии традиционного суверенитета, то в случае Евросоюза его функция должна быть иной, поскольку Евросоюз не обладает суверенитетом. В этом аспекте, как поясняет Floridi, обсуждение цифрового суверенитета в ЕС идет «не в смысле замены национального суверенитета в современном понимании, который является необходимым, но все более недостаточным. Оно касается дополнения этого суверенитета наднациональным, современным цифровым суверенитетом» (Floridi, 2020). В работе Roberts et al. отмечено, что это обсуждение является «сигналом о намерениях и отражением актуальной политической повестки внутри ЕС. Цифровой суверенитет рассматривается как основа для укрепления роли Евросоюза во взаимосвязанном мире, продвижения его насущных интересов, защиты фундаментальных ценностей, на которых он был основан, а именно человеческого достоинства, свободы, демократии, равенства, главенства закона и соблюдения прав человека» (Roberts et al., 2021).

Заключение

Отношения между суверенитетом и цифровым суверенитетом непросты. С контекстуальной точки зрения это независимые категории. В цифровом контексте нет совпадения между государствами, которые поддерживают принцип суверенитета в киберпространстве, и теми, кто выступает за цифровой суверенитет. Более того, когда первые заявляют о цифровом суверенитете, их мотивация и содержание данного понятия отличаются. Если суверенитет – это общий принцип, обладающий

²¹ Towards a more resilient EU. Digital sovereignty for Europe. *EPRS Ideas Paper*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

равным объемом и значением повсюду и для всех государств, то цифровой суверенитет понимается по-разному в разных странах и ситуациях. Различные контексты применения цифрового суверенитета изменяют его функции и содержание.

С концептуальной точки зрения цифровой суверенитет определяется как власть, как способность, как автономия, а также он может идентифицироваться с аксиологической точки зрения. Хотя консенсус в отношении этой концепции еще не достигнут, в большинстве случаев определение цифрового суверенитета не связано с принципом суверенитета.

С функциональной точки зрения в отличие от принципа суверенитета не достигнут консенсус по поводу функций и назначения цифрового суверенитета. Однако стремление к достижению цифрового суверенитета как отдельных государств, так и Евросоюза в целом имело ряд важных последствий.

Во-первых, существует значительная разница между концепциями суверенитета и цифрового суверенитета, поскольку первый может применяться только к государствам, тогда как второй также используется по отношению к ЕС.

Во-вторых, в той мере, в какой понятие цифрового суверенитета применяется к отдельным государствам, обладающим суверенитетом, и к международной организации, не обладающей таковым, оно не обязано быть ни следствием, ни расширением суверенитета в традиционном смысле.

В-третьих, если в случае отдельных государств цифровой суверенитет оправдан в качестве гарантии традиционного суверенитета, то в случае Евросоюза его функция должна быть иной, поскольку Евросоюз не обладает суверенитетом. Существуют различные толкования европейского цифрового суверенитета, но ни одно из них не связано с традиционным суверенитетом. Следовательно, функции, приписываемые суверенитету и цифровому суверенитету, различны, а функции цифрового суверенитета также несколько различаются в случае отдельных государств и Евросоюза в целом.

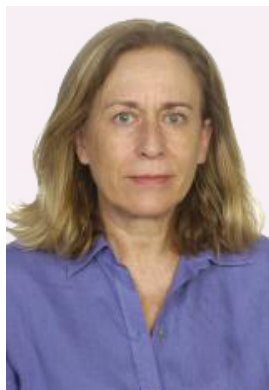
Категория цифрового суверенитета возникла и развивалась как дополняющая по отношению к национальному суверенитету отдельных государств и как независимая категория по отношению к ЕС. Таким образом, она является следствием или расширением принципа суверенитета только в отношении государств, но не в общем смысле. В любом случае цифровой суверенитет – это не просто онлайн-версия традиционного суверенитета, он не заменяет и не отменяет принцип суверенитета. Цифровой суверенитет имеет ряд отличий от физического суверенитета с контекстуальной, концептуальной и функциональной точек зрения, и его следует рассматривать как независимую категорию знаний.

Список литературы

- Brack, N., Coman, R., & Crespy, A. (2019). Unpacking old and new conflicts of sovereignty in the European polity. *Journal of European Integration*, 41(7), 817–832. <https://doi.org/10.1080/07036337.2019.1665657>
- Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613. <https://doi.org/10.1177/1367549417751151>
- Crespi, F., Caravella, S., Menghini, M., & Salvatori, Ch. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics. Review of European Economic Policy*, 56(6), 348–354. <https://doi.org/10.1007/s10272-021-1013-6>
- Chander, A., & Sun, H. (2021). *Sovereignty 2.0*. Georgetown University Law Center. <http://dx.doi.org/10.2139/ssrn.3904949>

- Christakis, T. (2020). "European Digital Sovereignty": Successfully Navigating Between the Brussels Effect and Europe's Quest for Strategic Autonomy. *Studies of Digital Governance*. Data institute. Université Grenoble Alpes. <https://ai-regulation.com/european-digital-sovereignty-successfully-navigating-between-the-brussels-effect-and-europes-quest-for-strategic-autonomy/>
- Elms, D. (2021). *Digital Sovereignty: protectionism or autonomy*. Hinrich foundation, Asian Trade Centre.
- Fabiano, N. (2020). Digital Sovereignty Between "Accountability" and the Value of Personal Data. *Advances in Science, Technology and Engineering Systems Journal*, 5(3), 270–274. <https://doi.org/10.25046/aj050335>
- Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, 9(2), 364–386. <https://doi.org/10.1017/S2045381720000167>
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU. *Philosophy & Technology*, 33, 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist? *The Air Force Law Review*; Maxwell AFB, 64, 1–42. <https://www.proquest.com/docview/195182873>
- Heller, K. J. (2021). In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, 97, 1432–1499. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2987&context=ils>
- Irion, K., Burri, M., Kolk, A., & Milan, S. (2021). Governing "European values" inside data flows: interdisciplinary perspectives. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1582>
- Jiangyu, W., & Huaer, Che. (2022). China's Approach to International Law: From Traditional Westphalianism to Aggressive Instrumentalism in the Xi Jinping Era. *The Chinese Journal of Comparative Law*, 10(1), 140–153. <https://doi.org/10.1093/cjcl/cxac020>
- Kaloudis, M. (2021). Digital sovereignty – European Union's action plan needs a common understanding to succeed. *History Compass*, 8. <https://doi.org/10.1111/hic3.12698>
- Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, 5(2), 215–232. <https://doi.org/10.1017/eis.2020.4>
- Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, 22(4), 779–801. <https://doi.org/10.1093/isr/viz044>
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Posch, R. (2015). Digital Sovereignty and IT-Security for a Prosperous Society. En Werthner, H. y Van Harmelen, F. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit (ECSS 2015)*. Vienna. https://doi.org/10.1007/978-3-319-55735-9_7
- Roberts, H., Cows, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1575>
- Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, 31, 439–456. <https://doi.org/10.48550/arXiv.2012.02724>
- Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty". *Politics & Policy*, 45(3), 432–464. <https://doi.org/10.1111/polp.12202>

Сведения об авторе



Маргарита Роблес-Каррильо – доктор наук, профессор международного и европейского права, Группа сетевых технологий и безопасности, Гранадский университет

Адрес: Королевство Испания, г. Гранада, Университетская площадь, 1, CP:18071

E-mail: mrobles@ugr.es

ORCID ID: <https://orcid.org/0000-0002-6324-4665>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57203316304>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/ADD-1696-2022>

Google Scholar ID: <https://scholar.google.ru/citations?user=PSUjIYgAAAAJ>

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Работа выполнена при поддержке Министерства экономики и конкурентоспособности Правительства Испании в рамках проекта TIN2017-83494-R Европейского фонда регионального развития.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.15.41 / Государственный суверенитет

Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 2 февраля 2023 г.

Дата одобрения после рецензирования – 30 апреля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.29>

Sovereignty vs. Digital Sovereignty

Margarita Robles-Carrillo

University of Granada
Granada, Spain

Keywords

Concept,
context,
digital sovereignty,
digital technologies,
digital transformation,
functions,
law,
safety,
security,
sovereignty,
state power

Abstract

Objective: the aim of this paper is to analyze the relationship between sovereignty and digital sovereignty in order to determine whether they are linked or autonomous concepts and in which cases and to what extent there is or is not a connection between the two categories.

Methods: the methodology is based on the analysis of international, European and national practice and scientific discourse, taking into account sovereignty and digital sovereignty from a threefold perspective: contextual, conceptual and functional.

Results: 1) analysis of the correlation between sovereignty and digital sovereignty showed that both are related concepts; 2) important consequences that digital sovereignty has in the case of States and the European Union are defined: a) there is a substantial difference between sovereignty and digital sovereignty because the former is only applied to States, while the latter is also used in reference to the EU; b) digital sovereignty is not necessarily a consequence or an extension of sovereignty; c) while in the case of States, digital sovereignty is justified as a safeguard of traditional sovereignty, in case of European Union its function must necessarily be different, since the European Union lacks sovereignty.

Scientific novelty: the analysis of this relationship provides an objective scientific premise for a comprehensive understanding of the idea of digital sovereignty. From the perspective of the context where they operate, as well as their concept and functions, sovereignty and digital sovereignty seem to be autonomous and, in some cases, complementary categories.

© Robles-Carrillo M., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Practical significance: the dual functionality of digital sovereignty as a concept attached to national sovereignty and as an autonomous concept helps to explain the use of this category in the case of states and in the case of an organization such as the European Union, as well as the differences in its scope and meaning in each scenario.

For citation

Robles-Carrillo, M. (2023). Sovereignty vs. Digital Sovereignty. *Journal of Digital Technologies and Law*, 1(3), 673–690. <https://doi.org/10.21202/jdtl.2023.29>

References

- Brack, N., Coman, R., & Crespy, A. (2019). Unpacking old and new conflicts of sovereignty in the European polity. *Journal of European Integration*, 41(7), 817–832. <https://doi.org/10.1080/07036337.2019.1665657>
- Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613. <https://doi.org/10.1177/1367549417751151>
- Crespi, F., Caravella, S., Menghini, M., & Salvatori, Ch. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics. Review of European Economic Policy*, 56(6), 348–354. <https://doi.org/10.1007/s10272-021-1013-6>
- Chander, A., & Sun, H. (2021). *Sovereignty 2.0*. Georgetown University Law Center. <http://dx.doi.org/10.2139/ssrn.3904949>
- Christakis, T. (2020). “European Digital Sovereignty”: Successfully Navigating Between the Brussels Effect and Europe’s Quest for Strategic Autonomy. *Studies of Digital Governance*. Data institute. Université Grenoble Alpes. <https://ai-regulation.com/european-digital-sovereignty-successfully-navigating-between-the-brussels-effect-and-europes-quest-for-strategic-autonomy/>
- Elms, D. (2021). *Digital Sovereignty: protectionism or autonomy*. Hinrich foundation, Asian Trade Centre.
- Fabiano, N. (2020). Digital Sovereignty Between “Accountability” and the Value of Personal Data. *Advances in Science, Technology and Engineering Systems Journal*, 5(3), 270–274. <https://doi.org/10.25046/aj050335>
- Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2020). Authority conflicts in internet governance: Liberals vs. sovereignists? *Global Constitutionalism*, 9(2), 364–386. <https://doi.org/10.1017/S2045381720000167>
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU. *Philosophy & Technology*, 33, 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist? *The Air Force Law Review; Maxwell AFB*, 64, 1–42. <https://www.proquest.com/docview/195182873>
- Heller, K. J. (2021). In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, 97, 1432–1499. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2987&context=ils>
- Irion, K., Burri, M., Kolk, A., & Milan, S. (2021). Governing “European values” inside data flows: interdisciplinary perspectives. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1582>
- Jiangyu, W., & Huaer, Che. (2022). China’s Approach to International Law: From Traditional Westphalianism to Aggressive Instrumentalism in the Xi Jinping Era. *The Chinese Journal of Comparative Law*, 10(1), 140–153. <https://doi.org/10.1093/cjcl/cxac020>
- Kaloudis, M. (2021). Digital sovereignty – European Union’s action plan needs a common understanding to succeed. *History Compass*, 8. <https://doi.org/10.1111/hic3.12698>
- Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, 5(2), 215–232. <https://doi.org/10.1017/eis.2020.4>
- Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, 22(4), 779–801. <https://doi.org/10.1093/isr/viz044>
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>

- Posch, R. (2015). Digital Sovereignty and IT-Security for a Prosperous Society. En Werthner, H. y Van Harmelen, F. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit (ECSS 2015)*. Vienna. https://doi.org/10.1007/978-3-319-55735-9_7
- Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1575>
- Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, 31, 439–456. <https://doi.org/10.48550/arXiv.2012.02724>
- Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty". *Politics & Policy*, 45(3), 432–464. <https://doi.org/10.1111/polp.12202>

Author information



Margarita Robles-Carrillo – PhD, Full Professor of International Law and European Law, Network Engineering & Security Group, University of Granada

Address: Plaza de la Universidad, 1, CP:18071, Granada, Spain

E-mail: mrobles@ugr.es

ORCID ID: <https://orcid.org/0000-0002-6324-4665>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57203316304>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/ADD-1696-2022>

Google Scholar ID: <https://scholar.google.ru/citations?user=PSUjIYgAAAAJ>

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

This work is supported by the Spanish Government-MINECO (Ministerio de Economía y Competitividad), using the Fondo Europeo de Desarrollo Regional (FEDER), under Project TIN2017-83494-R.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – February 2, 2023

Date of approval – April 30, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:347.469:004

EDN: <https://elibrary.ru/ozhvue>

DOI: <https://doi.org/10.21202/jdtl.2023.30>

Особенности онлайн-урегулирования потребительских споров платформами электронной торговли в Китайской Народной Республике

Елена Петровна Ермакова

Российский университет дружбы народов имени Патриса Лумумбы
г. Москва, Российская Федерация

Ключевые слова

Таобао,
интернет-магазин,
онлайн-разрешение споров,
онлайн-урегулирование
споров,
покупатель,
право,
продавец,
суд,
цифровые технологии,
электронная торговля

Аннотация

Цель: исследование особенностей онлайн-урегулирования споров платформами электронной торговли в Китайской Народной Республике, выявление положительных черт и недостатков технологий ODS, применяемых платформами.

Методы: эмпирические методы сравнения, описания, интерпретации; теоретические методы формальной и диалектической логики, а также частно-научные методы: юридико-догматический и метод толкования правовых норм.

Результаты: выявлено, что внутренняя модель ODS на платформах электронной торговли Таобао ODS является прямым, ясным и эффективным способом онлайн-разрешения потребительских споров. Однако, будучи не независимой «третьей стороной», внутренний механизм ODS платформ электронной торговли никогда не сможет заменить другие внешние системы разрешения споров. ODS полагается на данные и интернет-процессы гораздо больше, чем традиционное разрешение споров. Среди многих факторов безопасности, возникающих в результате онлайн-процессов, ODS создает риски утечки данных, отсутствия конфиденциальности и небезопасной защиты потребителей. ODS также вызывает серьезную озабоченность в связи с традиционными принципами правосудия, такими как принципы беспристрастности, конфиденциальности и безопасности данных в процессе урегулирования споров. Не только Китайской Народной Республике, но и любой стране мира, внедряющей технологии ODS в процедуры разрешения споров, необходимо предпринять важные шаги для обеспечения того, чтобы процессы ODS были справедливыми, непредвзятыми и гарантировали процессуальные права.

© Ермакова Е. П., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: состоит в комплексном исследовании онлайн-урегулирования споров платформами электронной торговли в Китайской Народной Республике, практика применения которых имеет свою специфику, вытекающую из модели саморегулирования указанных отношений, закреплённой впоследствии нормативными правовыми актами Китайской Народной Республики и отражающейся в деятельности частных платформ ODS.

Практическая значимость: обусловлена отсутствием в настоящее время возможности применения к отношениям, использующим технологии ODS на частных платформах правовых норм и правил, учитывающих их специфику. Основные положения и выводы исследования могут быть использованы для совершенствования механизмов правового регулирования технологий ODS в процессуальном законодательстве Российской Федерации.

Для цитирования

Ермакова, Е. П. (2023). Особенности онлайн-урегулирования потребительских споров платформами электронной торговли в Китайской Народной Республике. *Journal of Digital Technologies and Law*, 1(3), 691–711. <https://doi.org/10.21202/jdtl.2023.30>

Содержание

Введение

1. Особенности урегулирования споров на платформе Taobao ODS
2. Характеристики технологии Taobao ODS
 - 2.1. Модульность конструкции платформы Taobao ODS
 - 2.2. Строгое соблюдение сроков, установленных внутренними регламентами разрешения споров
 - 2.3. Совпадение характеристик электронной торговли и платформы Taobao ODS
 - 2.4. Социальное участие для создания «экосистемы электронной торговли»
3. Сравнение практики разрешения споров между различными платформами ODS (государственным судом, арбитражем, частными платформами электронной торговли)
 - 3.1. Преимущества ODR
 - 3.2. Срок рассмотрения спора и постановки решения для платформ ODS
 - 3.3. Возможность внедрения в Российской Федерации
4. Недостатки в работе платформы Taobao ODS
 - 4.1. Не независимость третьей стороны при разрешении спора на частной платформе ODR
 - 4.2. Предвзятость технологий искусственного интеллекта в системах ODR
 - 4.3. Безопасность данных
 - 4.4. Необходимость строгого законодательного регулирования

Выводы

Список литературы

Введение

В 2021 г. на долю Китайской Народной Республики (далее – Китай, КНР) пришлось более 37 % мирового рынка электронной торговли с точки зрения объема платежей (по количеству транзакций – более 50 %). Ожидается, что китайский рынок электронной торговли, который на данный момент стал крупнейшим в мире, продемонстрирует уверенный рост в 2022 г. и достигнет 14,5 трлн юаней (2,3 трлн долл.), прогнозирует агентство GlobalData. Статистические отчеты утверждают, что китайские и зарубежные потребители товаров на площадках электронной торговли Китая все чаще переходят из офлайна в онлайн. Пандемия COVID-19 еще больше ускорила деятельность электронной торговли в Китае, поскольку осторожные потребители все чаще используют онлайн-канал для покупок, чтобы избежать контакта с переносчиками болезней, и эта тенденция сохраняется и после пандемии, утверждал Р. Шарма, ведущий аналитик GlobalData¹. Ожидается, что на китайском рынке электронной торговли среднегодовой темп роста составит 11,3 % в период с 2022 по 2027 г. Основными факторами, стимулирующими рост рынка электронной торговли в регионе, являются: культура мобильной торговли, основанная на смартфонах; инновационные системы цифровых платежей и растущие платформы для онлайн-торговли.

Бум электронной торговли принес десятки миллионов споров на площадках электронной торговли – интернет-платформах. Безусловно, ни в одной стране мира не было ни миллиона арбитров, ни миллиона медиаторов для разрешения указанных споров. Так, на платформах онлайн-торговли, первоначально в Соединенных Штатах Америки и Европе (eBay, Amazon), затем в Китае (Alibaba) стихийно, без нормативного регулирования со стороны государства, стали появляться платформы онлайн-урегулирования споров. Как отмечали Э. Катш и О. Рабинович-Эйни в 2018 г., платформа eBay, например, сообщила, что рассматривает более 60 млн споров в год через свою систему ODR; китайский гигант электронной коммерции Alibaba рассказал о сотнях миллионов споров в год. Некоторые из этих споров возникают по отношению к платформе, в то время как другие – с другими пользователями. Подавляющее большинство этих споров никогда не дойдут до судов или ADR: они связаны с небольшими суммами денег и требуют быстрого, доступного и эффективного урегулирования. Характеристики онлайн-споров часто делают их плохо подходящими для традиционных механизмов разрешения споров офлайн, а именно судов и альтернативного разрешения споров (ADR). Необходимость найти надлежащий способ для урегулирования онлайн-споров возникла в середине 1990-х гг., когда Интернет открылся для торговли (Katsh & Rabinovich-Einy, 2018).

Известный американский практик К. Рул, директор департамента ODR Modria, а также eBay и PayPal в период с 2003 по 2011 г., писал: «Технологии также меняют ожидания людей относительно того, как должны разрешаться споры. Люди теперь считают, что они должны иметь возможность сообщить о проблеме в любое время суток и получить быструю круглосуточную поддержку для ее прозрачного и эффективного решения. Теперь, когда общество восприняло технологии в такой степени, ключевой вопрос для профессионалов в области разрешения споров заключается в том, как мы можем использовать технологии, чтобы наилучшим образом помочь сторонам в разрешении их споров?» (Rule, 2015).

¹ China continues to lead global e-commerce market with over \$2 trillion sales in 2022. (2022, Aug 9). GlobalData. <https://www.globaldata.com/media/banking/china-continues-to-lead-global-e-commerce-market-with-over-2-trillion-sales-in-2022-says-globaldata>

На сегодняшний день законодательство и государственная политика Китая в отношении Интернета являются одними из самых передовых в мире и включают подробные и конкретные положения, определяющие отношения между платформами электронной торговли, бизнес-операторами и потребителями в онлайн-транзакциях. Примером государственной политики Китая в этой области может служить учреждение интернет-судов в Ханчжоу, Пекине и Гуанчжоу, при этом был использован опыт компании Alibaba (платформа Taobao ODS).

Автономная платформа ODS в Taobao была разработана в соответствии с американской платформой eBay ODR. Но создатели платформы Taobao ODS пошли дальше – компания внедрила новую систему вынесения решений квази-коллегией присяжных, а именно – Общественным жюри Alibaba, что стало спецификой и преимуществом компании в подтверждении характеристик справедливости и прозрачности процедуры ODS. Ошеломляющий успех системы ODS в Taobao способствовал тому, что она вышла за рамки других китайских платформ, таких как WeChat и DiDi. Именно этот аспект обусловил выбор темы настоящего исследования.

Следует особо отметить, что в доктрине Китая различают термины «онлайн-урегулирование споров» (Online Dispute Settlement – ODS) и «онлайн-разрешение споров» (Online Dispute Resolution – ODR). Об этом писали китайские, американские и немецкие специалисты (Shang & Guo, 2020; Shi et al., 2021). По их мнению, ODS осуществляют государственные интернет-суды и внутренние платформы электронной торговли, а ODR – прежде всего арбитражные учреждения (третейские суды), а также различные медиаторские организации Китая.

Российские авторы не придают особого значения различию между терминами ODR и ODS. Например, А. Н. Кутовая и К. Р. Хаджи подчеркивали: «термин “онлайн-урегулирование споров” (англ. Online Dispute Resolution, далее – ОУС) появился в 1990-х гг. Согласно одной из трактовок ОУС, это одна из форм альтернативного урегулирования споров (АУС), проводимого (частично или полностью) с помощью Интернета. Оно может также включать споры, начатые в киберпространстве, но с внешним источником. В литературе термины «электронное АУС», «онлайн-АУС» и «урегулирование споров в Интернете» рассматриваются как синонимы. Современные исследователи склоняются к тому, чтобы выделять ОУС в качестве абсолютно нового и обособленного метода урегулирования споров» (Кутовая, Хаджи, 2020).

1. Особенности урегулирования споров на платформе Taobao ODS

Правительство Китая разработало упорядоченную систему для разрешения споров, связанных с онлайн-торговлей. В августе 2017 г. в провинции Ханчжоу (где зарегистрирована компания Alibaba) открылся первый интернет-суд КНР для урегулирования конфликтов, связанных с онлайн-торговлей и нарушением авторских прав, а также споров между пользователями и интернет-компаниями; весь процесс происходил онлайн. В 2018 г. аналогичные суды были созданы в Пекине (где зарегистрирована компания Baidu) и Гуанчжоу (где зарегистрирована компания Huawei) (Русакова, 2021). Эти суды работают независимо от частных платформ онлайн-урегулирования споров, но их услуги все же могут быть задействованы. Тем не менее в Китае пока существует только три интернет-суда, и большинство споров в сфере электронной торговли разрешаются через частные платформы электронной торговли, которые также предоставляют услуги ODS (Wei & Tian, 2021).

Отметим, что правительство Китая консультировалось с компанией Alibaba по поводу дизайна интернет-суда Ханчжоу. Кроме того, компания Alibaba предоставляет интернет-суду Ханчжоу облачные услуги (cloud services). Компания Alibaba также создала способ одним щелчком мыши передавать доказательства в интернет-суд со своих сайтов электронной торговли. В 2019 г. в интернет-суд Ханчжоу был введен новый проект – пилотный помощник судьи искусственного интеллекта (试点AI助理法官), также разработанный компанией Alibaba.

В 2019 г. в КНР был принят Закон об электронной торговле (E-Commerce Law)², который разрешил операторам электронной торговли создавать собственные онлайн-системы урегулирования споров. В июне 2021 г. Верховный народный суд КНР опубликовал «Регламент онлайн судебных разбирательств народного суда», а в декабре того же года были приняты поправки в ГПК КНР в части развития онлайн-слушаний. Все нормативные акты были созданы на основе изучения и обобщения практики разрешения споров платформами электронной торговли Китая.

Мы разделяем позицию американских авторов Л. Лю (Джорджтаунский университет) и Б. Вайнгаста (Стэнфордский университет), которые в статье 2020 г. «Закон в китайском стиле: решение правовой дилеммы авторитарного режима с помощью частного права» утверждали, что китайское правительство согласилось с усилиями Таобао; более того, оно начало активно сотрудничать с Taobao (Liu & Weingast, 2020). Платформы электронной торговли приняли от государства полномочия по обеспечению соблюдения законов в пределах своей компетенции; кроме того, они также помогали государству создавать формальное законодательство, экспериментируя с характером и содержанием правовых норм, подходящих для управления их платформами. Во многих отношениях это развитие проходило аналогично более ранним реформам Китая (1980-е – начало 1990-х гг.), которые создали федерализм в китайском стиле.

Правительство КНР не единственное правительство, стремящееся к сотрудничеству с частными технологическими компаниями для цифрового реформирования своей правовой системы. Примечательно, что медиаконгломерат Thomson Reuters и разработчик программного обеспечения McGirr являются крупнейшими поставщиками технологий интернет-судов в Австралии, США и Великобритании³.

Платформа электронной торговли Taobao Marketplace была создана компанией Alibaba в 2003 г., с тех пор превратилась в гигант онлайн-покупок в Китае, а также стала восьмым самым посещаемым сайтом в мире (Liu & Weingast, 2018). Платформа Таобао считается китайским аналогом американской платформы eBay, основанной на восемь лет ранее – в 1995 г. (Ballesteros, 2021). По состоянию на март 2021 г. ежемесячные активные пользователи Таобао достигли 792 млн, занимая первое место среди китайских и мировых платформ электронной торговли⁴. Согласно

² E-Commerce Law of the People's Republic of China (Adopted at the Fifth Session of the Standing Committee of the 13th National People's Congress on August 31, 2018). IPKey. https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf

³ Mingay, A. (2019, Oct 17). Size matters: Alibaba shapes China's first "Court of the Internet. *Merics*. <https://merics.org/en/analysis/size-matters-alibaba-shapes-chinas-first-court-internet>

⁴ You, X. (2018, September 3). Six key features of Taobao – Alibaba's online shopping platform. *Croud*. <https://croud.com/blog/six-key-features-of-taobao-alibabas-online-shopping-platform>

статистическим данным, платформа Taobao была самой популярной платформой электронной торговли на август 2022 г. в Китае⁵. Подобно американским торговым платформам eBay и Amazon, Taobao предоставляет собой платформу для розничной торговли от клиента к клиенту (C2C), поэтому крупные бренды, малые предприятия, предприниматели и частные лица могут открывать свои собственные интернет-магазины с помощью платформы Taobao.

Платформа предлагает четыре способа урегулировать онлайн-спор в соответствии с регламентами Taobao ODS:

- а) переговоры между сторонами;
- б) вмешательство службы поддержки потребителей Taobao;
- в) система общественного контроля;
- г) онлайн-отчет.

Беспристрастная, быстрая и доступная система урегулирования споров может снизить неопределенность, связанную с электронной торговлей, и повысить доверие к онлайн-рынкам. Опыт КНР показал, что конструкция внутренней системы онлайн-урегулирования споров (ODS) компании Alibaba является научной, разумной, недорогой и высокоэффективной, отмечала в 2018 г. Ч. Цзюаньцзюань (Университет Макао, КНР) (Juanjuan, 2018).

Модель Taobao ODS также была распространена для решения проблем реализации систем ODS на некоторых других интернет-платформах Китая, таких как WeChat (мобильная коммуникационная система для передачи текстовых и голосовых сообщений) и Didi (платформа, предоставляющая услуги агрегатора такси, каршеринга и райдшеринга). Примечательно, что ни одна из этих систем не имела такой же популярности или успеха, как система Taobao ODS, подчеркивали исследователи К. Шу Чжан, (Политехнический университет штата Калифорния, США) и Вэньли Го (компания Beiming Software Co Ltd) (Shang & Guo, 2020).

2. Характеристики технологии Taobao ODS

По мнению китайских ученых, научный подход к формированию внутренней системы Taobao ODS проявился в следующих факторах: а) модульность конструкции платформы; б) строгое соблюдение сроков, установленных внутренними регламентами разрешения споров; в) совпадение характеристик электронной торговли и платформы Taobao ODS; г) социальное участие для создания «экосистемы электронной торговли» (Juanjuan, 2018). Рассмотрим каждый показатель подробно.

2.1. Модульность конструкции платформы Taobao ODS

Специалисты Taobao ODS обнаружили, что в разных категориях товаров причины споров и результаты урегулирования всегда совпадают. Проведя исследование рынка и анализ статистики, сотрудники Taobao ODS обобщили наиболее распространенные причины споров, включая:

- а) повреждение товара;
- б) неправильную или пропущенную доставку товара;

⁵ E-commerce in China. (2022, August 3). Moore MS Advisory. URL: <https://www.msadvisory.com/ecommerce-in-china>

- в) необходимость ремонта товара;
 - г) несоответствие товара описанию;
 - д) проблему с качеством товара;
 - е) доставку товара позже установленного срока и т. д.
- Методы урегулирования спора суммируются в следующие группы:

- а) изменение стоимости товара;
- б) возврат товара;
- в) возмещение издержек и т. д.

При разработке процедуры урегулирования споров специалисты Таобао использовали такой метод модульности, чтобы предоставить заявителям выбор. Для заявителя, с одной стороны, это могло бы сэкономить время на описании проблемы, с которой он столкнулся; с другой – результат можно было бы предсказать. Более того, это могло бы побудить службы по защите прав потребителей быть более профессиональными, когда они вмешиваются в споры (Juanjuan, 2018).

2.2. Строгое соблюдение сроков, установленных внутренними регламентами разрешения споров

Каждый этап процедуры урегулирования споров на платформе Таобао ODS строго ограничен по времени. Например, через три дня после подачи заявления о возврате средств покупатель может обратиться в службу поддержки потребителей, которая должна принять решение о вмешательстве в спор в течение двух дней, а затем – окончательное решение в течение 15 дней. При этом стороны должны представить доказательства, которые включают: фотографии товара, записи чата Aliwangwang, запись на платформе Таобао, касающуюся процедуры транзакции, и т. д.⁶ Урегулирование споров должно соответствовать этому темпу, который является важным содержанием для обеспечения правосудия на платформе Таобао ODS. Если какая-либо сторона спора не сможет представить доказательства в установленный срок, она потерпит неудачу.

2.3. Совпадение характеристик электронной торговли и платформы Таобао ODS

Платформа Таобао ODS обладает характеристиками, сравнимыми с правилами электронной торговли:

- а) высокой скоростью;
- б) простотой процедуры;
- в) низкими затратами на урегулирование спора.

Популярность платформы свидетельствует о том, что в спорах B2C и C2C эффективность и экономия важнее справедливости, нейтральности, профессионализма и обоснованности, которые как раз совпадают с характеристиками электронной торговли.

⁶ Taobao Rules of Dispute Settlement. (2019, 5 июня). 淘宝平台争议处理规则. <https://rulechannel.taobao.com/?type=detail&ruleId=99&cId=1154&spm=a2177.72311#/rule/detail?ruleId=99&cId=1154&spm=a2177.72311>

2.4. Социальное участие для создания «экосистемы электронной торговли»

Благодаря процедурам урегулирования споров на платформе Taobao ODS – «Системе общественного контроля» и «Онлайн-отчету» – платформа представила социальную силу, в том числе покупателя и продавца, для совместного участия в создании и управлении экосистемой электронной торговли Ali. Чтобы снять часть давления со своей службы поддержки потребителей, крупнейший онлайн-рынок Китая использует «народный суд» с полумиллионом судей-любителей, чтобы помочь урегулировать общие жалобы потребителей⁷.

С точки зрения справедливости система Taobao ODS использует метод случайной передачи задания рецензенту (method of delivering the task to the interviewer at random) и систему оспаривания (challenge system), чтобы эффективно помешать рецензенту выбирать дела (споры) в своих интересах. Более того, и покупатель, и продавец могут лично участвовать в «системе общественного контроля» и «онлайн-отчете», так что это хороший шанс рассказать участникам о причине спора, а затем предпринять усилия для его мирного урегулирования. Зарубежные авторы полагали, что наиболее важным обстоятельством является то, что система Taobao ODS представляет собой способ реализации социального кооперативного управления (Iqbal et al., 2022).

3. Сравнение практики разрешения споров между различными платформами ODS (государственным судом, арбитражем, частными платформами электронной торговли)

3.1. Преимущества ODR

Американский автор К. Рул выделял следующие преимущества ODR⁸:

- 1) эффективность и удобство;
- 2) процессуальная экономия;
- 3) удовлетворение участников спора;
- 4) дистанция охлаждения» (асинхронный характер ODR создает «дистанцию охлаждения» которая дает спорящим время проверить свои ответы, вместо того чтобы реагировать импульсивно)⁹;
- 5) асинхронные взаимодействия;
- 6) предварительный коммуникационный рефрейминг (под рефреймингом в нейролингвистическом программировании подразумевают способы изменения, которые связаны только с комбинацией элементов опыта, без добавления чего-либо «снаружи» – рефрейминг позволяет нам иначе интерпретировать ситуацию)¹⁰;

⁷ Staff, A. (2014, July 17). How Taobao Is Crowdsourcing Justice in Online Shopping. Alizila. <https://www.alizila.com/how-taobao-is-crowdsourcing-justice-in-online-shopping-disputes>

⁸ Rule, C. (2010, November 1). Using Technology to Manage High Volume Caseloads: The eBay/PayPal Experience. <https://www.archives.gov/files/ogis/events-presentations/acus-colin.pdf>

⁹ Condlin, R. (2017). Online Dispute Resolution: Stinky, Repugnant, or Drab? *Faculty Scholarship*, 1576. https://digitalcommons.law.umaryland.edu/fac_pubs/1576

¹⁰ Любимов, А. (2022). Модель НЛП: рефрейминг. <https://trenings.ru/entsiklopediya-nlp/modeli/959-model-nlp-refrejmng.html>

- 7) одновременное проведение совещаний;
- 8) архивированные сообщения;
- 9) автоматизированные процедуры («четвертая сторона») (Wing et al., 2021).

В отношении последнего пункта следует привести разъяснения российского медиатора М. А. Авдыева, что «в ОРС [онлайн-разрешении споров] роль управления информационными потоками часто осуществляется не только арбитрами и медиаторами, но также компьютерами, программным обеспечением. Участие ИКТ в урегулировании спора получило наименование “четвертая сторона”, поскольку ОРС рассматривается как независимая точка входа в управление конфликтом» (Авдыев, 2015). Американские авторы Итан Катш и Джанет Рифкин считали основным достижением ODR внедрение технологии в процесс разрешения споров в качестве «четвертой стороны», поддерживающей третью сторону [арбитра, медиатора, эксперта и пр.] (Katsh & Rifkin, 2001).

Отметим, что вопрос о разделении терминов «онлайн-урегулирование споров» (Online Dispute Settlement – ODS) и «онлайн-разрешение споров» (Online Dispute Resolution – ODR) в других странах (кроме КНР) не ставился. Как правило, применительно к системам онлайн-урегулирования споров на частных платформах электронной торговли чаще всего использовался термин ODR (Wing et al., 2021). Например, К. Рул в своих публикациях писал о том, что разрешение споров на платформах электронной торговли Modria, eBay и PayPal происходит в форме ODR¹¹. Можно также обратиться к известной работе английских юристов Дж. Барнетта и Ф. Треливена 2018 г. «Алгоритмическое разрешение споров – автоматизация профессионального разрешения споров с использованием технологий искусственного интеллекта и блокчейна», которые подразделяли онлайн-разрешение споров (ODR) на: а) потребительское ODR; б) судебное ODR; в) корпоративное ODR» (Barnett & Treleaven, 2017).

Дж. Тан из Монреальского университета подчеркивал, что «дистанция охлаждения» (асинхронный характер ODR) приводит к ограничению эффективности коммуникации¹². Таким образом, можно заключить, что асинхронная письменная коммуникация оценивается одними специалистами как достижение технологии ODR (К. Рул, Дж. Барнетт, Ф. Треливен и др.), а другие авторы (Дж. Тан) считают это недостатком (Iqbal et al., 2022).

Китайский исследователь Ч. Цзюаньцзюань отмечала, что преимуществами разрешения споров на частных платформах ODS являются: а) сроки рассмотрения спора; б) простота разрешения спора. Одним из самых больших достижений частных платформ ODS стал канал быстрого урегулирования споров (внутренний механизм платформы ODS электронной торговли) (Juanjuan, 2018).

¹¹ Rule, C. (2015). Modria – The Operating System for ODR. *MediatorAcademy*. https://www.judiciary.uk/wp-content/uploads/2015/02/colin_rule_modria_os_for_odr.pdf

¹² Tan, J. (2022, July 19). The Future of ODR: Immersive technology enhancement and underlying technology evolution. *Laboratoire de cyberjustice*. <https://www.cyberjustice.ca/2022/07/19/the-future-of-odr-immersive-technology-enhancement-and-underlying-technology-evolution>

3.2. Срок рассмотрения спора и постановки решения для платформ ODS

Срок рассмотрения спора и постановки решения для различных платформ ODS составляет:

1) при вмешательстве службы поддержки потребителей или системы общественного контроля Taobao ODS (компании Alibaba) – семь дней после принятия решения о вмешательстве в спор;

2) в Китайской международной экономической и торговой арбитражной комиссии (CIETAC) при наиболее быстрой ускоренной процедуре – через 15 дней после формирования арбитражного суда (ст. 50 Арбитражного регламента CIETAC)¹³;

3) в государственном суде КНР при упрощенной процедуре (summary procedure) – три месяца (ст. 161 Гражданско-процессуального кодекса КНР).

По мнению китайских авторов, скорость урегулирования споров тесно связана со сложностью процедуры. Обычно чем проще процедура, тем меньше времени уходит на решение проблемы. Если сравнить три механизма ODS, процедура Taobao ODS компании Alibaba является самой простой:

первый этап – консультации;

второй этап – вмешательство службы поддержки потребителей или общественного контроля;

третий этап – представление доказательств;

четвертый этап – постановление окончательного решения (Juanjuan, 2018).

ODR на платформе любого арбитражного суда КНР сложнее в два раза:

а) хотя процедура переговоров и медиации аналогична процедуре Taobao ODS, сторонам сложнее собирать доказательства, потому что, поскольку Alibaba – платформа электронной торговли, все следы транзакций, оставленные на ней, могут быть непосредственно приняты в качестве доказательств при процедуре ODS. Поскольку платформа ODR арбитражного суда является независимой третьей стороной, все доказательства не передаются автоматически арбитражу, а должны быть собраны сторонами и представлены платформе;

б) процедура онлайн-арбитража аналогична процедуре офлайн-арбитража, которая является более сложной, чем на платформе Taobao.

Арбитражная процедура в Китае такова:

во-первых, при наличии арбитражного соглашения истец подает заявку на онлайн-арбитраж;

во-вторых, должен быть создан онлайн арбитражный трибунал;

в-третьих, ответчик должен предоставить отзыв;

в-четвертых, стороны представляют доказательства;

в-пятых, онлайн арбитражный трибунал принимает решение.

Наконец, процедура онлайн судебного разбирательства в государственном суде должна соответствовать гражданско-процессуальному законодательству, которое в целом является более сложным (Juanjuan, 2018).

¹³ Online Arbitration Rules of CIETAC, art 50. *Arbitration Law*. https://arbitrationlaw.com/sites/default/files/free_pdfs/CIETAC%20Online%20Arbitration%20Rules.pdf

3.3. Возможность внедрения в Российской Федерации

Учитывая положительные характеристики, система ODR должна быть внедрена в России, в первую очередь на частных платформах онлайн-торговли, таких как Wildberries или Ozon. Мы разделяем мнение К. Рула, что основная причина, по которой ODR распространилось во многих странах мира, – это удобство (Rule, 2015). Для граждан, которые живут в отдаленных районах, ODR может быть огромным преимуществом в сравнении с физической явкой в здание суда в строго определенное время. Вторым важным преимуществом ODR является низкая стоимость либо бесплатное предоставление таких услуг. Третьим по важности фактором является доступность ODR для любых категорий граждан (для тех, кто не может оплатить адвоката; для тех, кто ухаживает за детьми или престарелыми, и пр.). Четвертое преимущество – скорость процедуры ODR.

4. Недостатки в работе платформы Taobao ODS

Исследователи Цзе Чжэн, Ч. Цзюаньцзюань, Дж. Тан, П. Фу, А. Никитков и другие отмечали, что недостатки механизма Taobao ODS очевидны (Shang & Guo, 2020; Juanjuan, 2018; Zheng, 2016; Fu et al., 2013). Это как раз те причины, по которым так необходимы другие способы разрешения споров – арбитраж, медиация и пр. К ним относятся:

- а) неопределенность правил урегулирования спора;
- б) то, что решения платформы Taobao ODS не имеют юридической силы¹⁴;
- в) ограниченность методов установления фактов на платформе;
- г) третья сторона, которая помогает урегулировать спор, может быть связана с одной из сторон или с обеими сторонами и иметь свои собственные интересы в деле;
- д) отсутствие механизма надзора и регулирования разрешения споров на платформе;
- е) справедливость решения спора на платформе Taobao ODS сомнительна (Cheng, 2022);
- ж) наконец, существует необоснованный иммунитет от ответственности самой платформы.

4.1. Не независимость третьей стороны при разрешении спора на частной платформе ODR

Будучи не независимой третьей стороной, внутренний механизм ODS платформ электронной торговли никогда не сможет заменить другие внешние системы разрешения споров. Рассматривая вопрос о независимости и нейтральности членов жюри (арбитров), китайские авторы констатируют, что нейтральность арбитров при ODR в арбитраже и нейтральность судей при ODS в государственном суде намного выше, чем нейтральность частной платформы ODS компании Alibaba. Внутренний механизм ODS предоставляется самой платформой электронной торговли (Taobao Marketplace), в службу поддержки потребителей входят сотрудники

¹⁴ Tan, J. (2022, July 19). The Future of ODR: Immersive technology enhancement and underlying technology evolution. *Laboratoire de cyberjustice*. <https://www.cyberjustice.ca/2022/07/19/the-future-of-odr-immersive-technology-enhancement-and-underlying-technology-evolution>

платформы, а рецензент службы общественного контроля платформы также является покупателем или продавцом с платформы. Неизбежно, что указанная третья сторона может иметь больший или меньший интерес или отношения с платформой, что может повлиять на ее нейтральность.

Напротив, независимо от ODR в арбитраже или ODS в государственном суде медиатор, арбитр или судья являются независимой и более нейтральной третьей стороной. Нейтралитет и независимость влияют на справедливость окончательного решения арбитра или судьи (Juanjuan, 2018).

На практике в Китае (и других странах) существует множество жалоб и обвинений на нечестность обслуживания потребителей платформой Taobao ODS. Более серьезной является проблема коррупции в сфере обслуживания потребителей: от ранних замаскированных средств, таких как подделка репутации фирмы на платформе и удаление плохой оценки, до прямых правонарушений, таких как получение взятки (Fu et al., 2013). С 2012 г. платформа Taobao Marketplace навсегда закрыла многие магазины электронной торговли и запустила судебную процедуру, в ходе которой подозревается во взяточничестве служба поддержки потребителей платформы. В мае 2012 г. после внутреннего антикоррупционного расследования компания Alibaba объявила, что подала в суд на некоторых своих сотрудников, работающих на платформе Taobao. Как сообщается, внутреннее расследование показало, что несколько сотрудников платформы Taobao помогли некоторым онлайн-продавцам удалить негативные комментарии, оставленные клиентами, чтобы повысить рейтинги поставщиков. В обмен на неправомерное предоставление доступа к сайту комментариев сотрудники получали незаконные выплаты от продавцов¹⁵.

Одной из причин, по которой служба поддержки потребителей легко могла быть вовлечена в скандал со взяточничеством, стало отсутствие особых квалификационных требований для сотрудников указанной службы. Напротив, для рецензентов в службе общественного контроля платформа Taobao создала некоторые требования: покупатель (или продавец) мог подать заявку на занятие должности рецензента, только если он является участником платформы Taobao и срок его регистрации составляет до одного года, а также если система Alipay подтвердила реальную идентификацию (ID) рецензента. В то же время покупатель (продавец) должен соответствовать другим предварительным требованиям, таким как отсутствие задолженности на платформе, определенная сумма сделок на платформе и условие соблюдения правил платформы и т. д., что, по мнению сотрудников платформы, должно помочь рецензенту вынести более обоснованное решение (Qin, 2017).

4.2. Предвзятость технологий искусственного интеллекта в системах ODR

Исследователи К. Шу Чжан и Вэньли Го отмечали, что еще одно препятствие для надлежащей правовой процедуры при применении технологий ODR возникает из-за «предвзятостей» (biases), присущих решениям, основанным на алгоритмах. Такие «предвзятости» подрывают использование алгоритмов китайской судебной системой и системой ODR. Эти «предвзятости» включают точность результатов,

¹⁵ Colwell, G. (2012, June 11). Monthly China Anticorruption Update Report – May 2012. *Squire Patton Boggs*. <https://www.anticorruptionblog.com/china/monthly-china-anticorruption-update-report-may-2012/#:~:text=Monthly%20China%20Anticorruption,June%2011%2C%202012>

«черные ящики алгоритмов» кодов ODR и конфликты интересов в государственно-частных партнерствах при создании систем ODR (Shang & Guo, 2020). Общая проблема систем ODR заключается в том, что результаты решений, основанных на алгоритмах, не всегда точны. Искусственный интеллект и другие типы хорошо построенных алгоритмов могут помочь людям принимать решения; однако полезность этих алгоритмов в более сложных случаях не совсем понятна. Кроме того, в механизмах принятия решений, основанных на алгоритмах, были обнаружены системные ошибки, а ошибки кодирования и искажения кода также могут приводить к искаженным результатам (Katsh & Rabinovich-Einy, 2018). Использование алгоритмов и анализа данных также может сделать систему ODR менее надежной, потому что причины решений, принимаемых этими автоматизированными инструментами, подлежат слабому общественному контролю. Системы искусственного интеллекта, которые учатся распознавать закономерности в данных для принятия решений, часто описываются как «черные ящики», так как даже их разработчики часто не знают, как они приходят к выводам. Поскольку алгоритмы, которые управляют ODR, являются секретными и известны только их владельцам и создателям, участники таких систем не имеют возможности узнать, как алгоритмы понимают правильный результат или действительно ли информация, используемая алгоритмами для принятия решений, является точной.

Такого же мнения придерживаются другие юристы. Так, австралийский автор Т. Бальестерос отмечала, что преимущества ODR должны быть взвешены на фоне ловушек цифровых сред. Среди многих факторов безопасности, возникающих в результате онлайн-процессов, ODR создает риск утечки данных, отсутствия конфиденциальности и небезопасной защиты потребителей. По этим причинам ODR может быть успешным в урегулировании мелких претензий, но не всегда может подходить для более сложных дел. Использование ODR на основе технологий может быть наиболее подходящим способом разрешения споров по мелким претензиям, в первую очередь в сегментах B2C и C2C. Однако для более сложных и единичных дел, связанных с B2B (business-to-business), и потенциально коллективных исков, связанных со спорами B2C, дискреционные полномочия судов по-прежнему будут крайне необходимы (Ballesteros, 2021).

4.3. Безопасность данных

ODR полагается на данные и интернет-процессы гораздо больше, чем традиционное разрешение споров. Это вызывает дополнительные проблемы безопасности данных. Двумя вопросами безопасности и сохранности данных, которые особенно заметны в ODR, являются:

1) защита информации о частных делах от внешних сторон, стремящихся взломать систему для получения этой информации («внешняя защита»);

2) защита информации о частных делах от ненадлежащего раскрытия или неправомерного использования лицами, управляющими системой («внутренняя защита»).

Внешняя защита касается целостности платформы или самой системы, когда она используется для генерации, отправки, получения, хранения, обмена или иной обработки информации. В Китае, несмотря на быстрые темпы развития ODR, практически не произошло никаких изменений для обеспечения безопасности системных данных. Лишь ограниченные научные исследования были сосредоточены на этой области, отмечали китайские авторы (Shang & Guo, 2020).

Вопрос о защите данных от внутреннего неправомерного использования или ненадлежащего раскрытия информации был изучен несколько лучше. В последние годы правительство Китая ужесточило регулирование кибербезопасности, безопасности данных и защиты личной информации. С 2016 г. были приняты три важных закона:

- а) Закон КНР о кибербезопасности 2016 г. (中华人民共和国网络安全法);
- б) Закон о безопасности данных КНР 2021 г. (中华人民共和国数据安全法);
- в) Закон КНР о защите личной информации 2021 г. (PIPL) (中华人民共和国个人信息保护法)¹⁶.

Подчеркнем, что китайская система регулирования кибербезопасности, безопасности данных и защиты личной информации все еще находится в процессе динамичного развития, и многие вопросы реализации еще предстоит прояснить¹⁷. В настоящее время многие виды технологий предотвращения споров, разработанные китайскими форумами ODR, основаны на широком сборе, анализе и обмене большим объемом пользовательской информации и данных, связанных с судебными разбирательствами; однако это порождает скрытые опасности, связанные с внутренней безопасностью данных (Simkova & Smutny, 2021).

Несмотря на все указанные выше недостатки и учитывая особенности быстрого, большого объема и низкой стоимости транзакций B2C (business-to-consumer) и C2C (consumer-to-consumer), внутренняя модель ODS на платформах электронной торговли Taobao ODS, несомненно, является наиболее прямым и эффективным способом онлайн-решения споров, утверждали некоторые исследователи (Juanjuan, 2018; Simkova & Smutny, 2021; Liu, 2022).

4.4. Необходимость строгого законодательного регулирования

Учитывая недостатки процедур ODR, выявленные в ходе деятельности платформы Taobao ODS, процедуры ODR должны быть строго урегулированы. Российскому законодателю следует заимствовать опыт КНР, где такое регулирование предусмотрено Законом КНР об электронной торговле 2019 г. При этом закон жестко определил, что платформы e-commerce должны раскрывать каналы подачи жалоб, а также другую исходную информацию о транзакциях судам, арбитражным и медиаторским органам. Платформы также должны своевременно принимать и рассматривать любые жалобы. Платформы подлежат наказанию за подделку, уничтожение, фальсификацию или отказ предоставить такую информацию. Эти положения были направлены на защиту прав потребителей.

¹⁶ Садовников, Д. (2021, 17 сентября). Обзор закона КНР о защите персональной информации (Personal Information Protection Law of the People's Republic of China (PIPL)). Издательская группа «Закон». https://zakon.ru/blog/2021/09/17/obzor_zakona_knr_o_zaschite_personalnoj_informacii_personal_information_protection_law_of_the_peoples

¹⁷ Si, J. et al. (2022, January 3). Overview of Chinese Cybersecurity, Data and Privacy Laws. *Zhong Lun Law Firm*. <https://www.zhonglun.com/Content/2022/03-01/1621106430.html>

Выводы

1. Можно согласиться с мнением китайских ученых, что внутренняя модель ODS на платформах электронной торговли Taobao ODS, несомненно, является прямым, ясным и эффективным способом онлайн-разрешения потребительских споров. Однако, будучи не независимой третьей стороной, внутренний механизм ODS платформ электронной торговли никогда не сможет заменить другие внешние системы разрешения споров. ODS полагается на данные и интернет-процессы гораздо больше, чем традиционное разрешение споров. Среди многих факторов безопасности, возникающих в результате онлайн-процессов, ODS создает риск утечки данных, отсутствия конфиденциальности и небезопасной защиты потребителей.

2. Поэтому к быстрому росту онлайн-урегулирования споров на платформах электронной торговли в Китае следует относиться с осторожностью. Онлайн-урегулирование споров на платформах изменило традиционные представления о правосудии. Широкое использование технологий ODS при создании интернет-судов в Китае изменило отношения в судах между практикующими юристами и тяжущимися сторонами, трансформировало судебные результаты и в конечном итоге изменило общий опыт правосудия. Китайские специалисты подчеркивали, что политические стимулы, ведущие к более быстрому внедрению технологий ODS в судах, будут и впредь подчеркивать положительные стороны ODS, включая доступность, эффективность, предсказуемость и предотвращение споров. Однако ODS также вызывает серьезную озабоченность в связи с традиционными принципами правосудия, такими как принципы беспристрастности, конфиденциальности и безопасности данных в процессе урегулирования споров.

3. Не только в Китае, но и в любой стране мира, внедряющей технологии ODS в процедуры разрешения споров, необходимо предпринять важные шаги для обеспечения того, чтобы процессы ODS были справедливыми, непредвзятыми и гарантировали процессуальные права.

Список литературы

- Авдыев, М. А. (2015). Сервисы разрешения споров онлайн: избранные кейсы. *Современные технологии управления*, 8(56), 2–8. <https://www.elibrary.ru/ykrunf>
- Кутовая, А. Н., Хаджи, К. Р. (2020). Онлайн-урегулирование споров: международные, страновые и частные практики и дальнейшие перспективы. *Международная торговля и торговая политика*, 4(24), 95–112. EDN: <https://www.elibrary.ru/zlwqtk>. DOI: <https://doi.org/10.21686/2410-7395-2020-4-95-112>
- Русакова, Е. П. (2021). Интегрирование «смарт» технологий в гражданское судопроизводство КНР. *Вестник Российского университета дружбы народов. Серия: Юридические науки*, 25(3), 622–633. <https://doi.org/10.22363/2313-2337-2021-25-3-622-633>
- Ballesteros, T. (2021). International Perspectives on Online Dispute Resolution in the E-Commerce Landscape. *International Journal of Online Dispute Resolution*, 8(2), 85–101. <https://doi.org/10.5553/ijodr/235250022021008002002>
- Barnett, J., & Treleaven, P. (2017). Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies. *The Computer Journal*, 61(3), 399–408. <https://doi.org/10.1093/comjnl/bxx103>
- Cheng, Z. (2022). Antitrust Concerns Over Digital Self-regulation of Chinese E-Commerce Platform. *US-China L. Rev.*, 19(3), 99–113. <https://doi.org/10.17265/1548-6605/2022.03.001>
- Fu, P., Nikitkov, A., & Bay, D. (2013). Fraud on Taobao: an application of routine activity theory. *International Journal of Business Information Systems*, 14(3), 305–321. <https://doi.org/10.1504/ijbis.2013.056719>

- Iqbal, M. O., Obaid, A. J., Agarwal, P., Mufti, T., & Hassan, A. R. (2022). Blockchain Technology and Decentralized Applications Using Blockchain. In *ICT Infrastructure and Computing: Proceedings of ICT4SD 2022* (pp. 555–563). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5331-6_57
- Juanjuan, Z. (2018). On China Cross-Border Online Dispute Settlement Mechanism-Following UNCITRAL Tnodr and Alibaba Experience. *Victoria University of Wellington. Hors serie*, 22, 191–228. https://www.wgtn.ac.nz/_data/assets/pdf_file/0004/1642594/10-juanjuan.pdf
- Katsh, E. E., & Rifkin, J. (2001). *Online dispute resolution: Resolving conflicts in cyberspace*. John Wiley & Sons, Inc.
- Katsh, E., & Rabinovich-Einy, O. (2018, May 1). Facebook, Big Data, and the Privatization of Justice in the Digital Age. *Foundation for Law, Justice and Society*. <https://www.fljs.org/facebook-big-data-and-privatization-justice-digital-age>
- Liu, L., & Weingast, B. R. (2018). *Taobao, Federalism, and the Emergence of Law, Chinese Style*. Minnesota Law Review, 111. <https://scholarship.law.umn.edu/mlr/111>
- Liu, L., & Weingast, B. R. (2020). *Law, Chinese Style: Solving the Authoritarian's Legal Dilemma Through the Private Provision of Law*. Unpublished manuscript.
- Liu, S. (2022). Book Review: Dispute Resolution in China: Litigation, Arbitration, Mediation, and their Interactions. *Social & Legal Studies*, 31(5), 796–798. <https://doi.org/10.1177/09646639221088529>
- Qin, P. (2017). Integration in Chinese e-commerce and public policy concerns: An analysis of Alibaba Group. *Thammasat Review Of Economic And Social Policy*, 3(1), 68–84. <https://doi.org/10.13140/RG.2.2.16772.01921>
- Rule, C. (2015). Technology and the Future of Dispute Resolution. *Dispute Resolution Magazine*. <https://law.scu.edu/wp-content/uploads/Rule-Technology-and-the-Future-of-Dispute-Resolution-copy.pdf>
- Shang, C. S., & Guo, W. (2020). The rise of online dispute resolution-led justice in China: An initial look. *ANU Journal of Law and Technology*, 1(2), 25–42.
- Shi, C., Sourdin, T., & Li, B. (2021). The Smart Court – A New Pathway to Justice in China? *International Journal for Court Administration*, 12(1). <https://doi.org/10.36745/ijca.367>
- Simkova, N., & Smutny, Z. (2021). Business E-NeGotiAtion: A Method Using a Genetic Algorithm for Online Dispute Resolution in B2B Relationships. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(5), 1186–1216. <https://doi.org/10.3390/jtaer16050067>
- Wei, D., & Tian, Z. (2021). Comparison of Online Dispute Resolution Mechanisms in the European Union, the United States and China: Suggestions on Possible Future Work The United Nations Commission on International Trade Law (UNCITRAL). *Victoria University of Wellington. Hors serie, Dispute Resolution, Digital Economy and Contemporary Issues in Harmonisation of International Commercial Law*, XXVI, 78–110. <https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/special-issues/hors-serie-volume-xxvi-2021/04-dan-wei-and-zehua-tian-pdf>
- Wing, L., Martinez, J., Katsh, E., & Rule, C. (2021). Designing ethical online dispute resolution systems: The rise of the fourth party. *Negotiation Journal*, 37(1), 49–64. <https://doi.org/10.1111/nej.12350>
- Zheng, J. (2016). The Role of ODR in Resolving Electronic Commerce Disputes in China. *International Journal of Online Dispute Resolution*, 3(1), 41–48. <https://doi.org/10.5553/ijodr/235250022016003001006>

Сведения об авторе



Ермакова Елена Петровна – кандидат юридических наук, доцент, доцент кафедры гражданского права и процесса и международного частного права, Российский университет дружбы народов имени Патриса Лумумбы

Адрес: 117198, Российская Федерация, г. Москва, ул. Миклухо-Маклая, 6

E-mail: ermakovaep@mail.ru

ORCID ID: <https://orcid.org/0000-0001-5722-3641>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57194130098>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/S-4388-2017>

Google Scholar ID: <https://scholar.google.com/citations?user=1BUYJfUAAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_profile.asp?id=613926

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование выполнено при финансовой поддержке Гранта Президента РФ № НШ-3270.2022.2 «Эволюция или революция гражданского судопроизводства: цифровизация через призму искусственного интеллекта».

Тематические рубрики:

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.23.65 / Ответственность в предпринимательском праве. Споры в предпринимательской деятельности и порядок их разрешения

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 23 января 2023 г.

Дата одобрения после рецензирования – 23 апреля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.30>

Features of Online Settlement of Consumer Disputes by e-commerce Platforms in the People's Republic of China

Elena P. Ermakova

Peoples' Friendship University of Russia named after Patrice Lumumba
Moscow, Russian Federation

Keywords

Buyer,
court,
digital technologies,
e-commerce,
Internet store,
law,
online dispute resolution,
online dispute settlement,
seller,
Taobao

Abstract

Objective: to research the features of online dispute settlement by e-commerce platforms in the People's Republic of China, to reveal positive features and drawbacks of ODS technologies applied by the platforms.

Methods: empirical methods of comparison, description, interpretation; theoretical methods of formal and dialectical logic. Specific scientific methods were used: legal-dogmatic and the method of legal norms interpretation.

Results: it was found that the internal ODS model on e-commerce Taobao ODS platforms is a direct, clear and effective means of online resolution of consumer disputes. However, being a non-independent "third party", the internal ODS mechanism of e-commerce platforms will never be able to substitute other external systems of dispute resolution. ODS relies on the data and Internet processes much stronger than traditional dispute resolution. Among the many safety factors emerging as a result of online processes, ODS creates the risk of data leakage, lack of confidentiality and unsafe consumer protection. ODS also causes concerns due to traditional principles of justice such as objectivity, confidentiality and safety of data in the process of dispute settlement. Not only the People's Republic of China but any country introducing the ODS technologies into the procedures of dispute resolution should take serious measures to ensure the ODS processes are just, unbiased and guarantee observance of procedural rights.

© Ermakova E. P., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: consists in a complex research of online dispute settlement by e-commerce platforms in the People's Republic of China, the practice of implementation thereof has its specific features stemming from the model of self-regulation of these relations, further stipulated by normative legal acts of the People's Republic of China and reflected in the activity of private ODS platforms.

Practical significance: is due to the current absence of possibility to apply the legal norms and rules, taking into account the specific features of ODS technologies on private platforms, to the relations using such technologies. The main provisions and conclusions of the research can be used to improve the mechanisms of legal regulation of ODS technologies in the procedural legislation of the Russian Federation.

For citation

Ermakova, E. P. (2023). Features of Online Settlement of Consumer Disputes by e-commerce Platforms in the People's Republic of China. *Journal of Digital Technologies and Law*, 1(3), 691–711. <https://doi.org/10.21202/jdtl.2023.30>

References

- Avdyev, M. A. (2015). Dispute resolution services online: selected cases. *Modern Management Technology*, 8(56), 2–8. <https://www.elibrary.ru/ykrunf>
- Ballesteros, T. (2021). International Perspectives on Online Dispute Resolution in the E-Commerce Landscape. *International Journal of Online Dispute Resolution*, 8(2), 85–101. <https://doi.org/10.5553/ijodr/235250022021008002002>
- Barnett, J., & Treleaven, P. (2017). Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies. *The Computer Journal*, 61(3), 399–408. <https://doi.org/10.1093/comjnl/bxx103>
- Cheng, Z. (2022). Antitrust Concerns Over Digital Self-regulation of Chinese E-Commerce Platform. *US-China L. Rev.*, 19(3), 99–113. <https://doi.org/10.17265/1548-6605/2022.03.001>
- Fu, P., Nikitkov, A., & Bay, D. (2013). Fraud on Taobao: an application of routine activity theory. *International Journal of Business Information Systems*, 14(3), 305–321. <https://doi.org/10.1504/ijbis.2013.056719>
- Iqbal, M. O., Obaid, A. J., Agarwal, P., Mufti, T., & Hassan, A. R. (2022). Blockchain Technology and Decentralized Applications Using Blockchain. In *ICT Infrastructure and Computing: Proceedings of ICT4SD 2022* (pp. 555–563). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5331-6_57
- Juanjuan, Z. (2018). On China Cross-Border Online Dispute Settlement Mechanism-Following UNCITRAL Tnodr and Alibaba Experience. *Victoria University of Wellington. Hors serie*, 22, 191–228. https://www.wgtn.ac.nz/_data/assets/pdf_file/0004/1642594/10-juanjuan.pdf
- Katsh, E. E. & Rifkin, J. (2001). *Online dispute resolution: Resolving conflicts in cyberspace*. John Wiley & Sons, Inc.
- Katsh, E. & Rabinovich-Einy, O. (2018, May 1). Facebook, Big Data, and the Privatization of Justice in the Digital Age. *Foundation for Law, Justice and Society*. <https://www.fljs.org/facebook-big-data-and-privatization-justice-digital-age>
- Kutovaya, A. N. & Khadzhi, K. R. (2020). Online dispute resolution: international, domestic and private practices and further prospects for development. *International Trade and Trade Policy*, 4(24), 95–112. <https://doi.org/10.21686/2410-7395-2020-4-95-112>
- Liu, L. & Weingast, B. R. (2018). *Taobao, Federalism, and the Emergence of Law, Chinese Style*. Minnesota Law Review, 111. <https://scholarship.law.umn.edu/mlr/111>
- Liu, L. & Weingast, B. R. (2020). *Law, Chinese Style: Solving the Authoritarian's Legal Dilemma through the Private Provision of Law*. Unpublished manuscript.

- Liu, S. (2022). Book Review: Dispute Resolution in China: Litigation, Arbitration, Mediation, and their Interactions. *Social & Legal Studies*, 31(5), 796–798. <https://doi.org/10.1177/09646639221088529>
- Qin, P. (2017). Integration in Chinese e-commerce and public policy concerns: An analysis of Alibaba Group. *Thammasat Review of Economic And Social Policy*, 3(1), 68–84. <https://doi.org/10.13140/RG.2.2.16772.01921>
- Rule, C. (2015). Technology and the Future of Dispute Resolution. *Dispute Resolution Magazine*. <https://law.scu.edu/wp-content/uploads/Rule-Technology-and-the-Future-of-Dispute-Resolution-copy.pdf>
- Rusakova, E. P. (2021). Integration of “smart” technologies in the civil proceedings of the People’s Republic of China. *RUDN Journal of Law*, 25(3), 622–633. <https://doi.org/10.22363/2313-2337-2021-25-3-622-633>
- Shang, C. S. & Guo, W. (2020). The rise of online dispute resolution-led justice in China: An initial look. *ANU Journal of Law and Technology*, 1(2), 25–42.
- Shi, C., Sourdin, T., & Li, B. (2021). The Smart Court – A New Pathway to Justice in China? *International Journal for Court Administration*, 12(1). <https://doi.org/10.36745/ijca.367>
- Simkova, N., & Smutny, Z. (2021). Business E-NeGotiAtion: A Method Using a Genetic Algorithm for Online Dispute Resolution in B2B Relationships. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(5), 1186–1216. <https://doi.org/10.3390/jtaer16050067>
- Wei, D., & Tian, Z. (2021). Comparison of Online Dispute Resolution Mechanisms in the European Union, the United States and China: Suggestions on Possible Future Work The United Nations Commission on International Trade Law (UNCITRAL). *Victoria University of Wellington. Hors serie, Dispute Resolution, Digital Economy and Contemporary Issues in Harmonisation of International Commercial Law*, XXVI, 78–110. <https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/special-issues/hors-serie-volume-xxvi-2021/04-dan-wei-and-zehua-tian-pdf>
- Wing, L., Martinez, J., Katsh, E., & Rule, C. (2021). Designing ethical online dispute resolution systems: The rise of the fourth party. *Negotiation Journal*, 37(1), 49–64. <https://doi.org/10.1111/nej.12350>
- Zheng, J. (2016). The Role of ODR in Resolving Electronic Commerce Disputes in China. *International Journal of Online Dispute Resolution*, 3(1), 41–48. <https://doi.org/10.5553/ijodr/235250022016003001006>

Author information



Elena P. Ermakova – Candidate of Sciences in Jurisprudence, Associate Professor, Department of Civil Law and Procedure and International Private Law, Peoples' Friendship University of Russia named after Patrice Lumumba

Address: 6 Mikluho-Maklaya Str., 117198 Moscow, Russian Federation

E-mail: ermakovaep@mail.ru

ORCID ID: <https://orcid.org/0000-0001-5722-3641>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57194130098>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/S-4388-2017>

Google Scholar ID: <https://scholar.google.com/citations?user=1BUYJfUAAAAJ>

RSCI Author ID: https://elibrary.ru/author_profile.asp?id=613926

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research was carried out with the financial support of the Russian President's grant No. NSh-3270.2022.2 "Evolution or evolution of the civil court procedure: digitalization through the prism of artificial intelligence".

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – January 23, 2023

Date of approval – April 23, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:347.973:004:81`2:81`25

EDN: <https://elibrary.ru/pqiafk>

DOI: <https://doi.org/10.21202/jdtl.2023.31>

Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии

Йи Рэн

Университет штата Новый Южный Уэльс
г. Сидней, Австралийский Союз

Ключевые слова

Видеоконференции,
виртуальные слушания,
виртуальный зал суда,
нормы процессуального
права,
перевод в суде,
переводчик в суде,
право,
суд,
цифровые технологии,
языковое равенство

Аннотация

Цель: данный междисциплинарный обзор ставит своей целью информирование правоведов, практиков и пользователей услуг лингвистического перевода в судебной системе о проблемах профессионального перевода на виртуальных слушаниях и в дистанционных режимах.

Методы: исследование проведено на стыке права, лингвистики и теории коммуникации и анализирует новейшие подходы к использованию технологий в дистанционном формате. Результаты работы синтезируются в форме практических рекомендаций для эффективной коммуникации в юридической сфере, осуществляемой при посредстве переводчиков в виртуальных судах.

Результаты: преследуя глобальную цель – повышение эффективности сотрудничества между поставщиками и пользователями переводческих услуг в процессе многоязычного общения в юридической сфере для достижения процессуального равноправия и равного доступа к правосудию, данное исследование позволяет сделать следующие основные выводы: (1) переход к использованию виртуальных слушаний с применением технологий значительно ускорился благодаря пандемии COVID-19, (2) растет потребность в эффективной коммуникации в юридической сфере, осуществляемой при посредстве переводчиков в дистанционном формате, и (3) успешное сотрудничество между пользователями и поставщиками услуг может привести к обоюдной выгоде.

Научная новизна: обзор исследований в области права и лингвистики выявил три основные проблемы: (1) соблюдение норм процессуального права во время слушаний в формате видеоконференций и при использовании дистанционных технологий, (2) реализация принципов равноправия и доступности правосудия для лиц с ограниченным владением официальным языком судебной системы

© Рэн Йи, 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

и (3) осуществление эффективной коммуникации в юридической сфере при посредстве людей-переводчиков в виртуальных судах. Представленная работа восполняет пробелы в изучении данных вопросов.

Практическая значимость: статья затрагивает три аспекта системы взаимоотношений между правом и языком: (1) пандемия COVID-19 ускорила внедрение технологий виртуальных залов судов в Австралии и повлияла на переводческую деятельность в судах, (2) переводчики испытывают трудности при дистанционной работе, (3) необходимо добиваться лингвистической точности и межкультурной адекватности при сохранении стиля передачи содержания, заложенного автором оригинального сообщения. Исследование опирается на практику судебного перевода и подчеркивает важность эффективного сотрудничества в процессе успешной многоязычной коммуникации в юридической сфере на основе общих целей, ожиданий и понимания между профессионалами.

Для цитирования

Рэн, Йи. (2023). Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии. *Journal of Digital Technologies and Law*, 1(3), 712–724. <https://doi.org/10.21202/jdtl.2023.31>

Содержание

Введение

1. Обзор деятельности судебных переводчиков
2. Значимость переводчиков на примере Австралии
3. Развитие виртуальных залов судебных заседаний с помощью технологий
4. Обеспечение соблюдения прав в виртуальных залах судебных заседаний: задачи и сотрудничество

Заключение

Список литературы

Введение

Множество исследований посвящено одноязычной коммуникации в юридической сфере в очном формате. Однако межкультурная и междоязычная коммуникация в юридической сфере в условиях виртуальных слушаний и дистанционного формата изучена недостаточно. Обзор литературы в области права и лингвистики выявил три основные проблемы: (1) соблюдение норм процессуального права во время слушаний в формате видеоконференций и при использовании дистанционных технологий, (2) реализация принципов равноправия и доступности правосудия для лиц с ограниченным владением официальным языком судебной системы и (3) осуществление эффективной коммуникации в юридической сфере при посредстве людей-переводчиков в виртуальных судах. Данная работа восполняет пробелы в этой области знаний. Работа на стыке права, лингвистики и теории коммуникации анализирует новейшие подходы к использованию технологий в дистанционном формате. Результаты исследования синтезируются в форме практических рекомендаций для эффективной коммуникации в юридической сфере, осуществляемой при посредстве переводчиков

в виртуальных судах. Цель данного междисциплинарного обзора – проинформировать правоведов, практиков и пользователей услуг лингвистического перевода в судебной системе о проблемах, с которыми сталкиваются профессиональные переводчики на виртуальных слушаниях и при дистанционных режимах работы. Глобальная цель – повысить эффективность сотрудничества между поставщиками и пользователями переводческих услуг в процессе многоязычного общения в юридической сфере для достижения процессуального равноправия и равного доступа к правосудию. Данное исследование приводит к следующим основным выводам: (1) переход к использованию виртуальных слушаний с применением технологий значительно ускорился благодаря пандемии COVID-19, (2) растет потребность в эффективной коммуникации в юридической сфере, осуществляемой при посредстве переводчиков в дистанционном формате, и (3) успешное сотрудничество между пользователями и поставщиками услуг может привести к обоюдной выгоде. Статья состоит из разделов, раскрывающих следующие аспекты: (1) влияние пандемии COVID-19 на внедрение технологий виртуальных залов судов в Австралии и переводческую деятельность в судах, (2) трудности переводчиков при дистанционной работе, (3) достижение лингвистической точности и межкультурной адекватности при сохранении стиля передачи содержания, заложенного автором оригинального сообщения. Исследование опирается на практику судебного перевода и подчеркивает важность эффективного сотрудничества в процессе успешной многоязычной коммуникации в юридической сфере на основе общих целей, ожиданий и понимания между профессионалами.

1. Обзор деятельности судебных переводчиков

Перевод в суде – это языковая услуга, предоставляемая сертифицированным переводчиком, обученным осуществлять перевод между английским языком и местными языками, отличными от английского, как устными, так и жестовыми. Предоставление адекватных услуг перевода компетентными судебными переводчиками необходимо для обеспечения справедливого правосудия для истцов, ответчиков и других сторон процесса. Судебные переводчики должны соблюдать профессиональный кодекс этики и поведения и переводить максимально точно. Профессиональные судебные переводчики – это подготовленные специалисты, владеющие английским и другим языком (другими языками) на уровне, близком к носителю языка, обладающие широкой общей эрудицией и способные выполнять перевод в различных режимах: последовательном, синхронном переводе, нашептывании, жестовом переводе. Судебные переводчики – важнейшее звено в обеспечении равноправного доступа к судебным процедурам, особенно для недавних мигрантов, беженцев, представителей местных народностей, выживших пострадавших, маленьких детей, уязвимых и мобильных слоев населения с ограниченным знанием английского языка, а также глухих и слабослышащих.

2. Значимость переводчиков на примере Австралии

Сообщество в Австралии отличается разнообразием языков и культур. Более половины населения родились за рубежом, в стране используется более 300 языков. В последнее время наблюдается похвальный прогресс в области сертификации и профессионализма. Усилия в этом направлении заметны по следующим тенденциям: (1) рост числа членов профессиональной ассоциации Австралийского института переводчиков (Australian Institute of Interpreters and Translators, AUSIT), (2) введение

специальной сертификации судебных переводчиков, (3) поддержка со стороны Судебного совета по разнообразию и инклюзивности (Judicial Council on Diversity and Inclusion, JCDI), способствующая эффективному сотрудничеству для достижения общей цели, единству ожиданий и пониманию между специалистами различных направлений, (4) рост признания роли переводчиков судебным сообществом, что отразилось в высказываниях судьи Robert-Smiths (Robert-Smiths, 2009), почетных судей Perry и Zornada¹.

3. Развитие виртуальных залов судебных заседаний с помощью технологий

Распространение аудиовизуальных средств связи и технологий видеоконференций в судебном процессе привело к повышению сотрудничества как в реальных, так и в виртуальных залах судебных заседаний. Усилия в этом направлении предпринимались с обеих сторон судебной системы, что привело к трем несомненным достижениям: (1) использование техники записи при работе с переводчиками в судах, (2) появление методических указаний профессиональной ассоциации для дистанционной деятельности при переводе и рекомендаций по национальной стандартизации работ с переводчиками в судах и трибуналах, (3) обеспечение дополнительных ресурсов для судебных переводчиков, включая ознакомительные материалы, шаблоны глоссариев, ответы на часто задаваемые вопросы, которые выкладываются на сайты органов внутренних дел², местных центров юридической помощи³, государственной базы нормативно-правовых документов⁴ и других юридических служб.

Однако, несмотря на достигнутые успехи, немедленного внимания требуют три новые проблемы: (1) влияние ускоренного процесса внедрения виртуальных залов судебных заседаний и дистанционных услуг перевода в результате пандемии COVID-19 на деятельность судебных переводчиков и ожидания по поводу этой деятельности, (2) этические дилеммы, с которыми сталкиваются переводчики при дистанционной работе, и (3) лингвистическая точность и межкультурная адекватность при сохранении уровня воздействия языка, используемого юристами в зале суда, для корректного воспроизведения динамики процесса на другом языке с целью достижения справедливого результата.

Чтобы рассмотреть перспективы решения этих проблем, необходимо оценить вложения в финансовые ресурсы, технические знания, время и усилия, поддержку со стороны источников законодательства и практические соображения. С финансовой точки зрения в реализацию технологий в судебном процессе вложены миллионы долларов; это вложения, сделанные до пандемии COVID-19, в аудиовизуальные

¹ «Принципы справедливости и равенства перед законом являются основополагающими для демократического общества, и их соблюдение необходимо для поддержания доверия общественности к судебной системе». См. Perry, J. M., & Zornada, K (2015, March 13–14). *Working with Interpreters: Judicial Perspectives*. Federal Court of Australia. <https://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-perry/perry-j-20150313>

² Australian Government Department of Home Affairs. Translation and Interpreting Service. <https://www.tisnational.gov.au>

³ <https://www.clcns.org.au>

⁴ <https://www.legallaid.nsw.gov.au>

технологии, видеоконференции, хранение данных в электронном виде⁵. Использование этих технологий регулируется Законами «О доказательствах»⁶ и провозглашается различными штатами и территориями Австралии⁷. С практической точки зрения аудиовизуальные технологии и видеоконференции предназначены в основном для процессов, происходящих между штатами, включающих несовершеннолетних свидетелей и представителей других особых групп в удаленных регионах. Использование этих дистанционных технологий находит поддержку со стороны Федерального суда Австралии, в 2016 г. выпустившего Практическое руководство в области технологий и судебной практики (GPN-TECH), которое включает рекомендации по подготовке и проведению цифровых и гибридных слушаний во всех судебных юрисдикциях Австралии⁸.

Во время локдауна в связи с пандемией COVID-19 выросли масштабы проведения слушаний с помощью технологий и дистанционных переводческих услуг. Однако оценки практики виртуальных судов неоднозначны, существуют мнения правоведов, сотрудников судебной системы и профессиональных сообществ, как поддерживающие, так и критикующие этот опыт. К примеру, в начальный период пандемии COVID-19 сотрудники судебной системы воспринимали переход к слушаниям с помощью цифровых технологий как «навязанную инновацию»⁹. Это отношение было поддержано рядом правоведов (Legg & Song, 2021), которые предостерегали от использования аудиовидеосвязи и ее приложений в случаях уязвимых групп свидетелей, свидетелей, находящихся в иностранных юрисдикциях, заключенных в исправительных учреждениях, а также представителей вспомогательных служб, таких как переводчики и эксперты. Фактически ученые, высказывавшие сомнения по этом вопросу, привлекли внимание к необходимости проявлять настороженность относительно риска утраты справедливости и законности из-за изменения природы судебных слушаний в результате опосредованных судебных слушаний¹⁰. Подобные опасения в отношении уязвимости дистанционных технологий выражали также McIntyre, Olijnyk и Pender (McIntyre et al., 2020), описывая ряд трудностей при принятии решений, например, вопросы присутствия или отказа связи¹¹.

⁵ Smith, R., Savage, R. & Emami, C. (2021). Benchmarking the Use of Audiovisual Link Technologies. Australian Government Institute of Criminology. <https://www.aic.gov.au/publications/rr/rr23>

⁶ Evidence Act 1929 SA, Evidence Act 1939, Evidence Act QLD 1977, Evidence, Audio and Audio Visual Links Act NSW 1998, Evidence, Audio and Audio Visual Links Act TAS 1999.

⁷ Parliament of Australia, Factsheet 20 – The Australian System of Government. https://www.aph.gov.au/About_Parliament/House_of_Representatives/Powers_practice_and_procedure/00_-_Infosheets/Infosheet_20_-_The_Australian_system_of_government

⁸ Allsop, J. L. B. (2016). Technology and the Court Practice Note (GPN-TECH). *Federal Court of Australia*. <https://www.fedcourt.gov.au/law-and-practice/practice-documents/practice-notes/gpn-tech>

⁹ Australia's courts keep the justice system going during coronavirus pandemic. (2020, 9 May). SBS News. <https://www.sbs.com.au/news/article/australias-courts-keep-the-justice-system-going-during-coronavirus-pandemic/meo0niykf>

¹⁰ Legg, M., Song, A. (2021). The courts, the remote hearing and the pandemic: from action to reflection. *UNSW Law Journal*, 44(1), 126–166. <https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2021/04/04-Legg-Song.pdf>

¹¹ Courts and COVID-19: Challenges and Opportunities in Australia. (2020). *Australian Public Law*. <https://www.auspublaw.org/blog/2020/05/courts-and-covid-19-challenges-and-opportunities-in-australia>

Однако, несмотря на эти опасения, виртуальный доступ к судопроизводству в штате Новый Южный Уэльс получил признание как средство повышения гибкости в доступе населения к системе правосудия. Описывая его преимущества, генеральный прокурор штата Марк Спикман отметил, что на оснащение более 17 залов суда технологиями аудиовидеосвязи и оборудованием для жертв домашнего насилия было затрачено более 43 миллионов долларов¹². Это позитивное отношение к виртуальному доступу к судопроизводству, подкрепленное вложениями в области финансов и логистики, приводит к росту общей положительной обратной связи к этим возможностям. Примечательны результаты опроса, проведенного в 2021 г. Обществом юристов. Было выявлено, что более 90 % респондентов предпочли очному участию проведение судебных процессов в режиме онлайн, так как дистанционный формат отличается большей гибкостью в проведении слушаний и других мероприятий, не говоря уже о других преимуществах, таких как затраты времени участников процесса на дорогу до зала суда.

4. Обеспечение соблюдения прав в виртуальных залах судебных заседаний: задачи и сотрудничество

Хотя возможность дистанционного правосудия находит поддержку ученых, это не отменяет необходимости изучить роль работы переводчика в онлайн режиме в условиях многоязычного населения с ограниченным владением официальным языком судебной системы. Можно выделить три ключевых подхода к проблеме взаимодействий в дистанционном режиме с участием переводчика: (1) права человека, (2) нормы процессуального права, (3) языковое равноправие. Мы сосредоточимся на трех основных вопросах: (1) праве на справедливое представительство, предусмотренном нормативными документами на международном (Международный пакт о гражданских и политических правах 1966, статья 14), надгосударственном (Директива ЕС 2010/64) и местном (Закон «О доказательствах» штата Новый Южный Уэльс от 1995 года) уровнях, (2) праве на бесплатные услуги переводчика, предусмотренном разделом 32 Закона штата Квинсленд о правах человека от 2019 г., (3) праве на использование родного языка, в частности, коренными народами, предусмотренном Декларацией Организации Объединенных Наций о правах коренных народов (UNDRIP)¹³ и Конвенцией Международной организации труда (ILO) о коренных народах и народах, ведущих племенной образ жизни в независимых странах¹⁴.

Важность права на использование родного языка и права на услуги переводчика в суде общепризнана, однако малоизученным остается вопрос языковых трудностей, с которыми сталкиваются переводчики на дистанционных слушаниях, хотя уже изучаются технические и административные проблемы дистанционного перевода на трибуналах по иммиграции (Grieshofer, 2022), при работе полиции и в других

¹² Stonehouse, G. (2022, June 17). Survey finds virtual NSW courts favourable. *The West Australian*. <https://thewest.com.au/news/crime/survey-finds-virtual-nsw-courts-favourable-c-7196555>

¹³ United Nations Declaration on the Rights of Indigenous Peoples. https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf

¹⁴ International Labour Organization. Indigenous and Tribal Peoples Convention, 1989 (No. 169). https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C169

юридических контекстах (Braun, 2020). Неофициальные отзывы переводчиков, работающих на дистанционных судебных слушаниях, свидетельствуют о том, что они сталкиваются с этическими дилеммами, когда их клиенты не имеют опыта такого взаимодействия. Недостаток практического опыта сотрудничества с переводчиком иногда приводит к завышенным ожиданиям относительно обязанностей и возможностей переводчика. К примеру, технические и этические трудности представляет ситуация, когда переводчик под присягой должен войти в ту же видеоконференцию с другого устройства под другим аккаунтом, чтобы перевести не подлежащий записи разговор клиента с его адвокатом. Это этически проблематично, поскольку профессиональные переводчики связаны профессиональным этическим кодексом¹⁵, который обязывает добросовестно переводить все сказанное так, как это было сказано в оригинале.

Данный принцип точности обязывает переводчика передавать как содержание, так и языковую манеру сказанного. В реальности соблюдение языковой эквивалентности представляет большую сложность. Это происходит по трем основным причинам: (1) стиль первоначального сообщения получает свои особенности в зависимости от намерений говорящего, что выражается языковыми средствами (Gallai, 2022), такими как способы постановки вопросов, речевые маркеры, тон и интонация, взгляды, жесты; (2) особенности речи могут по-разному декодироваться разными людьми, в зависимости от знания предмета речи, социально-экономической и образовательной базы, психологических черт, индивидуальной и групповой культурной идентичности, институциональных норм и ожиданий страны происхождения (Yi, 2023a, 2023b); и (3) указанные особенности сложно передать в эквивалентной форме на другом языке с той же степенью воздействия, учитывая проблему переводимости (Lee, 2011) и трудности достижения языковой эквивалентности (Liu, 2020) и межкультурной уместности (Yi, 2022).

Для преодоления указанных трудностей необходимо осуществлять обоюдную коммуникацию, способствующую успешному сотрудничеству в процессе многоязычного общения в юридической сфере. Двусторонний подход характеризуется двумя видами реакции со стороны поставщиков и пользователей переводческих услуг. Эти реакции следующие: (1) со стороны переводчиков – понимание того, чего ожидают сотрудники судебных органов, (2) со стороны сотрудников судебных органов – понимание трудностей, возникающих при переводе в дистанционном режиме. Для переводчиков полезным руководством для понимания ожиданий в области межъязыковой точности и межкультурной уместности является Общее практическое пособие «Работа с переводчиками» (GPN-INTERP), выпущенное Федеральным судом Австралии 24 марта 2023 г.¹⁶ В пособии подчеркиваются два отдельных аспекта, важных для достижения точности, необходимой в судебной сфере: (1) определение «точности» перевода и (2) значение передачи как содержания, так и намерения коммуникации без пропусков и искажений. Эти аспекты отражены следующим образом: «...результатом является оптимальная и полная передача смысла с другого языка на английский язык и с английского языка на другой язык с сохранением содержания и намерения

¹⁵ AUSIT Code of Ethics and Code of Conduct. (2012, November). https://ausit.org/wp-content/uploads/2020/02/Code_Of_Ethics_Full.pdf

¹⁶ Allsop, J. L. B. (2023, 24 March). Working with Interpreters (GPN-INTERP). <https://www.fedcourt.gov.au/law-and-practice/practice-documents/practice-notes/gpn-interpret>

коммуникации, совершенной на английском или другом языке (в каждом отдельном случае), без пропусков и искажений, включая элементы, которые переводчик может счесть неприемлемыми или оскорбительными».

Представители судебной системы ожидают от судебного перевода точности в трех аспектах: (1) переводе всего, что было сказано в суде, включая эмоционально окрашенные слова и выражения, в том числе ругательства и проявления ненависти, (2) передаче того, что и как говорится в суде, включая содержание, манеру речи (использование вставных слов, ограничителей, исправлений, тона, интонации), намерения (в явной и неявной форме), (3) использовании профессиональных знаний и способностей для достижения оптимальной и полной передачи речи на другом языке. Однако на практике очень сложно передать манеру речи и намерения говорящего с эквивалентной степенью воздействия на другом языке. Основные причины сложностей следующие: (1) существуют различия в индексальности конкретных особенностей речи, то есть особенности манеры речи подразумевают различный смысл для разных людей, социокультурных групп и языковых общностей; (2) эти различия кажутся незаметными на фоне полного объема содержания речи в судебном процессе, включающей юридические аргументы, факты, источники права; (3) эти различия кажутся менее значимыми для судебного разбирательства.

Для выработки требований к переводческой деятельности необходимо дать рабочее определение указанным особенностям манеры речи в соответствии с их функциями и значением для судебного заседания. В научной литературе, посвященной переводческой деятельности в суде, исследований в области стиля речи недостаточно. Вместо выработки строгого лингвистического определения данного понятия, применимость которого должна быть проверена в условиях судебной практики, было бы более целесообразно предложить рабочее определение, отражающее указанные особенности на практике. Манера речи – это способ, которым говорящий выражает содержание высказывания в определенном контексте для конкретной аудитории. Манера речи может включать использование говорящим языковых средств и стиливых особенностей, таких как маркеры, вставные слова и ограничители, влияющие на степень ясности речи, а также отличаться характерными индивидуальными чертами стиля (например, вежливостью, используемым регистром, вульгаризмами) и манерой выражения (например, повторами и поправками). Сюда могут входить также особенности паралингвистической коммуникации, такие как тон голоса и интонация.

Манера речи выполняет важные прагматические функции при межкультурном/межязыковом общении в суде. То, как человек говорит, может непосредственно влиять на смысл, придаваемый его высказыванию или воспринимаемый другими людьми. Например, в ряде исследований ([Kerr-Thompson, 2002](#); [Hildebrand-Edgar & Ehrlich, 2017](#)) было описано влияние стиля речи на восприятие уверенности и степени воздействия в процессе очных судебных заседаний. В дистанционном режиме восприятие особенностей стиля речи осложняется за счет применения технологий. Так, в исследованиях указывалось на то, что недостаток невербальных сигналов и зрительного контакта из-за угла съемки камеры, размера экрана, аудио- и видеоразрешения, качества связи может приводить к ошибочному пониманию намерений и подразумеваемого содержания речи говорящего во время виртуальных судебных процессов.

Заключение

Учитывая значение передачи особенностей речи в дистанционном режиме, мы считаем необходимым дальнейшее изучение этих аспектов с целью повышения эффективности многоязычной коммуникации в виртуальных залах судов. Подводя итоги, отметим, что в данном кратком сообщении мы ставили своей целью проинформировать правоведов, практиков и пользователей переводческих услуг в судебной системе о трудностях, с которыми сталкивается переводчик на виртуальных слушаниях с использованием современных технологий и в дистанционных режимах переводческой деятельности. Участники судебного процесса, ограниченно владеющие официальным языком судебной системы, имеют право на справедливое представительство при посредстве компетентного, соблюдающего этические нормы профессионального переводчика. Это не только одно из фундаментальных прав человека, но и неотъемлемая часть норм процессуального права и языкового равноправия в суде. Наш обзор способствует лучшему пониманию значения и важности понятия манеры речи в ходе судебных взаимодействий с использованием современных технологий при посредстве переводчика.

Список литературы

- Braun, S. (2020). "You are just a disembodied voice really": Perceptions of video remote interpreting by legal interpreters and police officers. In H. Salaets, & G. Brone (Eds.), *Linking up with video: Perspectives on Interpreting Practice and Research*. Amsterdam: Benjamins. <https://doi.org/10.1075/btl.149.03bra>
- Gallai, F. (2022). *Relevance Theory in Translation and Interpreting: A Cognitive-Pragmatic Approach* (1st ed.). Routledge. <https://doi.org/10.4324/9781003183969>
- Grieshofer, T. (2022). Remote Interpreting in Immigration Tribunals. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, 36, 767–788. <https://doi.org/10.1007/s11196-022-09908-3>
- Hildebrand-Edgar, N., & Ehrlich, S. (2017). She was quite capable of asserting herself": Powerful Speech Styles and Assessments of Credibility in a Sexual Assault Trial. *Linguagem e Direito [Language and Law]*, 4(2), 89–107.
- Kerr-Thompson, J. (2002). "Powerful/Powerless" language in court: A critical re-evaluation of the Duke Language and Law Programme. *International Journal of Speech, Language and the Law*, 9(2), 153–167.
- Lee, J. (2011). Translatability of Speech Style in Court Interpreting. *International Journal of Speech Language and the Law*, 18(1), 1–33. <https://doi.org/10.1558/ijssl.v18i1.1>
- Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *UNSW Law Journal*, 44(1), 126–166. <https://doi.org/10.53637/ZATE4122>
- Liu, X. (2020). Pragmalinguistic challenges for trainee interpreters in achieving accuracy: An analysis of questions and their interpretation in five cross-examinations. *Interpreting*, 22(1), 87–116. <https://doi.org/10.1075/intp.00035.liu>
- McIntyre, J., Olijnyk, A., & Pender, K. (2020). Civil courts and COVID-19: Challenges and opportunities in Australia. *Alternative Law Journal*, 45(3), 195–201. <https://doi.org/10.1177/1037969X20956787>
- Roberts-Smith, L. (2009). Forensic Interpreting: Trial and Error. <https://doi.org/10.1075/btl.87.03rob>
- Yi, R. (2022). Does Style Matter in Remote Interpreting: A Survey Study of Professional Court Interpreters in Australia. *International Journal of Translation and Interpretation Studies*, 2(1), 48–59. <https://doi.org/10.32996/ijtis.2022.2.1.7>
- Yi, R. (2023a). The promise of linguistic equity for migrants in Australian courtrooms: a cross-disciplinary perspective, *Australian Journal of Human Rights*, 29(1), 174–180. <https://doi.org/10.1080/1323238X.2023.2232171>
- Yi, R. (2023b). The Routledge Handbook of Public Service Interpreting. By Gavioli, Laura and Wadensjö, Cecilia, London, UK: Routledge. *Public Integrity*. <https://doi.org/10.1080/10999922.2023.2206236>

Информация об авторе



Рэн Йи – доктор наук, научный сотрудник, Школа гуманитарных наук и языков, Университет штата Новый Южный Уэльс

Адрес: Австралийский Союз, г. Сидней, Хай Стрит, Кенсингтон, NSW 2052

E-mail: ran.yi@unsw.edu.au

ORCID ID: <https://orcid.org/0000-0003-0630-8623>

Google Scholar ID: <https://scholar.google.com/citations?user=InljgmwAAAAJ>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/HPH-4932-2023>

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.31.41 / Процессуальные акты и действия

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 12 июня 2023 г.

Дата одобрения после рецензирования – 27 июня 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.31>

Human Interpreters in Virtual Courts: A Review of Technology-Enabled Remote Settings in Australia

Yi Ran

University of New South Wales
Sydney, Australia

Keywords

Court,
court interpreting,
digital technologies,
interpreter in court,
law,
linguistic equity,
procedural justice,
videoconferencing,
virtual courtroom,
virtual hearings

Abstract

Objective: This interdisciplinary review intends to inform legal scholars, practitioners, and users of language interpretation services in the judiciary of challenges encountered by professional interpreters in virtual hearings and remote settings.

Methods: Situated at the intersection of law, language, and communication, this review analyses the latest discourses about technology-enabled remote settings and synthesises insights into recommended practices in effective legal communication mediated by interpreters in virtual courts.

Results: With an overarching aim to improve effective collaboration between interpreting service providers and users in multilingual legal communication for procedural equity and access to justice, this review establishes three central claims: (1) the technology-enabled virtual hearings is accelerated by the covid-19 pandemic, (2) the need for effective legal communication mediated by the use of interpreters in remote settings is mounting, and (3) successful collaboration between the service user and provider can achieve a win-win outcome.

Scientific novelty: A review of existing studies in law and language reveals three main gaps: (1) procedural justice in videoconferencing hearings and remote technologies, (2) equity and access for people with limited

© Ran Yi, 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

proficiency in the official language of the court system, and (3) effective legal communication mediated by human interpreters in virtual courts. This review bridges the existing gaps in knowledge.

Practical significance: it touches on three aspects of the law-language nexus: (1) Covid-19 accelerated adoption of the virtual courtroom technologies in Australia and its impact on court interpreting, (2) challenges for interpreters in remote settings, and (3) achieving linguistic accuracy and intercultural appropriateness when preserving the manner in which the content is expressed as intended or implied by the original speaker. Grounded in courtroom interpreting practices, it highlights the importance of effective collaboration in successful multilingual legal communication rooted in mutual purpose, shared expectations, and interprofessional understanding.

For citation

Ran, Yi. (2023). Human Interpreters in Virtual Courts: A Review of Technology-Enabled Remote Settings in Australia. *Journal of Digital Technologies and Law*, 1(3), 712–724. <https://doi.org/10.21202/jdtl.2023.31>

References

- Braun, S. (2020). "You are just a disembodied voice really": Perceptions of video remote interpreting by legal interpreters and police officers. In H. Salaets, & G. Brone (Eds.), *Linking up with video: Perspectives on Interpreting Practice and Research*. Amsterdam: Benjamins. <https://doi.org/10.1075/btl.149.03bra>
- Gallai, F. (2022). *Relevance Theory in Translation and Interpreting: A Cognitive-Pragmatic Approach* (1st ed.). Routledge. <https://doi.org/10.4324/9781003183969>
- Grieshofer, T. (2022). Remote Interpreting in Immigration Tribunals. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, 36, 767–788. <https://doi.org/10.1007/s11196-022-09908-3>
- Hildebrand-Edgar, N., & Ehrlich, S. (2017). She was quite capable of asserting herself": Powerful Speech Styles and Assessments of Credibility in a Sexual Assault Trial. *Linguagem e Direito [Language and Law]*, 4(2), 89–107.
- Kerr-Thompson, J. (2002). "Powerful/Powerless" language in court: A critical re-evaluation of the Duke Language and Law Programme. *International Journal of Speech, Language and the Law*, 9(2), 153–167.
- Lee, J. (2011). Translatability of Speech Style in Court Interpreting. *International Journal of Speech Language and the Law*, 18(1), 1–33. <https://doi.org/10.1558/ijsl.v18i1.1>
- Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *UNSW Law Journal*, 44(1), 126–166. <https://doi.org/10.53637/ZATE4122>
- Liu, X. (2020). Pragmalinguistic challenges for trainee interpreters in achieving accuracy: An analysis of questions and their interpretation in five cross-examinations. *Interpreting*, 22(1), 87–116. <https://doi.org/10.1075/intp.00035.liu>
- McIntyre, J., Olijnyk, A., & Pender, K. (2020). Civil courts and COVID-19: Challenges and opportunities in Australia. *Alternative Law Journal*, 45(3), 195–201. <https://doi.org/10.1177/1037969X20956787>
- Roberts-Smith, L. (2009). Forensic Interpreting: Trial and Error. <https://doi.org/10.1075/btl.87.03rob>
- Yi, R. (2022). Does Style Matter in Remote Interpreting: A Survey Study of Professional Court Interpreters in Australia. *International Journal of Translation and Interpretation Studies*, 2(1), 48–59. <https://doi.org/10.32996/ijtis.2022.2.1.7>
- Yi, R. (2023a). The promise of linguistic equity for migrants in Australian courtrooms: a cross-disciplinary perspective, *Australian Journal of Human Rights*, 29(1), 174–180. <https://doi.org/10.1080/1323238X.2023.2232171>
- Yi, R. (2023b). *The Routledge Handbook of Public Service Interpreting*. By Gavioli, Laura and Wadensjö, Cecilia, London, UK: Routledge. Public Integrity. <https://doi.org/10.1080/10999922.2023.2206236>

Author information



Ran Yi – PhD, Researcher, School of Humanities and Languages, The University of New South Wales

Address: High Street, Kensington, NSW 2052, Sydney, Australia

E-mail: ran.yi@unsw.edu.au

ORCID ID: <https://orcid.org/0000-0003-0630-8623>

Google Scholar ID: <https://scholar.google.com/citations?user=InljgmwAAAAJ>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/HPH-4932-2023>

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – June 12, 2023

Date of approval – June 27, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:341.9:004:130.1

EDN: <https://elibrary.ru/hgbqgl>

DOI: <https://doi.org/10.21202/jdtl.2023.32>

Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция

Ярослав Кириллович Ярутин 

Дипломатическая академия Министерства иностранных дел Российской Федерации
г. Москва, Российская Федерация

Елена Евгеньевна Гуляева

Дипломатическая академия Министерства иностранных дел Российской Федерации
г. Москва, Российская Федерация

Ключевые слова

Виртуальный актив,
законодательство,
криптоактив,
криптовалюта,
международное право,
право,
стейблкоин,
токен,
цифровая валюта,
цифровые технологии

Аннотация

Цель: оценка российского законодательства на предмет его соответствия международно-правовым подходам к формированию симметричного регулирования оборота криптоактивов и возможности дополнения новыми международно-правовыми категориями, отражающими глубинные изменения в мировой экономике и структуре международных финансов, обусловленные широким внедрением новых финансовых технологий, в основе которых находятся технологии распределенного реестра.

Методы: методологическую основу исследования составляет совокупность методов научного познания, среди которых важное значение имеют специально-юридические (формально-юридический и сравнительно-правовой) методы, дополненные риск-ориентированным подходом, правовым моделированием и юридическим прогнозированием, в совокупности позволившие осмыслить архитектуру, «букву» и «дух» современного международного финансового права и национального законодательства в их понятийно-терминологической корреляции, спрогнозировать дальнейшее развитие и корректировку правового регулирования оборота криптоактивов.

 Контактное лицо

© Ярутин Я. К., Гуляева Е. Е., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Результаты: выявлено, что в регулировании оборота криптоактивов устойчивой становится тенденция доминирования среди источников актов «мягкого» права (особенно это заметно в сфере международного финансового права в сравнении, например, с конвенциями или международными договорами); наряду с этим усиливается тенденция «фрагментации» международного права в части оборота криптоактивов; отмечено несоответствие понятийного аппарата, содержащегося в международных актах и российском законодательстве, и пробелы в режиме оборота криптоактивов на уровне национального права; обозначены тенденции и прогнозы развития международно-правового регулирования сферы криптоактивов.

Научная новизна: состоит прежде всего в комплексном сопоставлении на основе в том числе принципиально новых концепций регулирования таких прогрессивных международно-правовых категорий, как криптоактив, виртуальный актив, криптовалюта, стейблкоин и другие, отдельные из которых редко используются в российском правовом дискурсе и практически не употребляются в законодательстве.

Практическая значимость: сформулированы научно обоснованные предложения, направленные на совершенствование понятийно-терминологического аппарата российского законодательства в сфере оборота криптоактивов, реализация которых позволит в перспективе выстроить единое правовое пространство с наиболее технологически развитыми государствами, будет содействовать улучшению инвестиционного климата и финансовой привлекательности государства; усовершенствует национально-правовой режим оборота криптоактивов не только с точки зрения реальных потребностей рынка, но и интересов государственной безопасности и повышения конкурентоспособности Российской Федерации.

Для цитирования

Ярутин, Я. К., Гуляева, Е. Е. (2023). Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция. *Journal of Digital Technologies and Law*, 1(3), 725–751. <https://doi.org/10.21202/jdtl.2023.32>

Содержание

Введение

1. Международно-правовое регулирование криптоактивов
 - 1.1. Особенности международного финансового права
 - 1.2. Понятие криптоактивов в международном праве
2. Отражение норм международного права в правовой системе Российской Федерации
 - 2.1. Вопросы понятийно-терминологической корреляции в международных актах и законодательстве Российской Федерации
 - 2.2. Правовое регулирование оборота криптоактивов в Российской Федерации
3. Предложения по совершенствованию российского законодательства

Заключение

Список литературы

Введение

По мнению Всемирного экономического форума, с высокой долей вероятности к 2025 г. около 10 % глобального валового внутреннего продукта будет тесно ассоциировано с технологией blockchain¹. При этом, согласно оценке Совета по финансовой стабильности, глобальная капитализация рынка криптоактивов на начало 2022 г. составляла 2,6 трлн американских долларов². Глубинные изменения в структуре международных финансов, обусловленные широким внедрением технологий распределенного реестра, требуют от международного сообщества выстраивания симметричного международно-правового регулирования, которое было бы понятно участникам рынка и национальным регуляторам. Кроме того, удовлетворяя интересы государств, такое регулирование не должно чрезмерно препятствовать развитию финансовых технологий и новых областей мировой экономики.

С другой стороны, если исходить исключительно из текущего состояния архитектуры норм международного финансового права, необходимо констатировать особую важность национального права. Именно в нем закреплены практические требования, имеющие приоритетное значение для участников рынка.

Наряду с этим криптоактивы, очевидно, распространяются вне пределов государственных границ. По этой причине, несмотря на текущую международную обстановку, международное сообщество и развитые государства заинтересованы в сотрудничестве (как минимум в рассматриваемой области), направленном на регулирование данной среды. В этом смысле представляется, что Российская Федерация в высшей степени заинтересована в глубоком осмыслении не только буквы, но и духа международно-правового регулирования. Изложенными выше факторами и продиктована необходимость в осмыслении российского законодательства и его оценки на предмет соответствия международно-правовым подходам. С учетом «фрагментации» международного права особенно важно синхронизировать финансовое регулирование не только с интересами государственной безопасности, но и с требованиями времени и реальными потребностями рынка. Представляется, что построение правового регулирования на национальном уровне потребует практико-ориентированных предложений в части дополнения российского права прогрессивными международно-правовыми категориями (криптоактив, виртуальный актив, криптовалюта, стейблкоин).

1. Международно-правовое регулирование криптоактивов

1.1. Особенности международного финансового права

Глобализация экономики и формирование единой мировой экономической системы, как представляется, изменяет и облик тех областей международного права, которые призваны регулировать экономические отношения. Это усиливает тенденции по «фрагментации» и «денационализации» соответствующих областей международного права (Мажорина, 2018).

¹ Шваб, К. (2016). *Четвертая промышленная революция*. Москва: Эксмо.

² FSB. (2022). *Assessment of Risks to Financial Stability from Crypto-assets*. FSB, Basel. <https://www.fsb.org/wp-content/uploads/P160222.pdf>

Помимо этого, на сегодняшний момент доминирующими источниками в рамках международного финансового права являются акты «мягкого» права (Кудряшов, 2013а; 2013b; 2013с; 2014; Ní Aoláin, 2021; Borlini, 2020; Brummer, 2010). Вероятно, обусловлено это тем, что процедура принятия актов «мягкого» права допускает их согласование в сжатые сроки (в сравнении, например, с конвенциями или международными договорами). В каком-то смысле бурное развитие финансовых технологий не оставило человечеству иного выбора: либо регулирование будет приниматься быстро (вслед за появлением той или иной озабоченности международного сообщества), либо новые отрасли экономики будут функционировать всецело вне международно-правового поля, что в конечном счете может оказать прямое влияние на эффективность всей архитектуры международного права.

У такого подхода существуют, однако, и минусы. Как указывалось выше, международно-правовое регулирование, сформированное посредством актов «мягкого» права, как правило, носит узкоспециальный характер. Таким образом, основной проблемой является тот факт, что формируемое правовое регулирование не носит всестороннего характера; оно ограничивается лишь отдельными областями практики. Более того, актами «мягкого» права международное сообщество указывает государствам на некоторые общие направления для правотворческой работы; эти направления носят рекомендательный характер. Реальное же содержание таких международно-правовых норм, которыми, как предполагается, и будут руководствоваться участники рынка, определяется государствами.

Необходимо учитывать и тот факт, что международно-правовое регулирование может радикально измениться, так как авторитетные ученые предлагают принципиально новые концепции регулирования, в том числе концепцию «децентрализованного регулирования» (Nabilou, 2019).

1.2. Понятие криптоактивов в международном праве

Хотя понятие «криптоактивы» крайне редко используется в российском правовом дискурсе, в том числе научном, и фактически отсутствует в законе, его употребление видится наиболее корректным с точки зрения проведения международно-правового исследования. Такая оценка обусловлена тем, что данное понятие употребляется не только участниками международного рынка, но и руководителями государств «Группы двадцати» (например, вопросам криптоактивов посвящен ряд пунктов Балийской декларации «Группы двадцати» от 16 ноября 2022 г.³).

Согласно определению, сформулированному Советом по финансовой стабильности, криптоактивы являются отображением ценности в цифровом виде (digital representation of value), которое основано на криптографии и технологии распределенного реестра (Distributed Ledger Technology, DLT), аналогичных технологиях и которое может использоваться как в платежных, так и в инвестиционных целях⁴

³ G20 Bali Leaders' Declaration. (2022, 16 November). G20, Bali. https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20%20Bali%20Leaders'%20Declaration.pdf

⁴ FSB. (2020). Final Report and High-Level Recommendations on Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. FSB, Basel. <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

(Droll & Minto, 2022). Совет по финансовой стабильности подчеркивает, что данным понятием не охватывается цифровое отображение фиатных валют⁵. Очевидно, что это замечание сделано с целью разграничить криптоактивы и цифровые валюты центральных банков (central bank digital currency, CBDC), которые в настоящий момент активно разрабатываются рядом государств (Tsang & Chen, 2022; Keister & Sanches, 2023; Zellweger-Gutknecht et al., 2021). Кроме того, Совет по финансовой стабильности между строк указывает: хотя цифровые валюты центральных банков криптоактивами не являются (Помулев, 2021), в рассматриваемое понятие (т. е. «криптоактивы») включаются криптовалюты, которые также являются цифровыми валютами⁶ (Geva, 2019).

Руководствуясь пруденциальными целями, Банк международных расчетов (Bank for International Settlements, BIS) принял решение разделить криптоактивы на группы с различными уровнями риска, выделив таким образом токенизированные формы традиционных активов, криптоактивы со стабилизационным механизмом, т. е. стейблкоины (stablecoin), и прочие криптоактивы, к которым отнесли, в частности, наиболее известную криптовалюту Bitcoin⁷. Так, был разработан международно-правовой подход, в соответствии с которым регуляторам и международным финансовым институтам, осуществляющим сделки с криптоактивами, рекомендуется применять следующие уровни риска:

- для токенизированных форм традиционных активов – как минимум уровень риска, характерный для традиционного (базового) актива;
- для стейблкоинов – уровень риска, сформированный исходя из оценки качества стабилизационного механизма;
- для иных криптоактивов, не обладающих стабилизационным механизмом, – фиксированный коэффициент риска в размере 1250 %⁸.

Важно упомянуть и о том, что особое внимание международные регуляторы уделяют именно стейблкоинам (Ferreira, 2021), поскольку они несут угрозу мировой финансовой системе (Хисамова, 2020). Во-первых, в настоящее время на международном уровне ведется активная работа по разработке критериев для оценки качества стабилизационного механизма⁹. Во-вторых, если обратиться к положению об уровне рисков, присущих стейблкоинам, то можно заметить следующее: рекомендуется рассматривать возможность по увеличению уровня риска сверх рисков, связанных со стабилизационным механизмом (with further consideration for capital add-ons). В сочетании с глобальной природой стейблкоинов подобная озабоченность международного сообщества позволяет выдвинуть предположение о том,

⁵ FSB. (2020). Final Report and High-Level Recommendations on Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements. FSB, Basel. <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

⁶ Frankenfield, J. (2023, April 20). Digital Currency Types, Characteristics, Pros & Cons, Future Uses. Investopedia. <https://www.investopedia.com/terms/d/digital-currency.asp>

⁷ BCBS. (2021). *Consultative Document: Prudential treatment of cryptoasset exposures*. BCBS, Basel. <https://www.bis.org/bcbs/publ/d519.pdf>; BCBS. (2022). *Consultative Document: Second consultation on the prudential treatment of cryptoasset exposures*. BCBS, Basel. <https://www.bis.org/bcbs/publ/d533.pdf>

⁸ BCBS. (2021). *Consultative Document: Prudential treatment of cryptoasset exposures*. BCBS, Basel. <https://www.bis.org/bcbs/publ/d519.pdf>

⁹ BCBS. (2022). *Consultative Document: Second consultation on the prudential treatment of cryptoasset exposures*. BCBS, Basel. <https://www.bis.org/bcbs/publ/d533.pdf>

что в перспективе нескольких лет именно проблемами стейблкоинов будет обоснована необходимость в формировании нового – в каком-то смысле наднационального – регулятора, в зону ответственности которого и войдет снижение глобальных рисков финансовой стабильности (сначала исключительно в части стейблкоинов)¹⁰.

С другой стороны, как было отмечено в Коммюнике встречи министров финансов и управляющих центральными банками стран «Группы двадцати» от 9 июня 2019 г., ключевая озабоченность международного сообщества лежит не в плоскости обеспечения финансовой стабильности, а в вопросах надлежащего противодействия отмыванию денег¹¹.

Необходимо констатировать, что понятийный аппарат, сформированный Группой разработки финансовых мер борьбы с отмыванием денег (Financial Action Task Force, FATF, далее – ФАТФ) для этих целей, имеет принципиально иной характер.

ФАТФ выделяет понятие «виртуальный актив» (virtual asset, VA) и производное от него понятие «лицо, оказывающее [отдельные] услуги в области виртуальных активов» (virtual asset service provider, VASP) (Schmidt, 2021). Так, виртуальный актив является отображением ценности в цифровом виде, которое может использоваться как в платежных, так и в инвестиционных целях. Согласно правовой позиции ФАТФ, виртуальные активы не включают в себя цифровое отображение фиатных валют, ценных бумаг и других финансовых активов, которые были урегулированы в рамках Рекомендаций ФАТФ ранее. По смыслу Рекомендаций ФАТФ виртуальные активы являются собственностью (property), доходами (proceeds), денежными средствами (funds), денежными средствами или иными активами (funds or other assets), корреспондирующей ценностью (corresponding value)¹².

Вероятно, читателей может в некотором смысле ввести в заблуждение поразительное сходство понятия «виртуальный актив», сформулированного ФАТФ, и понятия «цифровой актив», сформулированного Банком международных расчетов. Смысл и коннотация данных понятий, по мнению авторов, различаются: несмотря на то, что криптовалюты (относятся к цифровым валютам) включаются в понятие «виртуальный актив», ФАТФ прямо указывает на то, что не все цифровые валюты (имеются в виду цифровые валюты центральных банков) подпадают под действие международных стандартов в области виртуальных активов¹³. Таким образом, слово «цифровой», по оценке авторов, в понимании ФАТФ несет в себе коннотацию «более надежный», «регулируемый», «контролируемый государством», а в отношении собственно активов (не «валют») – «эмитируемый крупным бизнесом традиционного толка». При целостном рассмотрении финансово-технологического ландшафта данное различие, как представляется, должно быть учтено.

¹⁰ Ярутин, Я. К. (2023, март 13). Влияние криптоактивов на правительства стран и мировое сообщество: прогноз на период до 2035 года. <https://russiancouncil.ru/en/blogs/iaroslav-iarutin/the-impact-of-cryptoassets-on-governments-and-the-international-commun/?ysclid=ll689ieit3661964369>

¹¹ G20 Finance Ministers and Central Bank Governors Meeting Communiqué (2019, June 9). G20, Fukuoka. https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/communique.pdf

¹² FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>

¹³ Там же.

С практической точки зрения именно на «лицо, оказывающее [отдельные] услуги в области виртуальных активов», ложатся практические требования в части противодействия отмыванию денег, финансированию терроризма, финансированию распространения оружия массового уничтожения (далее – ПОД/ФТ/ПРОМУ); лица, зарегистрированные в качестве VASP либо признанные таковыми, стоят в одном ряду с иными «обязанными лицами» (например, банками, биржами, фондами). VASP в соответствии с определением, данным ФАТФ, – это физическое либо юридическое лицо, осуществляющее предпринимательскую деятельность, которая имеет признаки как минимум одного из следующих видов деятельности:

- обмен виртуальных активов на денежные средства в безналичной форме;
- обмен виртуальных активов на другие виртуальные активы;
- перевод виртуальных активов с одного адреса либо аккаунта на другой;
- хранение и/или администрирование виртуальных активов или инструментов, позволяющих контролировать виртуальные активы;
- оказание финансовых услуг, связанных с размещением виртуальных активов эмитента и/или продажей таких активов, либо участие в оказании таких услуг.

Так как ФАТФ подчеркивает, что якорное понятие «виртуальный актив», характерное для международно-правового механизма ПОД/ФТ/ПРОМУ, «не включает в себя цифровое отображение фиатных валют, ценных бумаг и других финансовых активов, которые были урегулированы Рекомендациями ФАТФ ранее»¹⁴, то для целей ПОД/ФТ/ПРОМУ понятие «криптовалюты» предстает раздробленным: к виртуальным активам, т. е. к криптовалютам, отдельным невзаимозаменяемым токенам (non-fungible token, NFT), токенам, выпущенным на первичном размещении монет (initial coin offering, ICO), и к иным категориям криптоактивов, а именно токенизированным формам традиционных активов и большей части NFT¹⁵, применяются различные правила. Причем такое деление может применяться исключительно для правовых норм в области ПОД/ФТ/ПРОМУ; никакой смысловой общности так называемые виртуальные активы не имеют, так как цели их использования, частота сделок и структура рынка имеют принципиальные различия. С точки зрения пользователей, как правило, криптовалюты применяются в платежных целях, токены, выпущенные на ICO, – в инвестиционных (Blemus & Guégan, 2020), а NFT, которые могут быть признаны виртуальным активом лишь в отдельных случаях, – в гедонистических и, возможно, инвестиционных.

Выделение понятия «виртуальный актив» из общего ландшафта криптоактивов, тем не менее, обладает широким практическим значением. Так, в соответствии с международно-правовыми рекомендациями необходимо проведение превентивных мер по операциям, связанным с виртуальными активами, при минимальном пороговом значении в 1000 долл. США (Salami, 2021; Кинсбургская, 2020) (с учетом

¹⁴ FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>

¹⁵ Важно, однако, отметить, что подобное деление актуально только для международно-правового механизма ПОД/ФТ/ПРОМУ. На практике же, в том числе в контексте регулирования финансовых рынков, чаще выделяется категория “utility token”. При этом, по мнению ряда ученых, на уровне права ЕС (в частности, положениями MiCa) наличествует тенденция к расширительному толкованию данной категории, что, возможно, предвещает разработку более детального разграничения и классификации NFT (Tomczak, 2022).

«мягко-правовой» природы допускается установление меньшего порога на национальном уровне)¹⁶. Наряду с этим ФАТФ подчеркивает, что в отношении ранее урегулированных Рекомендациями видов имущества (токенизированных форм традиционных активов) правовой режим в части ПОД/ФТ/ФРОМУ может оставаться неизменным (минимальное пороговое значение составляет 15 000 долл. США)¹⁷. Иными словами, величину риска отмыwania денег, присущего токенизированным формам традиционных активов, регулятор оценивает на том же уровне, что и традиционного (базового) актива, – в отличие от Банка международных расчетов, который установил иной подход.

Таким образом, необходимо констатировать, что наличествует «фрагментация» международного права. Представляется, что это недопустимо: именно следствием подобной «фрагментации» является недопонимание, которое испытывают национальные регуляторы, участники рынка и законодатели.

2. Отражение норм международного права в правовой системе Российской Федерации

2.1. Вопросы понятийно-терминологической корреляции в международных актах и законодательстве Российской Федерации

Общеизвестно, что в нынешней редакции российского законодательства регламентирован оборот «цифровых финансовых активов» и «цифровых валют». Представляется, что понятие «цифровой финансовый актив», определяемое как «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, права требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. № 259-ФЗ, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы»¹⁸.

Вероятно, законодатели и финансовый регулятор планировали, что данное понятие будет корреспондировать с понятием «цифровой актив» (digital asset), сформулированным в Совете по финансовой стабильности. На международно-правовом уровне цифровые активы являются цифровым отображением ценности в цифровом виде (digital representation of value), которое может использоваться как в платежных, так

¹⁶ Там же.

¹⁷ FATF. (2012–2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>

¹⁸ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ от 31.07.2020 (в ред. от 11.01.2023). *Собрание законодательства Российской Федерации*, 31, ст. 5018.

и в инвестиционных целях¹⁹; цифровые активы, согласно позиции Совета по финансовой стабильности, включают в себя криптоактивы. Либо, может быть, планировалось, что российские цифровые финансовые активы будут криптоактивами? По замыслу российского законодателя, цифровые финансовые активы будут выпускаться крупными российскими и международными компаниями, а процесс выпуска и распространения таких активов будет всецело соответствовать высоким требованиям Банка России. Конечно, ссылка на «распределенный реестр» в российском определении отсылает нас к международно-правовому понятию «криптоактивы». Необходимо, однако, отметить, что российский закон – в отсутствие широкой практики выпуска цифровых финансовых активов – можно толковать двояко. С одной стороны, можно сделать предположение, что отсылка к «иным информационным системам» может указывать на возможности выпуска «централизованных» цифровых финансовых активов, которые криптоактивами, разумеется, не будут. С другой стороны, аналогичная структура нормы, т. е. ссылка не только на DLT, но и на иные технологии, присутствует в международно-правовом определении «криптоактивов».

Если руководствоваться тем, что российский законодатель использовал подходы, изложенные Советом по финансовой стабильности, то все цифровые финансовые активы являются криптоактивами. Однако в любом случае понятием «цифровые финансовые активы» не охватываются криптовалюты, стейблкоины, NFT, токены, выпущенные на ICO. Таким образом, российское понятие «цифровые финансовые активы» не обладает полным соответствием понятию «криптоактивы», а включает в себя исключительно регулируемую, подконтрольную государству и крупному бизнесу часть таких активов.

Подобное несоответствие органично дополняется тем, что российское понимание «распределенного реестра», по мнению ученых, несколько отличается от принятого в рамках международных стандартов, а именно международного стандарта ISO 22739:2020²⁰ (Вергелес, 2022).

Если возвратиться к рассмотрению дефиниций, то использование прилагательного «цифровой» применительно к понятию «цифровая валюта», которое содержится в том же законе, вызывает еще большие вопросы. Согласно российскому определению, цифровой валютой признается «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам»²¹. Иными словами, под цифровой валютой в России подразумевается исключитель-

¹⁹ FSB. (2020). *Final Report and High-Level Recommendations on Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements*. FSB, Basel. <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

²⁰ *Blockchain and distributed ledger technologies – Vocabulary*. <https://www.iso.org/standard/73771.html>

²¹ Там же.

но негосударственная «валюта», более того, такая «валюта» не разрабатывается и крупным бизнесом (требования Центрального банка Российской Федерации при ее разработке не соблюдаются).

В данном случае прилагательное «цифровой» употреблено некорректно по двум причинам. Во-первых, не учтено наличие международно-правовой категории «цифровая валюта центрального банка», которая, будучи цифровой, является законным средством платежа (например, разрабатываемый в настоящее время цифровой рубль). При этом, согласно позиции Базельского комитета по банковскому надзору²², цифровая валюта центрального банка, в отличие от цифровых валют в понимании российского законодателя, является прямым обязательством центрального банка; именно центральный банк в данном случае и является надлежащим «обязанным лицом». Во-вторых, в международных деловых кругах понятие «цифровая валюта» (digital currency) используется как собирательное для виртуальных валют, криптовалют и CBDC²³.

На самом деле, как уже указывалось выше, на международном уровне существует понятие «виртуальная валюта» (virtual currency) (Brown-Hruska & Wagener, 2018), которое в полной мере соответствует тому смыслу, который закладывается российским законодателем в понятие «цифровая валюта». Так, по типологии ФАТФ, виртуальная валюта – это отображение ценности в цифровом виде (digital representation of value); ей можно торговать в цифровом режиме (that can be digitally traded). Виртуальная валюта, по мнению ФАТФ, обладает функциями денег (как средство обмена, накопления и платежа), однако не является законным платежным средством ни в одной юрисдикции²⁴.

Несмотря на то, что сегодня в ФАТФ используется собирательный термин «виртуальный актив» (в настоящее время международный регулятор отошел от использования понятия «виртуальная валюта» (Кинсбургская, 2019; Рождественская, 2022; Рождественская, Гузнов, 2020)), представляется, что коннотация слова «цифровой», с которой данный термин употребляется в российском законе, не в полной мере соответствует нормам международного права, так как фактически в законе речь идет о криптоактивах и виртуальных валютах, а не цифровых валютах в общем. Как представляется, данное несоответствие вводит в заблуждение международные деловые круги, заинтересованные в российском рынке, и умаляет неформальный престиж нашего государства.

Важно отметить, что понятие «стейблкоин», на которое, как указывалось выше, международные регуляторы направляют свое пристальное внимание, в настоящий момент фактически не отражено в российском законе. Несмотря на то, что в практической среде существует мнение о том, что у стейблкоина наличествует «обязанное лицо», усилиями которого и обеспечивается функционирование стабилизационного механизма, данная позиция, по мнению авторов, несостоятельна. Согласно позиции Базельского комитета по банковскому надзору, цифровые валюты центральных

²² BIS. (2020). *Central bank digital currencies: foundational principles and core features*. BIS, Basel. <https://www.bis.org/publ/othp33.pdf>

²³ Frankenfield, J. (2023, April 20). *Digital Currency Types, Characteristics, Pros & Cons, Future Uses*. <https://www.investopedia.com/terms/d/digital-currency.asp>

²⁴ FATF. (2014). *FATF Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks*. FATF, Paris. <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

банков были названы прямым обязательством центрального банка. В отсутствие подобных разъяснений в отношении иных типов цифровых валют допустимо заключение о том, что исключительно государство (территория) может эмитировать обеспеченные правовыми гарантиями цифровые деньги, т. е. быть надлежащим обязанным лицом. Таким образом, стейблкоины включаются в понятие «цифровая валюта», которое было сформировано российским законом. Наряду с этим необходимо констатировать, что с учетом особенного внимания международных регуляторов к проблеме стейблкоинов данное понятие должно быть отражено на уровне национального права, в том числе с перспективой развития макропруденциальных установок по мере неизбежного развития норм международного права в данной сфере.

Итак, понятийный аппарат, сформулированный в нынешней редакции российского законодательства, не в полной мере отвечает международно-правовым рекомендациям; представляется, что недостаточное внимание законодателей к международно-правовым проблемам в существенной степени усложняет правовой режим криптоактивов, делает российское регулирование не до конца понятным международным деловым кругам. Все это умаляет конкурентные преимущества российской юрисдикции для криптобизнеса и заинтересованных финансовых структур.

2.2. Правовое регулирование оборота криптоактивов в Российской Федерации

Если обратиться к сути международно-правовой позиции Российской Федерации, то необходимо указать на правомерный характер операций с криптоактивами, но с некоторыми ограничениями – как прямо закрепленными на уровне права, так и существующими исключительно на уровне практики.

Если же обратиться к пруденциальной составляющей, то Центральным банком Российской Федерации пока не сформирована позиция относительно уровня рисков, присущих цифровым финансовым активам²⁵. Очевидно, однако, что оборот цифровых финансовых активов будет всецело пребывать в рамках российского правового поля, хотя и с некоторыми ограничениями. Так, сегодня сделки с некоторыми цифровыми финансовыми активами доступны исключительно для квалифицированных инвесторов²⁶. Наряду с этим в отношении цифровых валют (в понимании российского законодателя) позиция финансового регулятора обладает принципиальными отличиями. Например, согласно информационному письму Центрального банка Российской Федерации «Об отдельных видах финансовых инструментов» от 19 июля 2021 г. № ИН-06-59/52, организаторам торговли было рекомендовано отказываться в допуске к организованным торгам ценных бумаг российских и иностранных эмитентов, права владельцев на получение выплат по которым и (или) размер выплат по которым (размер дохода) либо доходность которых зависят от курсов цифровых валют²⁷.

²⁵ ЦБ призвал регламентировать оценку рисков при вложении банков в цифровые финансовые активы. (2022, 27 декабря). *Интерфакс*. <https://www.interfax.ru/business/878897>

²⁶ Указание Банка России от 25 ноября 2020 г. № 5635-У (зарегистрировано в Минюсте России 21.12.2020 № 61622).

²⁷ Информационное письмо Центрального банка Российской Федерации от 19 июля 2021 г. № ИН-06-59/52. https://cbr.ru/StaticHtml/File/117596/20210719_in_06_59-52.pdf

С точки зрения противодействия отмыванию преступных доходов необходимо также отметить разграничение правового регулирования в отношении цифровых финансовых активов и цифровых валют. Согласно ст. 6 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», операции с цифровыми финансовыми активами подвергаются обязательному контролю в случае, когда их объем превышает 1 млн рублей²⁸. Представляется, что данная мера соответствует международно-правовым рекомендациям о том, что правовой режим в отношении традиционных активов в токенизированной форме (например, ценных бумаг) не носит специального характера²⁹. С другой стороны, все операции с цифровой валютой (в понимании российского законодателя), по мнению Банка России, носят априори подозрительный характер, что прямо отражено в Классификаторе признаков, указывающих на необычный характер операции или сделки, который является приложением к Положению Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»³⁰. Более того, необходимо отметить, что на уровне адвокатской практики ощущается, что частота «заморожек» и блокировок банковских счетов при осуществлении операций с цифровыми валютами (даже шире – со всеми виртуальными активами) на основании Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»³¹ резко возросла примерно с конца весны 2022 г.³² Иными словами, государство старается всячески ограничить оборот цифровых валют, причем делается это без внесения соответствующих изменений на уровне закона³³.

Дополнительно необходимо отметить, что сегодня наличествует ряд ограничений в отношении оборота цифровой валюты (в российском понимании этого термина). Так, согласно ст. 14 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные

²⁸ О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. № 115-ФЗ от 07.08.2001 (в ред. от 09.01.2023). *Собрание законодательства РФ*, 33 (ч. 1), ст. 3418.

²⁹ FATF. (2012–2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. FATF. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>

³⁰ Положение Банка России от 2 марта 2012 г. № 375-П. (2012, 18 апреля). *Вестник Банка России*, 20.

³¹ О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. № 115-ФЗ от 07.08.2001. *Собрание законодательства Российской Федерации*, 33 (ч. I), ст. 3418.

³² Ярутин, Я. К. (2022, 20 октября). *Цифровая валюта и будущее мировой политики*. <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/tsifrovaya-valyuta-i-budushchee-mirovoy-politiki/>

³³ Там же.

законодательные акты Российской Федерации»³⁴, для российских организаций и физических лиц – резидентов установлен запрет на принятие цифровой валюты в качестве встречного предоставления за передаваемые ими (или им) товары и услуги. Несмотря на то, что данный тезис применительно к цифровой валюте был сформулирован впервые на уровне закона, анализ судебной практики показывает, что суды и ранее относились негативно к использованию цифровых валют в договорных обязательствах (Середа, 2017). Кроме того, в соответствии с этой же статьей судебная защита для указанных выше субъектов предусматривается лишь в случае информирования Федеральной налоговой службы (далее – ФНС России) о наличии цифровой валюты и совершении сделок с ней. Вместе с тем необходимо констатировать, что на практике данный вопрос упирается в отсутствие разъяснений ФНС России по данному вопросу, в том числе в отсутствие формы для такой отчетности. В связи с этим представляется, что в настоящее время реально детализированы лишь общие обязательства по информированию налогового органа (например, в рамках формы 3-НДФЛ).

Помимо этого, важно указать и на некоторое разделение, связанное с противодействием неправомерному использованию инсайдерской информации и манипулированию рынком (далее – ПНИИИ/МР). По смыслу Федерального закона от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком...»³⁵ применение к организациям, вовлеченным в оборот цифровых валют (в понимании, установленном действующим российским законом), положений российского закона в части ПНИИИ/МР видится в высшей степени маловероятным; при этом думается, что аналогичные положения будут применяться в отношении оборота цифровых финансовых активов, хотя это не предусмотрено прямо законом (следует из регулируемого характера вовлеченных организаций). Представляется, что необходимость в урегулировании принципиально новых видов имущества в этом ключе обострит многочисленные проблемы, которые характерны для действующего механизма ПНИИИ/МР, в том числе в его уголовно-правовой составляющей (Лифшиц, Яни, 2020; Арестова, Борбат, 2022; Ручкина, 2019; 2022). С другой стороны, применимость соответствующих норм к рассматриваемым правоотношениям не вызывает сомнения и с точки зрения зарубежного (американского) права (Verstein, 2019), что, как представляется, служит дополнительным аргументом в пользу недопустимости указанного выше разделения, сделанного на уровне российского законодательства и с учетом присущей ему логики.

Таким образом, российское законодательство – в первую очередь в части понятийного аппарата – не в полной мере соответствует нормам международного права. Выстроенная система правового регулирования обладает рядом недоработок и неточностей. Представляется, что подобная ситуация с учетом архитектуры рассматриваемых международно-правовых норм умаляет авторитет нашей страны и ее неформальный престиж; самобытное понимание норм международного финансового

³⁴ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ от 31.07.2020. *Собрание законодательства Российской Федерации*, 31 (ч. I), ст. 501.

³⁵ О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации. № 224-ФЗ от 27.07.2010 (в ред. от 07 октября 2022 г.). *Собрание законодательства Российской Федерации*, 31, ст. 4193.

права, закрепленное в российском законе, непонятно международным деловым кругам. Несмотря на природу рассмотренных норм международного права (в основном содержащихся в актах «мягкого» права), т. е. несмотря на их рекомендательную природу, Российская Федерация крайне заинтересована в их внедрении. Во-первых, международное сообщество предлагает некие общие стандарты, внедрение которых позволяет государству находиться в едином правовом пространстве с наиболее технологически развитыми государствами (речь идет о довольно узкой сфере крипто-активов), что, вне всяких сомнений, содействует повышению инвестиционной привлекательности государства, поднимает неформальный престиж его руководителей. В то же время в отсутствие внедрения правовых подходов, сформулированных положениями «мягкого» права, существует вероятность того, что в отношении игнорирующего их государства будут применены методы воздействия, известные как “*naming and shaming*” (Фогельсон, 2013a; 2013b). Во-вторых, если принять во внимание высокий уровень экспертизы международных регуляторов, необходимо констатировать пользу формируемых международно-правовых подходов с точки зрения нивелирования структурных проблем, имеющих глобальный характер, на уровне российского права.

3. Предложения по совершенствованию российского законодательства

Во-первых, представляется важным привести понятийный аппарат, сформированный на уровне российского закона, в соответствие международным стандартам. На смену понятия «цифровой финансовый актив» должно прийти международно-правовое понятие «криптоактив». Предлагается разделить криптоактивы на «традиционный актив в токенизированной форме» (с одной стороны, данное понятие употребляется на уровне Банка международных расчетов, а с другой – это аналог нынешних «цифровых финансовых активов») и «необеспеченный (виртуальный) криптоактив» (с одной стороны, это аналог термина *unbacked cryptoasset* как антонима *asset-backed cryptoasset*, с другой – наличие прилагательного «виртуальный» отсылает нас к понятию «виртуальный актив», которое было сформулировано ФАТФ).

Представляется важным дополнительно, возможно отдельным законом, детализировать и понятие «цифровая валюта», которое, как указывалось выше, широко используется участниками рынка и международными регуляторами, однако с иным значением. Смысл понятия «цифровая валюта» должен быть изменен в корне. Есть два варианта в части изложения подобных нововведений.

Первый: отдельным законом цифровая валюта может быть разделена на «обеспеченную цифровую валюту», т. е. такую цифровую валюту, у которой существует лицо, обязанное перед каждым обладателем таких электронных данных (центральный банк), и «необеспеченную цифровую валюту» («цифровая валюта» в нынешней редакции закона). Такой вариант видится логичным, однако представляется несколько утопичным с точки зрения государства, так как девальвирует коннотацию слова «валюта» как связанной с государством субстанции (получается тогда, что криптовалюта – тоже валюта, хоть и иного свойства).

Второй: понятие «цифровая валюта» будет упразднено, а на его место придет «цифровая валюта центрального банка», которая будет делиться по функциональному назначению (розничная цифровая валюта центрального банка, цифровая валюта центрального банка для межбанковских расчетов и т. д.) и по государственной (территориальной) принадлежности «обязанного лица» (национальная цифровая

валюта центрального банка, т. е. цифровой рубль, и иностранная цифровая валюта центрального банка, например цифровой юань, цифровой евро). Данный подход представляется наиболее оправданным.

К какой категории в этом случае будут относиться «виртуальные валюты», в том числе криптовалюты? Здесь, как представляется, необходимо обратиться к международно-правовому подходу, сформулированному ФАТФ. Если рассматривать ситуацию в долгосрочной перспективе, то, руководствуясь целями в части эффективного правового регулирования, государство не сможет изолироваться от неприятной для него темы, а именно от внедрения на уровне закона понятия «виртуальный актив», которое используется в рамках ФАТФ. К виртуальным активам будут отнесены упомянутые выше виртуальные криптоактивы, негосударственные «валюты», в том числе криптовалюты, стейблкоины и отдельные невзаимозаменяемые токены, которые признаются виртуальными активами по логике ФАТФ. Неизбежным, если принять во внимание нынешнюю озабоченность международного сообщества данной проблематикой, представляется и выделение в законе понятия «стейблкоин». Если руководствоваться предлагаемой логикой, это будет «необеспеченный (виртуальный) криптоактив со стабилизационным механизмом».

Представляется особенно важным произвести разграничение указанных видов имущества с той точки зрения, что построение эффективного регулирования не может осуществляться в отрыве от практики их использования (Середа, 2019); причем внимание к практическим вопросам видится не менее важным, чем следование международно-правовым рекомендациям.

Во-вторых, необходимо разработать новые подходы к макропруденциальному регулированию. Представляется, что с учетом регулируемой и абсолютно прозрачной архитектуры цифровых финансовых активов (в соответствии с предлагаемыми изменениями – традиционных активов в токенизированной форме) допустимо установление уровня риска, характерного для традиционного (базового) актива (с правом регулятора в части повышения уровня риска). Неизбежным видится и изменение нынешней запретительной риторики в отношении «виртуальных активов». По мнению авторов, с учетом публично-правовой природы вопросов финансовой стабильности подобное развитие возможно исключительно вслед за появлением соответствующего подхода на уровне международных регуляторов и при безусловном согласии с ними российской стороны.

Наряду с этим при конструировании национального регулирования важно понимать, что на уровне международного права видится крайне вероятным такой сценарий, в соответствии с которым в течение ближайших лет будет изменено отношение к стейблкоинам. С учетом глобальной природы стейблкоинов было бы логичным обеспечение единого – наднационального – надзора за их функционированием, в том числе, возможно, в форме установления единых критериев для надзора на национальном уровне. Возможно, в перспективе будет образован новый международный орган для целей осуществления пруденциального надзора³⁶. По мнению ученых,

³⁶ Ярутин, Я. К. (2023, март 13). Влияние криптоактивов на правительства стран и мировое сообщество: прогноз на период до 2035 года. <https://russiancouncil.ru/en/blogs/iaroslav-iarutin/the-impact-of-cryptoassets-on-governments-and-the-international-commun/?ysclid=ll689ieit3661964369>

стейблкоин в перспективе может идентифицироваться как денежные средства (для целей учета и отчетности) (Тетюшин, 2022), однако уровень риска такого криптоактива, как следует из рассмотренных выше позиций международных регуляторов, уже сегодня (на уровне теории) зависит от качества стабилизационного механизма. Международно-правовые рекомендации в части оценки стабилизационного механизма, несомненно, будут и далее детализироваться.

С точки зрения нашей страны отсутствие на уровне права понятия «стейблкоин» может лишить финансовую систему Российской Федерации, и без того ослабленную международными санкциями, конкурентного преимущества в виде гипотетической возможности использования надежных (поднадзорных) стейблкоинов, не обладающих столь высоким уровнем санкционного бремени.

В-третьих, из отсутствия в российском правовом поле понятия «виртуальный актив» органично вытекает и отсутствие понятия «лицо, осуществляющее [отдельные] операции с виртуальными активами». С точки зрения всей международной архитектуры ПОД/ФТ/ФРОМУ это понятие является осевым, потому что международное сообщество возлагает основную часть обязательств в данной области именно на «обязанных лиц» (например, банки, страховые компании); для виртуальных активов, т. е. частично и для криптоактивов, таким лицом выступает VASP. Таким образом, подобное обстоятельство негативно сказывается на эффективности национальной системы ПОД/ФТ/ФРОМУ.

В-четвертых, несмотря на многочисленные проблемы, связанные с российской практикой применения Закона о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком, представляется важным включить в перечень инсайдеров также «лиц, осуществляющих [отдельные] операции с виртуальными активами». Возможно, к инсайдерам можно будет относить не всех VASP, а лишь соответствующих определенным критериям, например, годовой оборот которых превышает определенную регулятором величину. Данное изменение видится важным в свете того, что с финансово-экономической точки зрения рынок криптоактивов ничем не отличается от традиционных финансовых рынков; на нем также возможны злоупотребления и недобросовестное поведение, экономический ущерб может быть значительным.

В-пятых, с учетом всех изложенных выше предложений особенно важным представляется внимание государства к изменениям на уровне международного права и позиций международных регуляторов, в том числе к экспертной аналитике подобных вопросов. Область криптоактивов слишком масштабна, и ее игнорирование со стороны государства может привести к многочисленным последствиям, в том числе в таких чувствительных областях, как противодействие отмыванию доходов, финансированию терроризма, обеспечение финансовой стабильности.

Заключение

Таким образом, можно сделать вывод о том, что международно-правовая позиция Российской Федерации в отношении криптоактивов носит сдержанно либеральный характер. На уровне федерального законодательства были введены понятия «цифровой финансовый актив» и «цифровая валюта»; оборот этих категорий носит правомерный характер, хотя и наличествуют некоторые ограничения. Представляется, что понятийный аппарат, сформулированный российским законодательством,

не в полной мере соответствует международным стандартам, что является существенным недостатком национальной правовой системы (и, вероятно, финансовой системы), умаляет деловую привлекательность нашей страны. Как представляется, самобытный российский подход попросту непонятен международным деловым кругам. В остальном, т. е. в вопросах пруденциального регулирования, противодействия отмыванию денег и гражданско-правовых особенностей, российское законодательство всецело соответствует духу и букве международно-правовых рекомендаций.

На основании изложенного можно предположить, что дальнейшее развитие российского права будет носить последовательный характер. Несомненно, рано или поздно, но понятийный аппарат будет изменен в соответствии с международно-правовыми рекомендациями. Если говорить о смысловом векторе российского регулирования, то государство оправданно делает повышенную ставку на цифровые финансовые активы, которые будут выпускаться крупным бизнесом при соблюдении высоких требований, выдвигаемых финансовым регулятором. Оборот цифровых валют (в российском понимании) на практике будет и далее ограничиваться, но в отсутствие явно запретительной риторики на уровне закона³⁷. Рынок так называемых цифровых валют будет замещаться цифровой валютой центрального банка, т. е. разрабатываемым в настоящее время цифровым рублем.

С высокой долей вероятности наиболее технологически развитые страны пойдут по пути более глубокой интеграции криптоактивов в правовую действительность, приведения новых финансовых рынков в соответствие с международными стандартами. Соответственно, с концептуальной точки зрения при формировании правового режима на уровне национального права необходимо исходить именно из такой оценки.

Наряду с этим в свете практической необходимости в актуализации национального права необходимым видится понимание не только международно-правовой действительности, но и внимание к футурологии, т. е. к тенденциям и прогнозам в части вектора развития международного права. Именно к требованиям будущего должна быть максимально адаптирована национальная правовая система, если мы действительно хотим находиться в авангарде глобального развития.

Список литературы

- Арестова, Е. Н., Борбат, А. В. (2022). Проблемы возбуждения уголовных дел о манипуляции рынком и неправомерном использовании инсайдерской информации. *Всероссийский криминологический журнал*, 16(3), 384–391. <https://elibrary.ru/moixbc>
- Вергелес, Э. Р. (2022). Криптоактивы: место в современном законодательстве. *Академическая мысль*, 1(18), 35–37. <https://elibrary.ru/ldxclf>
- Кинсбургская, В. А. (2019). Идентификация держателей криптовалюты в целях противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. *Национальная безопасность / Nota Bene*, 3, 1–13. EDN: <https://elibrary.ru/byjwhb>. DOI: <https://doi.org/10.7256/2454-0668.2019.3.29720>
- Кинсбургская, В. А. (2020). Требования ФАТФ по регулированию криптовалют: проблемы имплементации в национальное законодательство. *Национальная безопасность / Nota Bene*, 4, 1–18. EDN: <https://elibrary.ru/crgkhs>. DOI: <https://doi.org/10.7256/2454-0668.2020.4.33856>
- Кудряшов, В. В. (2013а). Мягкое право как метод регулирования международных финансовых отношений в зарубежной доктрине международного финансового права. *Финансовое право*, 4, 8–12. <https://elibrary.ru/qafzdz>

³⁷ Ярутин, Я. К. (2022, 20 октября). Цифровая валюта и будущее мировой политики. <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/tsifrovaya-valyuta-i-budushchee-mirovoy-politiki/>

- Кудряшов, В. В. (2013b). Мягкое право как метод регулирования международных финансовых отношений в зарубежной доктрине международного финансового права (продолжение). *Финансовое право*, 5, 17–21. <https://elibrary.ru/qavehl>
- Кудряшов, В. В. (2013c). «Мягкое право» как метод регулирования международных финансовых отношений в зарубежной доктрине международного финансового права. *Московский журнал международного права*, 2(90), 70–89. EDN: <https://elibrary.ru/qzhcsb>. DOI: <https://doi.org/10.24833/0869-0049-2013-2-70-89>
- Кудряшов, В. В. (2014). Международные финансовые стандарты как концепция регулирования международных финансовых отношений. *Право и экономика*, 1(311), 64–71. <https://elibrary.ru/rvezrf>
- Лифшиц, И. М., Яни, П. С. (2020). Уголовная ответственность за манипулирование рынком по праву России и Европейского союза. *Всероссийский криминологический журнал*, 14(5), 764–776. EDN: <https://elibrary.ru/jdgqlc>. DOI: [https://doi.org/10.17150/2500-4255.2020.14\(5\).764-776](https://doi.org/10.17150/2500-4255.2020.14(5).764-776)
- Мажорина, М. В. (2018). Международное частное право в условиях глобализации: от разгосударствления к фрагментации. *Право. Журнал Высшей школы экономики*, 1, 193–217. EDN: <https://elibrary.ru/yvvqnc>. DOI: <https://doi.org/10.17323/2072-8166.2018.1.193.217>
- Помулев, А. А. (2021). Цифровая валюта – инструмент противодействия теневой экономической деятельности? *Теневая экономика*, 5(4), 267–274. EDN: <https://elibrary.ru/yhdxrr>. DOI: <https://doi.org/10.18334/tek.5.4.113746>
- Рождественская, Т. Э. (2022). Риски легализации криптовалют для публичного правопорядка. В сб. *Россия: тенденции и перспективы развития* (т. 17–2, с. 150–155). <https://elibrary.ru/qaqxtx>
- Рождественская, Т. Э., Гузнов, А. Г. (2020). Реализация подходов ФАТФ к регулированию виртуальных активов в законодательстве Российской Федерации: перспективы развития. *Вестник Университета им. О. Е. Кутафина*, 9, 138–146. EDN: <https://elibrary.ru/kjrwef>. DOI: <https://doi.org/10.17803/2311-5998.2020.73.9.138-147>
- Ручкина, Г. Ф. (2019). Противодействие неправомерному использованию инсайдерской информации и манипулированию рынком: опыт Банка России. *Банковское право*, 1, 9–22. <https://elibrary.ru/yvaxln>
- Ручкина, Г. Ф. (2022). Противоправные практики на рынке ценных бумаг: к вопросу совершенствования правового регулирования. *Банковское право*, 1, С. 22–29. <https://elibrary.ru/lgeios>
- Середа, А. В. (2017). Осуществление расчетов при помощи виртуальных валют в РФ: анализ первого правоприменительного опыта. *Современный юрист*, 2, 57–64. <https://elibrary.ru/yurqrp>
- Середа, А. В. (2019). К вопросу о правовом регулировании блокчейн-технологий: анализ зарубежного опыта. *Проблемы экономики и юридической практики*, 15(5), 140–143. <https://elibrary.ru/jycpbq>
- Тетюшин, А. В. (2022). Классификация цифровых финансовых активов и их идентификация в финансовой отчетности. *Аудиторские ведомости*, 1, 24–29. <https://elibrary.ru/wpzlco>
- Фогельсон, Ю. Б. (2013a). Мягкое право в современном правовом дискурсе. *Журнал российского права*, 5, 37–48. <https://elibrary.ru/pysarz>
- Фогельсон, Ю. Б. (2013b). Мягкое право в современном правовом дискурсе (окончание). *Журнал российского права*, 9, 43–50. <https://elibrary.ru/qztjov>
- Хисамова, З. И. (2020). Концепция цифровых валют центральных банков: основные риски в части соблюдения требований AML («противодействия отмыванию денег») и KYC («знай своего клиента»). *Актуальные проблемы экономики и права*, 14(3), 508–515. EDN: <https://elibrary.ru/eilmjw>. DOI: <http://dx.doi.org/10.21202/1993-047X.14.2020.3.508-515>
- Blemus, S., & Guégan, D. (2020). Initial crypto-asset offerings (ICOs), tokenization and corporate governance. *Capital Markets Law Journal*, 15(2), 191–223. <https://doi.org/10.1093/cmlj/kmaa005>
- Borlini, L. (2020). On Financial Nationalism and International Law: Sovereignty, Cooperation and Hard/Soft Governance in International Finance. *European Journal of International Law*, 31(3), 1133–1155. <https://doi.org/10.1093/ejil/chaa065>
- Brown-Hruska, S., & Wagener, T. (2018). The virtual currency regulatory framework in global context. *Capital Markets Law Journal*, 13(4), 487–517. <https://doi.org/10.1093/cmlj/kmy028>
- Brummer, C. (2010). Why Soft Law Dominates International Finance – and not Trade. *Journal of International Economic Law*, 13(3), 623–643. <https://doi.org/10.1093/jiel/jgq026>
- Droll, T., & Minto, A. (2022). Hare or Hedgehog? The Role of Law in Shaping Current Technological Trends in the Securities Post-trading System. *Accounting, Economics, and Law: A Convivium*, 1–46. <https://doi.org/10.1515/acl-2022-0029>
- Ferreira, A. (2021). The Curious Case of Stablecoins – Balancing Risks and Rewards? *Journal of International Economic Law*, 24(4), 755–778. <https://doi.org/10.1093/jiel/jgab036>

- Geva, B. (2019). Cryptocurrencies and the Evolution of Banking, Money and Payments. In Ch. Brummer (Ed.). *Crypto-assets Legal, Regulatory and Monetary Perspectives* (pp. 11–38). Oxford University Press. <https://doi.org/10.1093/oso/9780190077310.003.0002>
- Keister, T., & Sanches, D. (2023). Should Central Banks Issue Digital Currency? *The Review of Economic Studies*, 90(1), 404–431. <https://doi.org/10.1093/restud/rdac017>
- Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, 27(3), 266–291. <https://doi.org/10.1093/ijlit/eaz008>
- Ní Aoláin, F. (2021). ‘Soft Law’, Informal Lawmaking and ‘New Institutions’ in the Global Counter-Terrorism Architecture. *European Journal of International Law*, 32, 919–942. <https://doi.org/10.1093/ejil/chab071>
- Salami, I. (2021). Challenges and Approaches to Regulating Decentralized Finance. *AJIL Unbound*, 115, 425–429. <https://doi.org/10.1017/aju.2021.66>
- Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, 29(4), 332–363. <https://doi.org/10.1093/ijlit/eaac001>
- Tomczak, T. (2022). Crypto-assets and crypto-assets’ subcategories under MiCA Regulation. *Capital Markets Law Journal*, 17(3), 365–382. <https://doi.org/10.1093/cmlj/kmac008>
- Tsang, C., & Chen, P. (2022). Policy responses to cross-border central bank digital currencies – assessing the transborder effects of digital yuan. *Capital Markets Law Journal*, 17(2), 237–261. <https://doi.org/10.1093/cmlj/kmac004>
- Verstein, A. (2019). Crypto Assets and Insider Trading Law’s Domain. *Iowa Law Review*, 105(1), 1–59.
- Zellweger-Gutknecht, C., Geva, B., & Grünewald, S. N. (2021). Digital Euro, Monetary Objects, and Price Stability: A Legal Analysis. *Journal of Financial Regulation*, 7(2), 284–318. <https://doi.org/10.1093/jfr/fjab009>

Сведения об авторах



Ярутин Ярослав Кириллович – аспирант кафедры международного права, Дипломатическая академия Министерства иностранных дел Российской Федерации, г. Москва

Адрес: 119021, Российская Федерация, г. Москва, ул. Остоженка, 53/2, стр. 1

E-mail: iaroslaviarutin@icloud.com

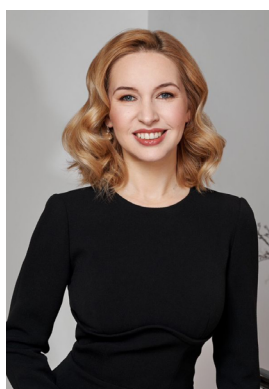
ORCID ID: <https://orcid.org/0000-0003-0036-6494>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/HJI-6696-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=w-imCpMAAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1175345



Гуляева Елена Евгеньевна – кандидат юридических наук, доцент кафедры международного права, Дипломатическая академия Министерства иностранных дел Российской Федерации

Адрес: 119021, Российская Федерация, г. Москва, ул. Остоженка, 53/2, стр. 1

E-mail: gulya-eva@yandex.ru

ORCID ID: <https://orcid.org/0009-0002-2708-8332>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56906889200>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/ISB-2036-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=KQqjjYAAAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=756727

Вклад авторов

Я. К. Ярутин осуществлял составление черновика рукописи; проведение сравнительного анализа; сбор, анализ и обобщение литературы; подготовку и редактирование текста статьи; интерпретацию общих результатов исследования; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.

Е. Е. Гуляева осуществляла формулирование идеи, исследовательских целей и задач; разработку методологии; критический пересмотр и редактирование текста рукописи; интерпретацию частных результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность руководству Клуба международного права Дипломатической академии Министерства иностранных дел Российской Федерации за организацию Международного межвузовского круглого стола, приуроченного к 220-летию Министерства юстиции Российской Федерации на тему «Актуальные проблемы международного права», на котором в рамках дискуссии авторами были высказаны отдельные идеи, получившие свое развитие в настоящей статье.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.89.25 / Право собственности

Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 20 января 2023 г.

Дата одобрения после рецензирования – 6 мая 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.32>

International and Russian Legal Regulation of the Turnover of Crypto-assets: Conceptual-Terminological Correlation

Iaroslav K. Iarutin ✉

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russian Federation

Elena E. Gulyaeva

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russian Federation

Keywords

Cryptoasset,
cryptocurrency,
digital currency,
digital technologies,
international law,
law,
legislation,
stablecoin,
token,
virtual asset

Abstract

Objective: to assess the Russian legislation for its compliance with the international-legal approaches to shaping symmetrical regulation of crypto-assets and possibility to complement it with new international-legal categories reflecting the in-depth changes in the global economy and structure of international finance, determined by the broad introduction of new financial technologies based on distributed ledger technologies.

Methods: the methodological basis of the research is a set of general scientific methods of scientific cognition, among which of utmost importance are special-legal (formal-legal and comparative-legal) methods, complemented with risk-oriented approach, legal modeling and juridical forecasting. Applied integrally, they allowed comprehending the architecture, "letter and "spirit" of the modern international financial law and national legislation in their conceptual-terminological correlation and to forecast further development and adjustment of the legal regulation of crypto-assets turnover.

✉ Corresponding author

© Iarutin Ia. K., Gulyaeva E. E., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Results: it was found that there appears a stable trend in the crypto-assets turnover regulation, according to which “soft” law dominates among the law sources (this is especially notable in the sphere of international financial law compared, for example, with conventions or international treaties); at the same time, there is a strengthening trend of “fragmentation” of international law with regard to crypto-assets turnover; the authors mark inconsistency of the conceptual framework contained in international acts and in the Russian legislation, as well as the gaps in the regime of crypto-assets turnover at the level of national law; the trends and forecasts are presented referring to the development of international-legal regulation of the sphere of crypto-assets.

Scientific novelty: consists, first of all, in a complex comparison, based on, among other aspects, the fundamentally new concepts of regulation of such progressive international-legal categories as cryptoasset, virtual asset, cryptocurrency, stablecoin, etc., some of them rarely used in the Russian legal discourse and actually never applied in legislation.

Practical significance: the scientifically grounded proposals are formulated, aimed at improving the conceptual-terminological framework of the Russian legislation in the sphere of crypto-assets turnover, implementation of which will allow constructing a common legal space with the technologically most advanced states, will help to improve investment climate and financial attraction of the state; will improve the national-legal regime of crypto-assets turnover from the viewpoint of not only actual market demands, but also state security interests and improving competitiveness of the Russian legislation.

For citation

Iarutin, Ia. K., Gulyaeva, E. E. (2023). International and Russian Legal Regulation of the Turnover of Crypto-assets: Conceptual-Terminological Correlation. *Journal of Digital Technologies and Law*, 1(3), 725–751. <https://doi.org/10.21202/jdtl.2023.32>

References

- Arestova, E. N., & Borbat, A. V. (2022). Problems of initiating criminal cases on market manipulation and illegal use of insider information. *Russian Journal of Criminology*, 16(3), 384–391. (In Russ.).
- Blemus, S., & Guégan, D. (2020). Initial crypto-asset offerings (ICOs), tokenization and corporate governance. *Capital Markets Law Journal*, 15(2), 191–223. <https://doi.org/10.1093/cmlj/kmaa005>
- Borlini, L. (2020). On Financial Nationalism and International Law: Sovereignty, Cooperation and Hard/Soft Governance in International Finance. *European Journal of International Law*, 31(3), 1133–1155. <https://doi.org/10.1093/ejil/chaa065>
- Brown-Hruska, S., & Wagener, T. (2018). The virtual currency regulatory framework in global context. *Capital Markets Law Journal*, 13(4), 487–517. <https://doi.org/10.1093/cmlj/kmy028>
- Brummer, C. (2010). Why Soft Law Dominates International Finance – and not Trade. *Journal of International Economic Law*, 13(3), 623–643. <https://doi.org/10.1093/jiel/jgq026>
- Droll, T., & Minto, A. (2022). “Hare or Hedgehog? The Role of Law in Shaping Current Technological Trends in the Securities Post-trading System”. *Accounting, Economics, and Law: A Convivium*, 1–46. <https://doi.org/10.1515/acl-2022-0029>
- Ferreira, A. (2021). The Curious Case of Stablecoins – Balancing Risks and Rewards? *Journal of International Economic Law*, 24(4), 755–778. <https://doi.org/10.1093/jiel/jgab036>

- Fogelson, Yu. B. (2013a). Soft law in the modern legal discourse (final part). *Journal of Russian Law*, 9, 43–50. (In Russ.).
- Fogelson, Yu. B. (2013b). Soft law in the modern legal discourse. *Journal of Russian Law*, 5, 37–48. (In Russ.).
- Geva, B. (2019). *Cryptocurrencies and the Evolution of Banking, Money and Payments*. In: Chris Brummer (Ed.). *crypto-assets Legal, Regulatory and Monetary Perspectives*. pp. 11–38. Oxford University Press. <https://doi.org/10.1093/oso/9780190077310.003.0002>
- Keister, T., & Sanches, D. (2023). Should Central Banks Issue Digital Currency? *The Review of Economic Studies*, 90(1), 404–431. <https://doi.org/10.1093/restud/rdac017>
- Khisamova, Z. I. (2020). Concept of central banks digital currencies: main risks in terms of observing the AML (“anti-money laundering”) and KYC (“know your client”) requirements. *Actual Problems of Economics and Law*, 14(3), 508–515. (In Russ.). <http://dx.doi.org/10.21202/1993-047X.14.2020.3.508-515>
- Kinsburskaya, V. A. (2019). Identification of cryptocurrency holders for combating illegal incomes laundering and terrorism funding. *Nota Bene*, 3, 1–13. (In Russ.). <https://doi.org/10.7256/2454-0668.2019.3.29720>
- Kinsburskaya, V. A. (2020). Requirements of FATF for regulating cryptocurrencies: problems of implementation in the national legislation. *Nota Bene*, 4, 1–18. (In Russ.). <https://doi.org/10.7256/2454-0668.2020.4.33856>
- Kudryashov, V. V. (2013a). Soft law as a method of regulating international financial relations in the foreign doctrine of international financial law. *Finansovoye pravo*, 4, 8–12. (In Russ.).
- Kudryashov, V. V. (2013b). Soft law as a method of regulating international financial relations in the foreign doctrine of international financial law (continuation). *Finansovoye pravo*, 5, 17–21. (In Russ.).
- Kudryashov, V. V. (2013c). Soft law as a method of regulating international financial relations in the foreign doctrine of international financial law. *Moskovskiy zhurnal mezhdunarodnogo prava*, 2(90), 70–89. (In Russ.). <https://doi.org/10.24833/0869-0049-2013-2-70-89>
- Kudryashov, V. V. (2014). International financial standards as a concept of regulating international financial relations. *Pravo i ekonomika*, 1(311), 64–71. (In Russ.).
- Lifshits, I. M., & Yani, P. S. (2020). Criminal liability for market manipulation according to the law of Russia and European Union. *Vserossiyskiy kriminologicheskiy zhurnal*, 14(5), 764–776. (In Russ.). [https://doi.org/10.17150/2500-4255.2020.14\(5\).764-776](https://doi.org/10.17150/2500-4255.2020.14(5).764-776)
- Mazhorina, M. V. (2018). International private law under globalization: from de-stating to fragmentation. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, 1, 193–217. (In Russ.). <https://doi.org/10.17323/2072-8166.2018.1.193.217>
- Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, 27(3), 266–291. <https://doi.org/10.1093/ijlit/eaz008>
- Ní Aoláin, F. (2021). ‘Soft Law’, Informal Lawmaking and ‘New Institutions’ in the Global Counter-Terrorism Architecture. *European Journal of International Law*, 32, 919–942. <https://doi.org/10.1093/ejil/chab071>
- Pomulev, A. A. (2021). Digital currency – an instrument for combating shadow economic activity? *Tenevaya ekonomika*, 5(4), 267–274. (In Russ.). <https://doi.org/10.18334/tek.5.4.113746>
- Rozhdestvenskaya, T. E. (2022). Risks of cryptocurrencies legalization for public law and order. In *Russia: trends and prospects of development*, 17-2, 150–155. (In Russ.).
- Rozhdestvenskaya, T. E., & Guznov, A. G. (2020). Using FATF approaches to regulating virtual assets in the legislation of the Russian Federation: prospects of development. *Vestnik Universiteta im. O. E. Kutafina*, 9, 138–146. (In Russ.). <https://doi.org/10.17803/2311-5998.2020.73.9.138-147>
- Ruchkina, G. F. (2019). Combating the illegal use of insider information and market manipulation: experience of the Bank of Russia. *Bankovskoe pravo*, 1, 9–22. (In Russ.).
- Ruchkina, G. F. (2022). Illegal practices in the securities market: on the issue of improving legal regulation. *Bankovskoye pravo*, 1, 22–29. (In Russ.).
- Salami, Iwa. (2021). Challenges and Approaches to Regulating Decentralized Finance. *AJIL Unbound*, 115, 425–429. <https://doi.org/10.1017/aju.2021.66>
- Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, 29(4), 332–363. <https://doi.org/10.1093/ijlit/eaac001>
- Sereda, A. V. (2017). Settlements with virtual currencies in the Russian Federation: analysis of the first law enforcement experience. *Sovremennyy yurist*, 2, 57–64. (In Russ.).
- Sereda, A. V. (2019). On the issue of legal regulation of blockchain technologies: analysis of foreign experience. *Problemy ekonomiki i yuridicheskoy praktiki*, 15(5), 140–143. (In Russ.).
- Tetyushin, A. V. (2022). Classification of digital financial assets and their identification in financial reporting. *Auditorskiye vedomosti*, 1, 24–29. (In Russ.).

- Tomczak, T. (2022). Crypto-assets and crypto-assets' subcategories under MiCA Regulation. *Capital Markets Law Journal*, 17(3), 365–382. <https://doi.org/10.1093/cmlj/kmac008>
- Tsang, C., & Chen, P. (2022). Policy responses to cross-border central bank digital currencies – assessing the transborder effects of digital yuan. *Capital Markets Law Journal*, 17(2), 237–261. <https://doi.org/10.1093/cmlj/kmac004>
- Vergeles, E. R. (2022). Crypto-assets: position in modern legislation. *Akademicheskaya zhizn*, 1(18), 35–37. (In Russ.).
- Verstein, A. (2019). Crypto Assets and Insider Trading Law's Domain. *Iowa Law Review*, 105(1), 1–59.
- Zellweger-Gutknecht, C., Geva, B., & Grünwald, S. N. (2021). Digital Euro, Monetary Objects, and Price Stability: A Legal Analysis. *Journal of Financial Regulation*, 7(2), 284–318. <https://doi.org/10.1093/jfr/fjab009>

Authors information



Iaroslav K. Iarutin – post-graduate student, Department of International Law, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation

Address: 53/2 Ostozhenka Str., building 1, 119021 Moscow, Russian Federation

E-mail: iaroslaviarutin@icloud.com

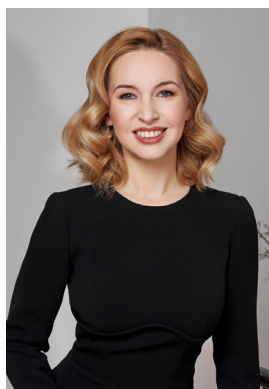
ORCID ID: <https://orcid.org/0000-0003-0036-6494>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/HJI-6696-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=w-imCpMAAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1175345



Elena E. Gulyaeva – Candidate of Sciences in Jurisprudence, Associate Professor, Department of International Law, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation

Address: 53/2 Ostozhenka Str., building 1, 119021 Moscow, Russian Federation

E-mail: gulya-eva@yandex.ru

ORCID ID: <https://orcid.org/0009-0002-2708-8332>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56906889200>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/ISB-2036-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=KQqjjYAAAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=756727

Authors' contributions

Iaroslav K. Iarutin compiled the manuscript draft; performed comparative analysis; collected, analyzed and summarized literature; prepared and edited the manuscript; interpreted the overall research results; formulated the key conclusions, proposals and recommendations; formatted the manuscript.

Elena E. Gulyaeva formulated the research idea, goals and tasks; elaborated the methodology; critically reviewed and edited the manuscript; interpreted the specific research results; approved the final version of the article.

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgement

The authors are grateful to the administrators of the International Law Club of Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation for organizing the International inter-university roundtable, commemorating the 220th anniversary of the Ministry of Justice of the Russian Federation, themed: "Topical issues of the international law", within which the authors expressed and discussed some of the ideas further developed in this article.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – January 20, 2022

Date of approval – May 6, 2022

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья

УДК 34:342.739:004

EDN: <https://elibrary.ru/hlhzbz>

DOI: <https://doi.org/10.21202/jdtl.2023.33>

Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации

Артем Павлович Перетолчин

Восточно-Сибирский институт Министерства внутренних дел Российской Федерации
г. Иркутск, Российская Федерация

Ключевые слова

Блокчейн,
законодательство,
криптовалюта,
право,
правовое регулирование,
распределенный реестр,
токен,
цифровые права,
цифровые технологии,
цифровые финансовые
активы

Аннотация

Цель: исследование существующих проблем и перспективных направлений правового регулирования цифровых финансовых активов как относительно нового инструмента современной цифровой экономики.

Методы: методологической основой работы выступает совокупность методов научного познания, таких как теоретический анализ, исследование, сопоставление, синтез, а также обобщения научной литературы.

Результаты: в работе рассмотрены существующие подходы к правовому регулированию цифровых финансовых активов в Российской Федерации и отдельных зарубежных странах, выявлены существующие пробелы отечественного законодательства в области обращения цифровых финансовых активов, дана оценка перспективам развития правового регулирования указанных инструментов и сформированы предложения по его совершенствованию. Кроме того, в процессе исследования проанализированы подходы к правовому регулированию цифровых валют и цифровых финансовых активов, принятые в ряде иностранных государств, рассмотрены тенденции и отражены положительные и отрицательные моменты использования криптографических алгоритмов для целей экономической и юридической сфер глобальной экономики.

Научная новизна: в рамках работы рассмотрены актуальные вопросы законодательного регулирования такого относительно нового явления, как цифровые финансовые активы. Проанализированы позиции отечественных и иностранных ученых-правоведов относительно существующих проблем и рисков, связанных с «токенизацией»

© Перетолчин А. П., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

и «блокчейнизацией» частного права. Помимо этого, в процессе исследования автор статьи приходит к выводу о существовании значительных пробелов в существующем подходе правового регулирования цифровых финансовых активов, указывает на них и предлагает отдельные механизмы решения данных проблем.

Практическая значимость: обусловлена несовершенством существующего законодательства в сфере регулирования отношений, возникающих в процессе использования технологий, базирующихся на базе распределенного реестра, в том числе цифровых финансовых активов. Исследование данных проблем позволяет оценить риски, рассмотреть существующие пути преодоления и разрешения возникающих дискуссионных вопросов. Кроме того, полученные в результате исследования выводы можно использовать для совершенствования отечественного законодательства, а также в учебной литературе, посвященной актуальным вопросам развития цифрового законодательства.

Для цитирования

Перетолчин, А. П. (2023). Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации. *Journal of Digital Technologies and Law*, 1(3), 752–774. <https://doi.org/10.21202/jdtl.2023.33>

Содержание

Введение

1. Генезис правового регулирования цифровых финансовых активов в Российской Федерации
2. Пробелы в российском законодательстве о цифровых финансовых активах
3. Перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации

Выводы

Список литературы

Введение

Мировые экономические кризисы последних лет вызывают значительный рост недоверия населения к традиционным финансовым инструментам, таким как банковские технологии, государственные или муниципальные ценные бумаги, инвестиционное страхование. Другим последствием катастрофически сокращающегося в результате политических и регулятивных ошибок времени между очередными глобальными потрясениями стало стремление общества к избавлению от лишних посредников в финансовом секторе. Причиной этого стали как растущие сомнения граждан в надежности политических систем, так и значительно увеличивающиеся, несмотря на повсеместную цифровизацию финансовых процессов, комиссии за базовые услуги в финансовом секторе. Данная тенденция нашла свое отражение в развитии современного направления экономики, основанного на системах,

которые позволяют устанавливать одноранговые (P2P) контакты между сторонами. Это, в свою очередь, создало существенные предпосылки для стремительного развития различных систем, базирующихся на технологии распределенного реестра, таких как блокчейн (Garcia-Teruel, 2019).

Самой популярной такой системой стал блокчейн первой цифровой валюты – биткойна, который был разработан как цифровая, неизменяемая, совместно используемая и синхронизированная база данных. Заложенные ее создателем (или создателями – до сих пор доподлинно неизвестно, кто запустил биткойн) криптографические алгоритмы, а также базовые функциональные принципы позволяют говорить о высокой надежности инструмента, а также об отсутствии необходимости в институте посредничества при реализации функционала системы.

В основу блокчейна была заложена технология так называемых смарт-контрактов, представляющих из себя последовательности компьютерных кодов, которые автоматически выполняют заранее установленные инструкции, определяемые внутренним исполняемым кодом. Смарт-контракты в настоящее время позволяют практически мгновенно переводить любую криптовалюту или цифровой актив между двумя виртуальными кошельками. Для того чтобы это стало возможным, была придумана и внедрена технология создания цифрового актива, предназначенного для удостоверения права пользователя. Этот цифровой актив в современном мире называют «токеном», а явление – «цифровой токенизацией».

Развитие технологии в дальнейшем позволило начать создавать виртуальные токены разных типов. Например, используя протокол ERC-20, стороны могут создавать взаимозаменяемые токены, которые могут быть обменены на соответствующий цифровой эквивалент, а также конвертированы. С протоколом ERC-721 стало возможным создание невзаимозаменяемых токенов, которые включают в свои метаданные некоторые конкретные свойства и характеристики, которые отличают их от других токенов и делают уникальными. Это открыло миру широкие перспективы использования цифровых активов не только в финансовом секторе, но и в других отраслях, таких как медицина, нотариат, государственная регистрация, туризм, образование и т. д.

В итоге за последние годы цифровые финансовые активы (далее – ЦФА) становятся все более востребованным инструментом в системе коммерческих и иных взаимоотношений в киберпространстве и даже за его пределами. Высокий интерес к ЦФА, а также к связанным с ними процессам обусловлен глобальной цифровизацией. Происходящие в настоящее время трансформации в сфере экономики и информационных технологий позволяют упростить различные виды деятельности человека, в том числе и в области финансовых отношений. К тому же одним из ключевых факторов, стимулирующих процесс виртуализации отдельных экономических процессов, стала глобальная пандемия. Рост популярности цифровых денег, в частности криптовалют, вызвал потребность в их правовом регулировании.

Цифровая токенизация в различных сферах деятельности человека и в киберпространстве может дать в будущем целый ряд преимуществ, таких как потенциально более дешевые и безопасные транзакции, повышенная прозрачность транзакционных данных и информации об эмитенте, предоставление инвесторам прямого доступа к первичным и вторичным рынкам, повышение уровня ликвидности активов, в том числе цифровых, с точки зрения возможности их реализации среди гораздо

более широкого круга участников. В сфере недвижимости эта технология может быть использована для разработки будущих платформ, облегчающих трансграничные транзакции с активами недвижимости в России и во всем мире, и в то же время за счет заложенных в основе технологии криптографических алгоритмов безопасности противостоять вызовам, связанным с цифровизацией глобальной экономики в условиях меняющегося баланса сил в мире и новой экономической реальностью, которая возникает после кризиса COVID-19 (Garcia-Teruel, 2020).

Следует отметить, что развитие таких интернет-инициатив благоприятно сказывается и на экономических процессах, происходящих внутри отдельно взятых государств, увеличивает их инвестиционную привлекательность, раскрывает экономический и интеллектуальный потенциал. Но наличие установленных случаев нарушения прав и интересов участников экономических отношений в сфере обращения ЦФА, а также ущемление интересов государства и общества позволяют сделать вывод о необходимости создания продуманной и актуальной нормативной базы, регламентирующей порядок функционирования и обеспечения работы указанных систем на определенной территории.

Определенные попытки действий в данном направлении были предприняты в целом ряде государств, например, в Германии, Франции, Италии, США, Монако, Люксембурге, Мальте. Отдельные страны Азии в принципе запретили криптовалюты в качестве средства платежа, например, Китай и Вьетнам, в то время как в ряде других они не признаются таковыми вообще (например, на Филиппинах или в Малайзии) (Garcia-Teruel & Simón-Moreno, 2021). Другие страны, такие как Португалия, не предприняли никаких действий по этому вопросу и ограничились проведением предупредительной и профилактической работы с инвесторами, направленной на информирование о сложностях и рисках, связанных с оборотом криптовалюты и других цифровых финансовых активов (Basilio, 2019). Ряд прогрессивных стран предприняли попытки интегрировать технологию распределенного реестра в существующие государственные процессы, например, Швеция и Грузия в качестве эксперимента применяют отдельный функционал блокчейна для регистрации земельных сделок и ведения их кадастрового учета.

Не осталась в стороне и Российская Федерация, которая также ищет актуальные и перспективные подходы к правовому регулированию криптовалют и цифровых финансовых активов. Здесь, прежде всего, следует акцентировать внимание на новеллу в процессе правового регулирования современных криптографических инструментов, которой является Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»¹ (далее – Закон о цифровых финансовых активах), вступивший в законную силу с 1 января 2021 г.

Однако сама структура и содержание вышеуказанного закона предусматривают выстраивание целой системы законодательных и подзаконных актов, направленных на регулирование современных блокчейн-технологий и созданных на их базе инструментов, в том числе и таких, как криптовалюты, цифровые финансовые активы. Но до настоящего времени такая структура выстроена не была, что в конечном итоге

¹ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ от 31.07.2020. (2020). *Собрание законодательства Российской Федерации*, 31 (ч. I), ст. 5018.

создает существенные сложности в правовом регулировании рассматриваемых технологий, приводит к ограниченности и узкопрофильности принятого закона, а в отдельных случаях и к нулевой эффективности и невозможности применения некоторых его норм. В связи с чем представляется целесообразным проведение анализа и формирование предложений по преодолению существующих проблем и пробелов в правовом регулировании общественных отношений, связанных с цифровыми валютами и ЦФА. В рамках данной статьи прежде всего будут рассмотрены вопросы правовой регламентации цифровых финансовых активов.

Представляется, что проблемы, связанные с системным анализом развития и правового регулирования цифровых финансовых активов, в настоящее время недостаточно проработаны.

Для достижения заявленных целей исследования следует признать целесообразным решение следующих задач:

- изучить существующие подходы к правовому регулированию цифровых финансовых активов в Российской Федерации и отдельных зарубежных странах;
- выявить существующие пробелы отечественного законодательства в области обращения ЦФА;
- оценить перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации.

Предметом рассмотрения являются административные и гражданско-правовые нормы, регулирующие порядок обращения ЦФА, а также практика применения соответствующих правовых норм и позиции ученых относительно эффективности существующей в Российской Федерации системы правового регулирования ЦФА.

Предполагается, что теоретическая и практическая значимость данного исследования заключается в выводах, которые могут быть использованы как в научно-исследовательской деятельности по данному направлению, так и в законотворчестве при разработке и совершенствовании административного, уголовного и гражданско-правового законодательства.

1. Генезис правового регулирования цифровых финансовых активов в Российской Федерации

С момента появления и развития блокчейна, цифровых валют и связанных с ними криптографических финансовых инструментов в отечественной правовой доктрине высказывались различные мнения и подходы относительно необходимости законодательного регулирования криптовалют и токенов. Одни ученые выступали за необходимость точечной регламентации оборота цифровых активов и только в тех случаях, где эта необходимость назрела, так как установление жестких регламентов в сфере обращения цифровых валют, по их мнению, противоречит самой сути данного явления, его истокам (Кудряшова, 2018). Другие представители научного сообщества настаивали на разработке всестороннего регулятивного законодательства процессов цифровизации и токенизации (Рыжов, 2018).

Впервые на официальном уровне о необходимости правового регулирования криптовалют в России заговорили около девяти лет назад. В январе 2014 г. были опубликованы рекомендации Банка России «Об использовании при совершении сделок “виртуальных валют”, в частности, биткойн», в соответствии с которыми было предложено рассматривать криптовалюту в качестве денежного суррогата,

а ее использование при совершении сделок – в качестве основания для рассмотрения вопроса об отнесении таких сделок (операций) к числу направленных на финансирование терроризма². Позицию Банка России по отнесению криптовалют к денежному суррогату на тот момент поддержали и Росфинмониторинг³, и Генеральная прокуратура Российской Федерации⁴.

В течение длительного периода роль цифровых финансовых активов и цифровой валюты в отечественной системе объектов гражданских прав не была определена, поскольку они не выделялись как самостоятельный объект гражданского права и их правовая природа не позволяла отнести их к каким-либо объектам правоотношений, обозначенных в ст. 128 Гражданского кодекса Российской Федерации⁵ (далее – ГК РФ). Это привело к формированию и утверждению противоположных подходов в правоприменительной практике судов и государственных органов в вопросе о том, являются ли цифровые финансовые активы и цифровая валюта объектами гражданских прав и не ограничен ли их оборот.

В октябре 2017 г. Президент Российской Федерации в рамках реализации программы «Цифровая экономика Российской Федерации» поручил Правительству Российской Федерации и Банку России обеспечить внесение изменений в законодательство Российской Федерации, определяющих статус современных цифровых и криптографических технологий, используемых в финансовом секторе, и определить условия их правового регулирования, основанные на подходе, согласно которому рубль является единственным законным средством платежа на территории Российской Федерации.

В результате появился Федеральный закон от 31 июля 2020 г. № 259-ФЗ, в соответствии с которым цифровые финансовые активы⁶ были признаны цифровыми правами. Цифровые права, в свою очередь, согласно ст. 128 ГК РФ, выступают в качестве имущественных прав. Справедливость данного вывода находит свое подтверждение и в комментариях Комитета Совета Федерации по бюджету и финансовым рынкам⁷.

² Банк России. (2014, 27 января). Об использовании при совершении сделок «виртуальных валют», в частности, биткойн. https://www.cbr.ru/press/pr/?file=27012014_1825052.htm

³ Федеральная служба по финансовому мониторингу. (2014, 6 февраля). Об использовании криптовалют. <https://www.fedsfm.ru/news/957>

⁴ В Генеральной прокуратуре Российской Федерации состоялось совещание по вопросу правомерности использования анонимных платежных систем и криптовалют. Официальный сайт Генеральной прокуратуры РФ. <https://epp.genproc.gov.ru/web/gprf/search?article=83101813>

⁵ Гражданский кодекс Российской Федерации. (1994, 5 декабря). (1994). *Собрание законодательства Российской Федерации*, 32, ст. 3301.

⁶ «Цифровыми финансовыми активами признаются цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы». (О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ от 31.07.2020. (2020). *Собрание законодательства Российской Федерации*, 31 (ч. I), ст. 5018).

⁷ Заключение по Федеральному закону «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (проект № 419059-7). Официальный сайт Совета Федерации Федерального Собрания Российской Федерации. http://budget.council.gov.ru/activity/legislation/resolutions_law/118341

В криптографическом мире ЦФА чаще всего выступают в качестве так называемых токенов и являются, по сути, цифровыми единицами учета, выпускаемыми конкретными лицами, в ценность которых заложены различные товары, услуги, акции, права и т. д. В соответствии с российским законодательством цифровые финансовые активы могут включать в себя:

- 1) ЦФА как право требования;
- 2) ЦФА на право участия в непубличном акционерном обществе;
- 3) ЦФА на права по эмиссионным ценным бумагам;
- 4) гибридные ЦФА, которые дополняются признаками утилитарного цифрового права.

Стоит также отметить, что для выпуска цифровых финансовых активов достаточно всего одного документа – решения о выпуске ЦФА, которое содержит в себе все основные реквизиты актива и все его основные параметры (стоимость, количество, информацию об эмитенте и пр.). Данный документ является ключевым для запуска цифрового актива в оборот.

Российское законодательство подразумевает использование системы распределенных реестров для оборота ЦФА, так называемого блокчейна. Эта технология упрощает оборот финансовых активов в связи с тем, что она обладает следующими важнейшими свойствами: неизменность информации внутри системы, операционная устойчивость, взаимная зависимость блоков внутри системы, устойчивость от взлома, а также эффективность, обусловленная тем, что распределенные системы гораздо дешевле централизованных.

Для наилучшего понимания инструмента цифровых финансовых активов следует сравнить их с действующими инструментами, которые уже есть на рынке.

1. Самым распространенным инструментом являются ЦФА как денежное требование.

Денежное требование – это требование передачи рублей или иной иностранной валюты. Специфика ЦФА обуславливает также, что они могут выступать в качестве права требования по передаче цифровой валюты. Однако следует подчеркнуть, что криптовалюты, в частности биткоин или эфир, по федеральному законодательству хоть и рассматриваются в качестве возможного средства платежа, но к деньгам не относятся.

Больше всего данный вид ЦФА похож на облигацию или кредит. Все зависит от того, что будет положено в основу указанного цифрового финансового актива. Например, если это решение подразумевает систематическую фиксированную выплату инвестору, то в данном случае мы можем говорить о сходстве с облигациями с купонным доходом.

Отличительным признаком ЦФА от классической облигации является то, что данный инструмент гораздо доступнее для рынка как с позиции инвесторов, так и эмитентов. Эмитент любого размера может выпустить ЦФА, и его привлекательность для инвесторов будет зависеть только от надежности самого эмитента и степени доверия к нему, что, в свою очередь, побуждает эмитентов вести свой бизнес более открыто и надежно.

Стоит отметить, что данный вид ЦФА сам по себе является денежным требованием инвестора к эмитенту. Таким образом, эмитент не сможет перевести обязательства выплаты по данным правам на третье лицо, например на своего должника. Это очень важно, поскольку основным фактором при принятии инвесторами решения о вложениях в данный тип ЦФА выступает, прежде всего, надежность эмитента, а не его должников.

2. Следующим видом являются ЦФА на право участия в капитале непубличного акционерного общества. Данный вид цифрового финансового актива подходит

для создания нового непубличного акционерного общества. Хотя при помощи этого инструмента нельзя токенизировать старое непубличное акционерное общество, но в сфере крупного бизнеса данный инструмент применим для быстрого создания совместных предприятий. Соответственно такой функционал ЦФА служит для привлечения долевого финансирования (так называемого equity financing), если участником совместного предприятия будет, например, банк. Малому бизнесу и перспективным стартапам ЦФА на право участия в капитале непубличного акционерного общества подходит для проведения ICO (Initial Coin Offering), т. е. первичного размещения цифровых акций в полном соответствии с законодательством РФ.

3. Еще одним инструментом выступают ЦФА на права по эмиссионным бумагам. Определение эмиссионных ценных бумаг содержится в ст. 2 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» – это различные ценные бумаги, характеризующиеся одновременно такими признаками, как равные объем и сроки осуществления прав внутри одного выпуска; соблюдение установленных в законе формы и порядка закрепления совокупности имущественных и неимущественных прав; размещение выпусками или дополнительными выпусками⁸.

Согласно российскому законодательству, к числу эмиссионных ценных бумаг относятся акции, облигации, опционы эмитента, а также российские депозитарные расписки.

4. Гибридные цифровые финансовые активы – это цифровые права, включающие одновременно ЦФА и иные цифровые права. К иным цифровым правам, в частности, относится право пользования услугой, товаром, скидкой. Другими словами, гибридные ЦФА имеют признаки как цифровых финансовых активов, так и утилитарного цифрового права.

Примером гибридного цифрового финансового актива является стейблкоин. Стейблкоины не являются однородными и способны обладать различными экономико-правовыми признаками. Большая часть стейблкоинов выпускается четко идентифицированными эмитентами на базе блокчейна как в форме обращающихся цифровых обязательств, так и депозитарных расписок, применяющихся в качестве средства обмена, сбережения и платежа. Самыми распространенными стейблкоинами являются централизованные, которые обеспечены фиатными валютами и золотом. Такие стейблкоины применяются для совершения биржевых обменных операций или розничных платежей. Локальные стейблкоины используются как средство сохранения стоимости, так и средство обмена. Глобальные стейблкоины способны ускорить трансграничные расчеты и снизить их себестоимость, а также повысить уровень финансовой доступности криптоактивов для пользователей без необходимости открытия счетов.

Указанный законодательный подход является значительным шагом в процессе легализации ЦФА и создает хорошую платформу для дальнейшего развития создаваемой системы правового регулирования. Тем не менее для реализации потенциальных преимуществ использования различных инструментов ЦФА необходимо решить правовые, нормативные и надзорные проблемы, которые связаны с национальным и трансграничным обращением.

⁸ О рынке ценных бумаг. № 39-ФЗ от 22.04.1996. *Собрание законодательства Российской Федерации*, 17, ст. 1918.

2. Пробелы в российском законодательстве о цифровых финансовых активах

В последние годы рынок криптовалют набирает обороты. Несмотря на значительное падение на 65 % в 2022 г., стоит отметить, что в определенный момент общая капитализация криптовалют составляла более \$2,4 трлн. И в настоящее время есть все основания предполагать, что актуальные мировые кризисы и вызовы, а также преимущества и перспективы технологии блокчейна будут способствовать возвращению рынка на прежние позиции в будущем и, вполне вероятно, значительному росту в дальнейшем. В связи с чем стоящие перед активно работающими с современными криптографическими финансовыми инструментами компаниями и физическими лицами вопросы легализации полученных доходов и реализации своей деятельности в правовом поле актуальны до сих пор⁹.

Кроме того, в научном сообществе активно обсуждают, помимо технологических аспектов системы, возможности и перспективы применения блокчейна к потребностям рынка и общества (Raskin, 2017), возможности токенизации прав собственности (Yapicioglu & Leshinsky, 2020), в том числе в контексте возможных изменений существующих процессов регистрации и ведения земельных и кадастровых реестров, реестров недвижимости, а также иных учетных баз (Verhey, 2017). Представляется, что возможности использования распределенного реестра и технологий невзаимозаменяемых токенов (далее – NFT) необходимо внедрять в эти процессы уже сейчас, так как это открывает широкие возможности для оптимизации деятельности государственных органов, совершенствования качества оказываемых государством услуг и оптимизации бюджетных трат.

Ряд ученых указывают также на отдельные проблемы, связанные с рисками «токенизации» и «блокчейнизации» частного права (Savelyev, 2018). Одним из актуальных и перспективных вопросов здесь видится потенциальная возможность замены существующего механизма передачи прав собственности новыми закодированными правилами, используемыми в рамках технологии блокчейн и цифровых токенов. Однако в этой связи существует серьезная потребность в качественном определении юридической природы таких токенов и разработке регулятивного законодательства в сфере цифровизации собственности (Ishmaev, 2017; Василевская, 2019). Полагаем, что здесь весьма успешно можно применять технологии NFT.

Другим интересным и дискуссионным вопросом видится экстраполяция договорных и имущественных отношений на смарт-контракты, что может привести, по мнению некоторых авторов, к началу конца «классического» договорного права (Savelyev, 2017). Вместе с тем отдельные исследователи полагают, что выбор того, какую технологию применять в рамках реализации своих прав и обязанностей, должен оставаться за гражданами и они должны иметь возможность использовать как классические концепции договорного права, так и современные, реализованные посредством криптографических алгоритмов (Konashevych, 2020). Мы с этим полностью согласны. Во всяком случае в условиях нынешнего переходного этапа.

Обозначенные выше вопросы и многие другие формируют для современных и будущих законодателей и научного сообщества серьезный вызов, который

⁹ «Закон о ЦФА разочаровал». Юристы о проблемах регулирования криптовалют. (2021, 25 января). *rbc.ru*. <https://www.rbc.ru/crypto/news/600eba6f9a79470a85424efa>

заключается в необходимости глубокого аналитического осмысления технологий, их правовой природы, рисков и перспектив. И создание на основе данного анализа актуального, современного и эффективного законодательства, способного не только облегчить жизнь граждан, но и успешно защитить их интересы.

Видится, что данный процесс должен реализовываться поэтапно, в тесном сотрудничестве практиков и теоретиков права, а также специалистов в области информационных технологий. Несмотря на то, что в России с 1 января 2021 г. в силу вступил федеральный закон, регулирующий ЦФА, некоторые вопросы все же остались нераскрытыми.

Настоящий нормативный правовой акт регулирует отношения, связанные с использованием новых цифровых инструментов, которые могут оказать существенное влияние на российский финансовый рынок. Законодатель РФ воздержался от полного запрета криптовалюты и цифровых токенов, поскольку такое табу могло бы привести к существенному развитию отдельных сегментов теневой экономики. Однако в рамках данного закона был предусмотрен целый ряд ограничений процесса обращения цифровых финансовых активов.

Как уже было отмечено ранее, к категории цифровых финансовых активов отечественный законодатель отнес отдельные права обладания и осуществления операций, реализованные в информационной системе, которая отвечает закрепленным в законодательстве требованиям. Что уже вызвало массу вопросов, так как в значительной степени противоречит складывающейся мировой практике и фактическим обстоятельствам.

Кроме того, не оправдались ожидания того, что Закон о цифровых финансовых активах урегулирует как процесс первичного размещения цифровых финансовых активов (ICO), так и процедуру выпуска и обращения виртуальной валюты, включая криптовалюты, а также майнинг. А особенности инвестирования с использованием цифровых инструментов, основанных на системе блокчейн, по-прежнему вызывают серьезные споры в российском юридическом сообществе ([Sarnakov, 2019](#)).

На этапе рассмотрения и принятия Закона о цифровых финансовых активах Центральный банк Российской Федерации, Министерство экономического развития Российской Федерации, Федеральная служба по финансовому мониторингу и Генеральная прокуратура Российской Федерации, действовавшие, как уже было отмечено выше, изначально согласованно, выразили радикально противоположные позиции относительно того, как регулировать ЦФА, что во многом замедлило принятие закона и привело к трем серьезным изменениям текста законопроекта ([Emtseva, & Morozov, 2018](#)).

Трудности с принятием Закона о цифровых финансовых активах показали, что российский законодатель не смог быстро определить, что такое криптовалюта и ЦФА и как их регулировать. В то же время в заключительной редакции проекта законодатель все же отметил, что указанные криптографические инструменты существуют, однако не объяснил в полной мере как они регулируются. В связи с чем порядок их оборота в значительной степени остался вне правового регулирования.

Между тем тот факт, что криптовалюта рассматривается в качестве потенциального объекта гражданских прав в перспективе, показывает, что в ближайшем будущем все же следует ожидать принятия нормативного правового акта, который будет регулировать порядок ее использования.

Что касается цифровых финансовых активов, называемых в криптографической среде токенами, большинство положений рассматриваемого закона посвящено именно им, а также процедуре их выпуска. В связи с этим представляется актуальной

необходимость изучения того, какие риски и выгоды они несут для российских инвесторов и других участников финансового рынка, а также соответствуют ли они тенденциям развития цифровой экономики.

Так, до принятия закона российские ученые выражали различные опасения, связанные с токенами. В частности, указывалось, что существующие правовые режимы объектов гражданских прав могут быть заменены правовым режимом токена (Savelyev, 2018), подчеркивалось, что возникает проблема определения характера прав на токены и средств правовой защиты их владельцев (Belykh & Bolobonova, 2019). Кроме того, были выражены определенные опасения по поводу сложностей налогообложения (Troyanskaya et al., 2020; Григорьев, 2020).

Таким образом, принятие Закона о цифровых финансовых активах обуславливает необходимость рассмотрения основных положений законодательства, касающихся цифровых финансовых активов, его влияния на финансовый рынок и инвесторов, а также сферы финансовых технологий.

Принятая в итоге версия законопроекта во многом аналогична его второй редакции, однако, в отличие от нее, содержит меньше запретов и ограничений, которые распространяются на оборот цифровых токенов. Российские научные изыскатели называют этот вариант, в отличие от двух предыдущих, компромиссным (Рождественская, Гузнов, 2020). Действительно, из его текста были исключены многие положения, препятствующие легализации ЦФА.

Несмотря на то, что в целом принятый подход к регулированию ЦФА и их выпуска был достаточно полно отражен в принятом нормативном правовом акте, в нем все еще имеются существенные недостатки, в частности вызванные вопросами определения правового статуса рассматриваемых инструментов.

Согласно ст. 1 рассматриваемого Закона, цифровые финансовые активы – это не что иное, как определенный объект, существующий в цифровой форме и удостоверяющий корпоративные права их владельца. Данный тезис прямо следует из ч. 4 ст. 1 Закона, согласно которой вопросы выпуска цифровых токенов, если они удостоверяют права на ценные бумаги, субсидиарно регулируются Федеральным законом от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг»¹⁰ с учетом особенностей, предусмотренных настоящим Законом о цифровых финансовых активах.

Из вышесказанного становится очевидным, что в Законе о цифровых финансовых активах понятие цифровых финансовых активов исходит из принятого в криптографическом сообществе понятия токена, однако существенно сужает его. Кроме того, в законе не предусмотрено разделение цифровых финансовых активов на типы в зависимости от их назначения. Это не учитывает реальную ситуацию, в рамках которой существуют инвестиционные, сырьевые, служебные, гибридные и иные виды токенов. В то время как инвестиционные токены подтверждают право на участие в управлении компанией, служебные токены не обладают этими качествами и подтверждают лишь право на какую-либо вещь (услугу) или скидку. Оба типа данных токенов принципиально отличаются друг от друга, а это значит, что они требуют разных подходов к регулированию их выпуска и обращения.

¹⁰ О рынке ценных бумаг. № 39-ФЗ от 22.04.1996. (1996). *Собрание законодательства Российской Федерации*, 17, ст. 1918.

В то же время гибридные цифровые финансовые активы (возможность выпуска которых в соответствии с Законом о цифровых финансовых активах прямо не прописана, но подразумевается) представляют из себя цифровые права, включающие одновременно и ЦФА, и иные цифровые права. Иными словами, гибридные ЦФА имеют признаки как цифровых финансовых активов, так и утилитарного цифрового права.

В связи с этим принятие единой процедуры выпуска и учета всех цифровых активов в едином механизме ставит под сомнение возможность легального обращения отдельных типов токенов в России. Этот шаг российского законодателя нельзя оценить положительно. Представляется, что целесообразно провести разграничение токенов по видам, так как различия в назначении токенов определяют различный порядок их оборота и использования, что также нуждается в соответствующей правовой регламентации, в целях устранения возможных разночтений и формирования четких механизмов выпуска и оборота соответствующих активов.

Таким образом, Закон о цифровых финансовых активах не содержит четкого соответствующего современным реалиям понятия токенов, не раскрывает их актуальных свойств. В нем перечислены только те права, которые могут быть ими подтверждены. Представляется, что такое положение дел является серьезным изъяном в законодательстве и не будет способствовать внесению ясности в сферу правового регулирования цифровых технологий. В связи с этим российскому законодателю следует внести поправки в закон или выпустить официальное разъяснение, которое позволит отличать различные типы цифровых финансовых прав друг от друга.

Исходя из положения п. 5 ст. 1 Закона о цифровых финансовых активах, к первичному размещению токенов (ICO) применяется российское законодательство. Это правило применяется даже в том случае, если цифровые токены выпущены с участием иностранных юридических лиц. Такое правовое закрепление подтверждает верховенство российского законодательства, что нельзя назвать чрезмерным ограничением. Это соответствует международным тенденциям, касающимся ICO.

Так, например, в Сингапуре, который по праву признан исследователями одним из лидеров в области цифровизации, на основании п. 339 Закона о ценных бумагах и фьючерсах, в случае приобретения гражданином Сингапура цифровых токенов законодательство Сингапура применяется экстерриториально к иностранному оператору платформы, на базе которой осуществляется размещение таких цифровых токенов (Gorian, 2020). Следовательно, лица, проводящие ICO и находящиеся за пределами Сингапура, должны иметь соответствующую лицензию, выданную компетентным органом этого государства. Такой подход обеспечивает правовую основу для судебного преследования операторов платформ независимо от их местонахождения и места, где было совершено преступление. Таким образом, экстерриториальное применение российского законодательства к лицам, осуществляющим ICO в России, можно оценить положительно, однако компетентным органам следует дать официальные разъяснения, чтобы иностранные организации, привлекающие средства российских инвесторов, понимали последствия деятельности в России.

Кроме того, следует решить, как будет регулироваться ICO, если российское законодательство вступит в противоречие с иностранным законодательством. Эти вопросы чрезвычайно важны и должны быть решены в процессе разработки регулятивного законодательства во исполнение Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Представляется,

что в случае реализации первичного выпуска токена в российском сегменте лицом, находящимся в российской юрисдикции, приоритетным должно выступать отечественное правовое регулирование.

Статьи 2, 3 и 15 Закона о цифровых финансовых активах устанавливают правила ICO. Таким образом, проводить ICO может только непубличное акционерное общество. В то же время только лицензированная организация может регистрировать выпуск токенов и хранить записи о совершенных с ними операциях. Это требование направлено на защиту прав инвесторов, а также на поддержание стабильности фондового рынка.

ICO может быть проведено только на основании решения, соответствующего требованиям ст. 3 Закона о цифровых финансовых активах. Так, в частности, решение о выпуске цифровых финансовых активов должно содержать информацию об эмитенте цифровых токенов; информацию о типе прав, удостоверенных токенами, количестве токенов, их цене, а также способе их оплаты; информацию об операторе информационной системы, в которой выпускаются цифровые финансовые активы, и т. д.

Несмотря на то, что перечень информации, которая должна быть отражена в решении по данному вопросу, достаточно широк, Центральный банк России вправе устанавливать дополнительные требования к решению о выпуске цифровых финансовых активов. Это демонстрирует его ключевую роль в выпуске подзаконных актов в области цифровых финансовых активов.

Учитывая тот факт, что размещение токенов происходит в цифровой среде, законодатель предусмотрел требование о том, что решение о выпуске ЦФА должно быть подписано усиленной квалифицированной электронной подписью и размещено на веб-сайте эмитента и оператора информационной системы. Это положение закона позволяет гарантировать, что решение о выпуске токенов действительно исходит от человека, который вправе это сделать.

Анализ положений Закона о цифровых финансовых активах и их сравнение с правилами выпуска акций позволяет сказать, что российское законодательство максимально приблизило правила ICO к тому, как осуществляется выпуск акций. Из закона ясно, что в Российской Федерации к ЦФА принят подход, аналогичный подходу к регулированию ценных бумаг (Alekseenko, 2020). Такой подход не является российским изобретением. Так, в Сингапуре, согласно Закону о ценных бумагах и фьючерсах, токен рассматривается как цифровое выражение ценной бумаги. Опыт применения законодательства о ценных бумагах к токенам имеется и в других странах.

Принятие в России Закона о цифровых финансовых активах является одним из важнейших событий для страны. С его помощью значительный сегмент цифровой экономики будет выведен из тени. Несмотря на проявленное в 2018 г. стремление сохранить баланс между тотальным контролем и «анархией» в правоотношениях, связанных с цифровыми активами, законодатель все же пошел по пути ужесточения контроля. Это было сделано для защиты прав инвесторов, но в то же время для защиты интересов государства в финансовом секторе. Государство, четко установив контроль за оборотом цифровых финансовых активов, с одной стороны, снизит свои риски, а с другой – сможет обеспечить судебную защиту обманутым инвесторам. Между тем обоснованность методов, выбранных Россией для регулирования деятельности операторов ICO, по-прежнему вызывает сомнения. Принятые правила дают больше преимуществ крупным инвестиционным банкам и IT-компаниям. Это может негативно сказаться на развитии начинающих проектов.

3. Перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации

После принятия Федерального закона от 31 июля 2020 г. № 259-ФЗ со стороны Федеральной налоговой службы (далее – ФНС России) поступило предложение о внесении соответствующих поправок в Налоговый кодекс Российской Федерации. В процессе рассмотрения законопроект неоднократно критиковался специалистами в области финансов, но в итоге поправки в соответствующее законодательство уже в первом чтении были одобрены Государственной Думой Российской Федерации в феврале 2021 г.

Одним из предложений ФНС России стало введение налога на криптовалюту, так как она была официально приравнена к имущественным активам. Также ФНС России считает необходимым обязать всех граждан, владеющих ЦФА и иными криптоактивами, уведомлять о совершении сделок, превышающих сумму в шестьсот тысяч рублей. За просрочку в предоставлении соответствующей информации предлагается ввести штраф – 10 % от суммы совершенных сделок, а за уклонение от уплаты налогов на криптовалюты – 40 %. Уведомлять же ФНС России предлагалось в срок до 30 апреля соответствующего года.

В свою очередь, Министерство финансов Российской Федерации приступило к разработке поправок в Уголовный кодекс РФ: неоднократное уклонение от уплаты налогов по результатам вышеуказанной деятельности предлагалось наказывать штрафом, принудительными работами, а в особых случаях и лишением свободы в ситуации, когда сумма произведенных за три года операций будет соответствовать крупному или особо крупному размеру. Однако в настоящее время многие из рассматриваемых вопросов и предложений не были реализованы в полной мере.

Стоит отметить, что Федеральный закон от 31 июля 2020 г. № 259-ФЗ хотя и заложил основы регулирования цифровой финансовой отрасли, но не является совершенным. Это обусловлено тем, что на сегодняшний момент отсутствует ответ на вопрос, что делать физическим или юридическим лицам, чтобы инвестиции в криптовалюты и ЦФА либо операции с криптовалютами и ЦФА не несли существенных рисков, связанных с нарушением законодательства.

С положительной стороны отметим то, что в рассматриваемом законе разграничены такие понятия, как цифровые валюты и цифровые финансовые активы. Понятие цифровых валют, изложенное в законе, в большей степени соответствует классическому подходу к определению криптовалют, под которыми понимаются монеты, эмитированные в рамках собственного независимого блокчейна. При этом законодатель отмечает, что в отношении цифровых валют, представляющих собой совокупность электронных данных, содержащихся в информационной системе, отсутствует лицо, обязанное перед каждым обладателем таких электронных данных. В то же время цифровые финансовые активы, как уже было отмечено ранее, по своему определению более близки к криптографическим токенам (но лишь отчасти), которые, в свою очередь, функционируют на базе уже существующих блокчейнов отдельных криптовалют. Вышеизложенное позволяет нам сделать вывод о том, что Закон разделяет криптовалюты, такие как Bitcoin или Ethereum, и цифровые финансовые активы, такие как токен DAI, функционирующий в экосистеме блокчейна Ethereum, или токен TRC-20, использующий блокчейн цифровой валюты Tron. Такой

подход в значительной степени соответствует современным криптографическим реалиям, и мы считаем целесообразным продолжать развивать отечественное законодательство через призму именно такой позиции.

Вместе с тем закон содержит бланкетные нормы, согласно которым правовое регулирование оборота цифровых валют осуществляется в соответствии с федеральным законодательством. При этом такое федеральное законодательство в установленном порядке принято до сих пор не было. Объясняется это как существующими сложностями в определении эффективных подходов к законодательному регулированию криптовалют, так и необходимостью соблюдения баланса между интересами государства в контроле происходящих на его территории финансовых потоков и пользователей, которых привлекает в криптовалютах именно отсутствие внешнего властного регулятора. В итоге на данный момент на территории Российской Федерации не предусмотрено каких-либо ограничений и особых условий для приобретения и реализации криптовалюты, за исключением частных случаев, оговоренных в специальном законодательстве или во внутренних ведомственных предписаниях. Например, в соответствии с информационным письмом Минтруда России от 16 декабря 2020 г. № 18-2/10/В-12085¹¹, чиновникам и сотрудникам силовых структур не разрешено приобретать и продавать криптовалюту.

Другой проблемой видятся отдельные аспекты, связанные с регулированием деятельности обменных систем и цифровых бирж. Представляется, что в законе они определены как «операторы обмена цифровых финансовых активов» и в целом данная дефиниция соотносится с существующим подходом к определению криптобирж и криптообменников. Вместе с тем остаются открытыми вопросы, признаются ли на территории Российской Федерации зарубежные обменные платформы и системы, каков порядок лицензирования операторов, юрисдикционное взаимодействие, регулирование ответственности за нарушение прав пользователей.

Аналогичные вопросы вызывает и порядок эмитирования цифровых валют и цифровых финансовых активов. Отдельные моменты, связанные с противодействием отмыванию денежных средств, распространению наркотических веществ, коррупционным преступлениям, определены в специальном законодательстве. Однако общий порядок лицензирования эмитентов криптовалют и токенов на территории Российской Федерации не определен, что создает сложности с обеспечением должного уровня защиты прав граждан и участников оборота цифровых активов.

Обозначенные проблемы открывают широкий спектр перспективных направлений развития как законодательства Российской Федерации, так и цифровизации различных сторон жизни общества, повышению эффективности взаимодействия граждан и государства.

Помимо обозначенных ранее, к таким направлениям также можно отнести совершенствование взаимодействия и выравнивание баланса между крупными банковскими учреждениями и малыми и средними финансово-кредитными организациями. Специфика цифровых транзакций в настоящее время такова, что в них могут принимать активное участие в том числе небольшие компании и частные лица. Однако крупные финансово-кредитные организации чаще всего укомплектованы

¹¹ Письмо Минтруда России № 18-2/10/В-12085 от 16 декабря 2020 г. <https://mintrud.gov.ru/docs/mintrud/employment/62>

квалифицированными кадрами, лучше оснащены технически, что позволяет им проводить более агрессивную политику на рынке, устанавливать неоправданно завышенные цены на свои услуги, вытеснять других участников сектора цифровых финансовых услуг. Но, как показывает опыт появления и развития криптовалют, в настоящее время в обществе назрела серьезная потребность уменьшения зависимости от сторонних регуляторов, в том числе посредством распределения ответственности между большим числом участников рынка в целях уменьшения уровня возможностей влияния крупных игроков на экономику как в частном сегменте, так и на глобальном уровне.

При этом важно соблюсти баланс, который позволил бы государству в лице, уполномоченных органов исполнительной власти, в том числе Центрального банка России, обеспечивать устойчивость большого числа относительно разрозненных цифровых финансовых экосистем и осуществлять контроль их деятельности, не ограничивая при этом их развитие. Решение этой задачи представляется крайне сложным, но важным перспективным направлением развития рынка цифровых финансовых активов в России. И от эффективности реализации данной задачи во многом зависит будущее страны, а с учетом существующих политических реалий, и возможности выживания отдельных отраслей экономики.

На основании изложенного можно сделать вывод о том, что для дальнейшего эффективного функционирования и развития государства необходимо как уточнение отдельных законодательных актов, так и разработка фактически с нуля широкого спектра нормативного регулирования новых сфер цифровой трансформации общества. Ключевым в этом процессе станет не только сбалансированность выстраиваемой системы, но и эффективность работы по снижению рисков утечки данных, неправомерного доступа к все более расширяющемуся частному цифровому миру.

Выводы

Таким образом, законодательная новелла в области ЦФА вводит существенные ограничения, но в то же время открывает определенные возможности для развития бизнеса в операциях с цифровыми финансовыми активами. Анализ показал, что терминология, используемая в Законе о цифровых финансовых активах, не всегда соответствует концепциям и стандартам, установленным в международной юридической и деловой практике, а также современным реалиям.

Переход от традиционной системы оказания финансовых услуг к цифровой предоставляет массу возможностей как крупным финансовым игрокам, так и перспективным стартапам для работы с финансовыми организациями и активами. Однако обратной стороной медали является то, что на мировой финансовый рынок выходят крупные технологические компании, которые получают все больше инструментов для расширения своего влияния на глобальном рынке. Все это порождает целый ряд рисков и барьеров, среди которых на первый план выдвигаются риски монополизации секторов экономики. В то же время цифровая трансформация становится частью объективной реальности, и снижение ее темпов в ближайшее время, вероятнее всего, наблюдаться не будет, в том числе и на территории Российской Федерации.

Более того, существующие геополитические реалии создают серьезные основания для роста внимания отечественного законодателя к рассматриваемым технологиям, позволяют оценивать их в качестве средства стратегического маневрирования,

снижения санкционного давления на экономику и разблокировки отдельных финансовых процессов, реализации бесперебойной оплаты товаров и услуг, поставляемых заграничными партнерами, и выполнения принятых долговых обязательств.

Это находит отражение в принимаемых в настоящее время решениях. Так, Председатель Правительства М. В. Мишустин 13 сентября 2022 г. дал Министерству финансов Российской Федерации, Центральному банку Российской Федерации и другим ведомствам отдельные поручения по итогам состоявшейся 30 августа стратегической сессии, посвященной финансовому развитию страны. В их числе большой блок указаний относительно развития цифровых валют и цифровых финансовых активов. До 1 декабря 2022 г. Минфину при участии Центробанка необходимо представить согласованные предложения по развитию в стране рынка цифровых финансовых активов, включая использование децентрализованных технологий, и с учетом данных предложений реализовать комплекс мероприятий по совершенствованию отечественного законодательства в 2023 г.

На основании изложенного можно сделать вывод о том, что вопросы правового регулирования цифровых финансовых активов в ближайшее время подвергнутся существенной переработке и расширению. Однако представляется, что данные изменения, чтобы они были действительно эффективными и отражали современные тенденции, должны быть реализованы во взаимодействии с соответствующими специалистами и представителями научного сообщества, занимающимися анализом проблематики юридического статуса технологии блокчейн и созданных на ее базе цифровых инструментов.

Список литературы

- Василевская, Л. Ю. (2019). Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права. *Актуальные проблемы российского права*, 5(102), 111–119. <https://doi.org/10.17803/1994-1471.2019.102.5.111-119>
- Григорьев, В. В. (2020). Регулирование налогообложения токенов на основе австралийского опыта. *Экономика. Налоги. Право*, 2, 146–154. <https://doi.org/10.26794/1999-849X2020-13-2-146-154>
- Кудряшова, Е. В. (2018). Правовое регулирование криптовалют: выбор вектора развития. *Финансовое право*, 6, 7–11. <https://elibrary.ru/xrbskl>
- Рождественская, Т. Э., Гузнов, А. Г. (2020). Цифровые финансовые активы: проблемы и перспективы правового регулирования. *Актуальные проблемы российского права*, 15(6), 43–54. <https://doi.org/10.17803/1994-1471.2020.115.6.043-054>
- Рыжов, Н. А. (2018). Анализ перспектив правового регулирования криптовалют в рамках обеспечения национальной и международной безопасности. *Юрист*, 5, 63–67. <https://doi.org/10.18572/1812-3929-2018-5-63-67>
- Alekseenko, A. P. (2020). Russian approach to ICO regulation. *Revista Gênero e Direito*, 9(4), 874–881.
- Basilio, T. A. (2019). Investment (security) tokens: a captação de fundos através de initial coin offerings e-token sales. *Revista de direito financeiro e dos mercados de capitais*, 1(2), 127–168.
- Belykh, V. S., & Bolobonova, M. O. (2019). Legal regulation of digital financial assets in Russia: controversial issues of theory and practice. *Russian Law: Theory and Practice*, 2, 38–47.
- Emtseva, S. S., & Morozov, N. V. (2018). Comparative analysis of legal regulation of ICO in selected countries. *KnE Social Sciences*, 3(2), 77–84. <https://doi.org/10.18502/kss.v3i2.1527>
- Garcia-Teruel, R. M. (2019). A legal approach to real estate crowdfunding platforms. *Computer Law & Security Review*, 35(3), 281–294. <https://doi.org/10.1016/j.clsr.2019.02.003>
- Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law*, 12(2), 129–145. <https://doi.org/10.1108/jppel-07-2019-0039>
- Garcia-Teruel, R. M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, 41. <https://doi.org/10.1016/j.clsr.2021.105543>

- Gorian, E. (2020). Singapore's cybersecurity act 2018: A new generation standard for critical information infrastructure protection. *Smart Innovation, Systems and Technologies*, 138, 1–9. https://doi.org/10.1007/978-3-030-15577-3_1
- Ishmaev, G. (2017). Blockchain Technology as an Institution of Property. *Metaphilosophy*, 48(5), 666–686. <https://doi.org/10.1111/meta.12277>
- Konashevych, O. (2020). General concept of real estate tokenization on blockchain the right to choose. *European Property Law Journal*, 9(1), 1–45. <https://doi.org/10.1515/eplj-2020-0003>
- Raskin, J. (2017). The law and legality of smart contracts. *Georget Law Technol. Rev.*, 305, 1–37.
- Sarnakov, I. (2019). Digital financial assets: segments and prospects of legal regulation in the BRICs countries. *BRICS Law Journal*, 4, 95–113. <https://doi.org/10.21684/2412-2343-2019-6-4-95-113>
- Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, 26(2), 116–134. <https://doi.org/10.1080/13600834.2017.1301036>
- Savelyev, A. (2018). Some risks of tokenization and blockchainization of private law. *Computer Law and Security Review*, 34(4), 863–869. <https://doi.org/10.1016/j.clsr.2018.05.010>
- Troyanskaya, M., Tyurina, Y., & Ermakova, E. (2020). Taxation of digital financial assets: international practices and comparative legal analysis. *Talent Development & Excellence*, 12(2), 1413–1421. https://doi.org/10.1007/978-3-030-15160-7_125
- Verheye, B. (2017). Real estate publicity in a blockchain world: a critical assessment. *European Property Law Journal*, 6(3), 441–477. <https://doi.org/10.1515/eplj-2017-0020>
- Yapicioglu, B., & Leshinsky, R. (2020). Blockchain as a tool for land rights: ownership of land in Cyprus. *Journal of Property, Planning and Environmental Law*, 12(2), 171–182. <https://doi.org/10.1108/JPPPEL-02-2020-0010>

Сведения об авторе



Перетолчин Артем Павлович – кандидат юридических наук, старший преподаватель кафедры гражданско-правовых дисциплин, Восточно-Сибирский институт Министерства внутренних дел Российской Федерации

Адрес: 664074, Российская Федерация, г. Иркутск, ул. Лермонтова, 110

E-mail: peretat@gmail.com

ORCID ID: <https://orcid.org/0000-0003-1319-8119>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=735650

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.19.43 / Правовой режим информационных ресурсов

Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 1 февраля 2023 г.

Дата одобрения после рецензирования – 23 апреля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.33>

Genesis and Prospects of Development of Legal Regulation of Digital Financial Assets in the Russian Federation

Artem P. Peretolchin

East Siberia Institute of the Ministry of Internal Affairs of the Russian Federation
Irkutsk, Russian Federation

Keywords

Blockchain,
cryptocurrency,
digital financial assets,
digital rights,
digital technologies,
distributed ledger,
law,
legal regulation,
legislation,
token

Abstract

Objective: to research the existing problems and promising directions of the legal regulation of digital financial assets as a relatively new tool of the modern digital economy.

Methods: the methodological basis of the work is the set of scientific cognition methods such as theoretical analysis, research, comparison, synthesis, and summarization of scientific literature.

Results: the work analyzes the existing approaches to legal regulation of digital financial assets in the Russian Federation and some foreign countries, reveals the existing gaps in the Russian legislation in the field of circulation of digital financial assets, gives estimation to the prospects of development of the legal regulation of these tools and forms proposals for its improving. Also, during the research, the approaches to legal regulation of digital currencies and digital financial assets, adopted in certain foreign countries, were analyzed, the trends were considered, and the positive and negative aspects of using cryptographic algorithms for the goals in economic and juridical spheres of the global economy were reflected.

Scientific novelty: within the work, the topical issues of legislative regulation of such a relatively new notion as digital financial assets are considered. The positions of Russian and foreign jurist are considered concerning

© Peretolchin A. P., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

the existing problems and risks associated with “tokenization” and “blockchainization” of private law. Besides, the author comes to a conclusion about the existence of significant gaps in the current approach to legal regulation of digital financial assets, indicates them and proposes certain mechanisms to solve these problems.

Practical significance: is due to the imperfect current legislation in the sphere of relations occurring when using the technologies based on distributed ledger, including digital financial assets. Research of these problems allows evaluating the risks, considering the existing ways of overcoming and solving the emerging disputable questions. Also, the conclusions obtained can be used to improve the Russian legislation, as well as in the academic literature devoted to the topical issues of developing the digital legislation.

For citation

Peretolchin, A. P. (2023). Genesis and Prospects of Development of Legal Regulation of Digital Financial Assets in the Russian Federation. *Journal of Digital Technologies and Law*, 1(3), 752–774. <https://doi.org/10.21202/jdtl.2023.33>

References

- Alekseenko, A. P. (2020). Russian approach to ICO regulation. *Revista Gênero e Direito*, 9(4), 874–881.
- Basilio, T. A. (2019). Investment (security) tokens: a captação de fundos através de initial coin offerings e-token sales. *Revista de direito financeiro e dos mercados de capitais*, 1(2), 127–168.
- Belykh, V. S., & Bolobonova, M. O. (2019). Legal regulation of digital financial assets in Russia: controversial issues of theory and practice. *Russian Law: Theory and Practice*, 2, 38–47.
- Emtseva, S. S., & Morozov, N. V. (2018). Comparative analysis of legal regulation of ICO in selected countries. *KnE Social Sciences*, 3(2), 77–84. <https://doi.org/10.18502/kss.v3i2.1527>
- Garcia-Teruel, R. M. (2019). A legal approach to real estate crowdfunding platforms. *Computer Law & Security Review*, 35(3), 281–294. <https://doi.org/10.1016/j.clsr.2019.02.003>
- Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law*, 12(2), 129–145. <https://doi.org/10.1108/jppe-07-2019-0039>
- Garcia-Teruel, R. M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, 41. <https://doi.org/10.1016/j.clsr.2021.105543>
- Gorian, E. (2020). Singapore’s cybersecurity act 2018: A new generation standard for critical information infrastructure protection. *Smart Innovation, Systems and Technologies*, 138, 1–9. https://doi.org/10.1007/978-3-030-15577-3_1
- Grigoriev, V. V. (2020). Regulation of token taxation based on the Australian experience. *Economics, Taxes & Law*, 2, 146–154. (In Russ.). <https://doi.org/10.26794/1999-849X2020-13-2-146-154>
- Ishmaev, G. (2017). Blockchain Technology as an Institution of Property. *Metaphilosophy*, 48(5), 666–686. <https://doi.org/10.1111/meta.12277>
- Konashevych, O. (2020). General concept of real estate tokenization on blockchain the right to choose. *European Property Law Journal*, 9(1), 1–45. <https://doi.org/10.1515/eplj-2020-0003>
- Kudryashova, E. V. (2018). Legal regulation of cryptocurrencies: choosing the vector of development. *Finansovoye pravo*, 6, 7–11. (In Russ.).
- Raskin, J. (2017). The law and legality of smart contracts. *Georget Law Technol. Rev.*, 305, 1–37.
- Rozhdestvenskaya, T. E., & Guznov, A. G. (2020). Digital financial assets: problems and prospects of legal regulation. *Aktualniye problemy rossiyskogo prava*, 15(6), 43–54. (In Russ.). <https://doi.org/10.17803/1994-1471.2020.115.6.043-054>

- Ryzhov, N. A. (2018). Analysis of the Prospects of Legal Regulation of Cryptocurrencies within the Framework of Ensuring National and International Security. *Juris*, 5, 63–67. (In Russ.). <https://doi.org/10.18572/1812-3929-2018-5-63-67>
- Sarnakov, I. (2019). Digital financial assets: segments and prospects of legal regulation in the BRICs countries. *BRICS Law Journal*, 4, 95–113. <https://doi.org/10.21684/2412-2343-2019-6-4-95-113>
- Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, 26(2), 116–134. <https://doi.org/10.1080/13600834.2017.1301036>
- Savelyev, A. (2018). Some risks of tokenization and blockchainization of private law. *Computer Law and Security Review*, 34(4), 863–869. <https://doi.org/10.1016/j.clsr.2018.05.010>
- Troyanskaya, M., Tyurina, Y., & Ermakova, E. (2020). Taxation of digital financial assets: international practices and comparative legal analysis. *Talent Development & Excellence*, 12(2), 1413–1421. https://doi.org/10.1007/978-3-030-15160-7_125
- Vasilevskaya, L. Yu. (2019). Token as a new civil rights object: issues of legal classification of digital law. *Actual Problems of Russian Law*, 5(102), 111–119. (In Russ.). <https://doi.org/10.17803/1994-1471.2019.102.5.111-119>
- Verhey, B. (2017). Real estate publicity in a blockchain world: a critical assessment. *European Property Law Journal*, 6(3), 441–477. <https://doi.org/10.1515/eplj-2017-0020>
- Yapicioglu, B., & Leshinsky, R. (2020). Blockchain as a tool for land rights: ownership of land in Cyprus. *Journal of Property, Planning and Environmental Law*, 12(2), 171–182. <https://doi.org/10.1108/JPEL-02-2020-0010>

Author information



Artem P. Peretolchin – Candidate of Juridical Sciences, Senior Lecturer, Department of Civil-legal Disciplines, East Siberia Institute of the Ministry of Internal Affairs of the Russian Federation

Address: 110 Lermontov Str., 664074 Irkutsk, Russian Federation

E-mail: peretat@gmail.com

ORCID ID: <https://orcid.org/0000-0003-1319-8119>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=735650

Conflict of interest

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – February 1, 2022

Date of approval – April 23, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:346.5:004:33:006

EDN: <https://elibrary.ru/ibfbaq>

DOI: <https://doi.org/10.21202/jdtl.2023.34>

Совершенствование системы обязательных требований, предъявляемых к бизнесу в условиях цифрового преобразования экономики

Светлана Александровна Минич

Национальный центр законодательства и правовых исследований Республики Беларусь
г. Минск, Республика Беларусь

Ключевые слова

Бизнес,
дерегулирование,
законодательство,
обязательные требования,
право,
правовое регулирование,
предпринимательская
деятельность,
регуляторная гильотина,
цифровые технологии,
экономика

Аннотация

Цель: подготовка научно обоснованных предложений по совершенствованию системы обязательных требований в сфере предпринимательской и иной экономической деятельности в условиях формирования цифровой экономики, с учетом зарубежного опыта по устранению препятствий для ведения бизнеса и имеющейся практики оптимизации законодательства в данной сфере.

Методы: методологическую основу исследования составляют традиционные общенаучные и частнонаучные методы научного познания: диалектический, формально-логический, историко-сравнительный, системный, терминологический, общелогические методы (анализ, синтез, обобщение, индукция, дедукция и др.), а также специальные методы: историко-правовой, формально-юридический, метод сравнительного правоведения.

Результаты: исследованы и систематизированы теоретические подходы и опыт совершенствования системы обязательных требований в зарубежных странах и Российской Федерации, рассмотрены возможности внедрения наиболее успешных инновационных правовых инструментов и практик для улучшения регулирования экономических отношений. Определена роль ретроспективной оценки регулирующего воздействия действующих нормативных правовых актов, содержащих обязательные требования, в решении вопросов по сокращению

© Минич С. А., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

обременительных правил и обеспечению правовой устойчивости в условиях цифровой трансформации экономики. Рассмотрен международный опыт реализации механизма регуляторной гильотины; раскрыты его суть, цель, задачи, основные принципы, алгоритм работы. Проанализированы вопросы установления и оценки применения содержащихся в нормативных правовых актах требований, предъявляемых к бизнесу.

Научная новизна: авторский всесторонний анализ имеющихся научных разработок по вопросам совершенствования системы обязательных требований, предъявляемых к бизнесу; систематизация научно-теоретических подходов к выбору инновационных правовых инструментов для устранения избыточного правового регулирования экономических отношений; обобщение успешных зарубежных практик реализации мероприятий «регуляторной гильотины».

Практическая значимость: выработка рекомендаций по эффективно-му сокращению обременительных требований, негативно влияющих на развитие предпринимательской деятельности в условиях цифровой трансформации экономики. Определение условий, необходимых для осуществления полноценной процедуры оценки регулирующего воздействия и успешной реализации регуляторных реформ. Результаты исследования могут быть использованы в нормотворческой деятельности, в образовательном процессе при освоении образовательных программ по экономическим и юридическим специальностям.

Для цитирования

Минич, С. А. (2023). Совершенствование системы обязательных требований, предъявляемых к бизнесу в условиях цифрового преобразования экономики. *Journal of Digital Technologies and Law*, 1(3), 775–802. <https://doi.org/10.21202/jdtl.2023.34>

Содержание

Введение

1. Направления совершенствования системы обязательных требований в условиях цифровой трансформации экономики
 - 1.1. Проблемы правового регулирования экономических отношений, обусловленные процессами цифровизации
 - 1.2. Внедрение новейших регуляторных технологий с целью совершенствования законодательства и устранения препятствий для бизнеса
2. Международный опыт реализации механизма регуляторной гильотины
 - 2.1. Практика применения инструментов правового дерегулирования и их отдельных элементов в зарубежных странах
 - 2.2. Примеры эффективных широкомасштабных регуляторных реформ с использованием современного механизма регуляторной гильотины
 - 2.3. Становление нового правового института обязательного требования в Российской Федерации

Выводы

Список литературы

Введение

В условиях перехода к новой технологической и инновационной реальности, глобальных цифровых трансформаций процесс поддержания действующего нормативно-правового массива в актуальном состоянии – достаточно сложная задача. Многие нормы и правила устаревают, приобретают формальный и избыточный характер. Привычные законодательные механизмы не всегда могут оперативно справиться с возрастающим объемом обременительных требований к бизнесу в той или другой области, блокирующих развитие предпринимательской деятельности, что служит основанием для поиска действенных инструментов дерегулирования в целях упорядочения и оптимизации законодательства.

Создание эффективной системы обязательных требований на сегодняшний день является серьезной проблемой многих стран, пути решения которой зачастую приводят как к внедрению комплексной полноценной оценки регулирующего воздействия законодательных актов, содержащих обязательные требования (включая ретроспективную оценку), так и к использованию отдельных новейших регуляторных технологий, среди которых наибольшую популярность набирает регуляторная гильотина.

Передовой опыт ряда стран по совершенствованию системы обязательных требований позволил рассмотреть возможности внедрения наиболее успешных инновационных правовых инструментов и практик для улучшения системы регулирования законодательства в экономической сфере. Анализ проведенных реформ также продемонстрировал, что не везде в мире применяют «регуляторную гильотину» в чистом виде, ряд стран разрабатывает свои собственные механизмы дерегулирования (законодательство с самоистекающим сроком регуляторного действия, принцип регулярности пересмотра законодательства и др.). Но суть их та же – сокращение избыточного регулирования при ведении бизнеса в целях обеспечения устойчивого экономического роста и социального благополучия страны путем искусственного сдерживания либо прекращения действия правовых предписаний в противовес их произвольному исключению (Rowthorn et al., 2017). Кроме того, необходимо иметь в виду, что любая программа реформы – это многогранная стратегия, которая должна быть адаптирована к приоритетам, институтам и общественным ожиданиям конкретной страны.

1. Направления совершенствования системы обязательных требований в условиях цифровой трансформации экономики

1.1. Проблемы правового регулирования экономических отношений, обусловленные процессами цифровизации

Экономическая сфера всегда выступала и выступает одной из наиболее важных в жизни общества. Внедрение прогрессивных цифровых технологий трансформирует традиционную экономику, открывая новые рыночные ниши, повышая качество, доступность и скорость оказания услуг, изменяя рыночную конъюнктуру, способы ведения бизнеса и получения прибыли, подстраивая производство под индивидуальные вкусы потребителей. Формирование цифровой экономики, соответствующей требованиям современной реальности, достигается за счет активного диалога закона, бизнеса, общества и власти, концентрации усилий государства на разработке эффективного

регулирования с использованием новейших регуляторных технологий (RegTech), направленных в том числе на устранение бюрократической нагрузки, максимальное сокращение излишних, обременительных правил и процедур, создающих определенные препятствия для развития предпринимательской деятельности (Chao et al., 2022).

В условиях меняющейся парадигмы регулирования многие страны осуществляют поиск и внедрение наиболее успешных инновационных правовых инструментов и практик для улучшения национальной системы регулирования, стремясь сделать ее более гибкой, согласованной, быстро реагирующей на рыночные и технологические изменения и пользующейся большим доверием со стороны бизнеса. Несмотря на уже предпринятые шаги ряда государств в направлении актуализации, упорядочения законодательного массива и гармоничного развития общественных отношений в экономической сфере, вопросы создания благоприятной регуляторной среды стоят на повестке дня и сегодня.

Говоря о совершенствовании правового регулирования в рассматриваемой сфере, необходимо раскрыть содержание данного понятия, чтобы четко обозначить его проблемное поле и с помощью принятия инновационных регуляторных решений беспрепятственно адаптировать к новой технологической реальности. Анализ устоявшихся в правовой науке и имеющихся в законодательстве определений показал, что в рамках общей теории права правовое регулирование – это воздействие права на различные группы общественных отношений¹. С. С. Алексеев под правовым регулированием понимает осуществляемое с помощью системы правовых средств результативное, нормативно-организационное воздействие на общественные отношения (Алексеев, 1966).

Объектом непосредственной юридической регламентации могут также выступать отдельные наиболее значимые общественные отношения. В частности, под правовым регулированием экономических отношений, связанных с предпринимательской деятельностью, понимается комплекс мер, принимаемых и применяемых со стороны государства в отношении адресатов регулирования, включающий в себя в первую очередь установление обязательных требований к субъектам хозяйствования, а также разрешительные, уведомительные и контрольные (надзорные) процедуры и меры воздействия на лиц, нарушивших обязательные требования². Исходя из содержания понятия правового регулирования в исследуемой сфере, можно определить последовательность его элементов: установление обязательных требований (правил, стандартов); осуществление контроля за их соблюдением; применение мер ответственности при их нарушении. Вся совокупность обязательных требований выступает фундаментом регулирования экономических отношений, нарушение которых может привести к ответственности подконтрольного субъекта или к иным неблагоприятным для бизнеса последствиям, а также повлиять на безопасность в регулируемой сфере общественных отношений.

¹ Кудрявцев, Ю. А. (2020). Правовое дерегулирование предпринимательской деятельности (оценка и риски применения «регуляторной гильотины» в условиях современной России). В сб. *Новеллы права, экономики и управления 2019 : сб. науч. трудов по материалам V Междунар. науч.-практ. конф., Гатчина, 22 нояб. 2020 г.* (с. 97–102). Гатчина: Гос. ин-т экономики, финансов, права и технологий.

² Об утверждении Правил регулирования торговли услугами, учреждения и деятельности: Решение Высшего Евразийского экономического совета № 24 [принято в г. Санкт-Петербурге 26.12.2016]. (2022). *ЭТАЛОН*. Законодательство Республики Беларусь. Минск.

Отмеченное позволяет заключить, что качественное и рациональное построение системы обязательных требований, понятных как для бизнеса, так и для контрольно-надзорных органов, выступает фундаментом эффективного правового регулирования экономической деятельности в условиях цифровой реальности. Результативное, без несения несоразмерных затрат, исполнение установленных обязательных требований их адресатами способствует формированию благоприятных и стимулирующих условий для развития всех секторов экономики, положительно влияет на общий бизнес-климат. Следовательно, данные требования должны быть актуальными, выполнимыми, ясными, разумными, соответствовать уровню развития цифровых технологий, отвечать запросам и принципам рыночной экономики (Polemīs & Stengos, 2020).

Однако, несмотря на все усилия со стороны большинства государств по обеспечению правовой стабильности в регуляторном пространстве, переход к цифровой экономике, активное внедрение инновационных технологий выступило серьезным фактором появления определенных сложностей в регулировании бизнеса (Purnomo et al., 2022). По мнению Ю. И. Грибанова, в ходе цифровой трансформации экономики нестабильность правового регулирования в большей степени затронула именно предпринимательскую деятельность, так как максимально полное раскрытие потенциала цифровых технологий обеспечивается в первую очередь за счет их активного использования во всех аспектах бизнеса: процессах, продуктах и сервисах, подходах к принятию решений³.

В частности, снизилась оперативность реагирования законодателя на изменения, появилось значительное количество правовых норм, во многом носящих формальный и избыточный характер, не отвечающих требованиям существующей цифровой реальности, что, безусловно, приводит к чрезмерной зарегулированности экономического поведения и бюрократической волоките, тормозит экономический рост, негативно влияет на общий бизнес-климат, права и интересы хозяйствующих субъектов (Youssef et al., 2021). Кроме того, наличие достаточно большого количества сфер общественных отношений, в рамках которых группируются обязательные требования и соответствующие им виды контроля (надзора), служит причиной того, что многие требования из-за смежности своих сфер носят избыточный характер, противоречат либо полностью дублируют друг друга и зачастую «разбросаны» по различным нормативным правовым актам, что не позволяет создать их исчерпывающий перечень, в результате чего подконтрольные лица не имеют четкого понимания того, что именно у них могут проверить. Ситуация усложняется еще и тем, что традиционные подходы в регулировании в силу объективной причины уже существенно исчерпали свой резерв, а новейшие регуляторные технологии имеют недостаточное описание, методическую базу и слабо адаптированы к имеющимся институтам и реальным правоотношениям (Grassi & Lanfranchi, 2022).

³ Грибанов, Ю. И. (2019). *Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции*: автореф. дис. ... д-ра экон. наук : 08.00.05. Санкт-Петербург.

Таким образом, в сфере контрольно-надзорной деятельности сложилась ситуация, невыгодная ни одной из заинтересованных сторон (ни подконтрольным лицам, ни контролирующим органам, ни обществу), что потребовало, помимо оптимизации видов государственного контроля и унификации регулирования проведения всех форм контроля, совершенствования системы обязательных требований в рамках внедрения новых подходов к регулированию экономических отношений, включая использование новейших регуляторных технологий, с целью эффективного обновления нормативных предписаний, проведения анализа регуляторного содержания нормативных правовых актов, устанавливающих обязательные требования, всестороннего пересмотра и систематизации всех требований, максимального сокращения неэффективных и корректировки действующих требований, предъявляемых к бизнесу, и др.

1.2. Внедрение новейших регуляторных технологий с целью совершенствования законодательства и устранения препятствий для бизнеса

Устойчивой попыткой изменить природу регулирования экономических отношений явилось принятие выверенных и последовательных подходов к процессу нормотворчества благодаря использованию таких инструментов экономической политики, как консультационные механизмы, измерение и уменьшение административного бремени, открытый доступ к законодательной базе и др. Кроме того, особую роль в формировании четких ориентиров, правил и приемов установления обязательных требований, направленных на повышение качества регуляторных решений, помимо уже используемых юридических технологий и аналитических инструментов, сыграло внедрение и развитие таких институтов права, как оценка регулирующего (регуляторного) воздействия (далее – ОРВ), анализ регулятивного воздействия (далее – АРВ) и оценка фактического воздействия (далее – ОФВ). Применение данных правовых инструментов позволило вывести на новый уровень процессы проектирования нормативных правовых актов и прогнозирования правовых последствий их принятия ([Шаулова, 2017](#)). Опыт использования, к примеру, ОРВ (АРВ) для совершенствования государственного регулирования экономики характерен для большинства стран Содружества Независимых Государств, что обусловлено высокой степенью их экономической интеграции (ряд стран являются членами Евразийского экономического союза). Однако используемые традиционные регуляторные технологии и аналитические инструменты, направленные на оптимизацию и инвентаризацию действующего законодательства, зачастую медлительны, дорогостоящи и отнимают много времени. Это не позволяет идти в ногу с ускорением и своевременно решать возникающие проблемы в экономической сфере, контролировать связанные с ними риски и защищать возможности, открываемые технологическим развитием. Кроме того, сравнительный анализ практик применения обозначенных инновационных институтов проверки в сферах правотворчества и правоприменения показал следующее.

Предварительная (прогнозная, ex-ante) оценка регулирующего воздействия осуществляется абсолютно во всех странах Содружества Независимых Государств.

Оценка ex post, определяющая регуляторный потенциал действующих нормативных правовых актов, проводится только в Российской Федерации, Кыргызской Республике и Республике Узбекистан. В Республике Казахстан АРВ выполняется

лишь в отношении тех действующих регуляторных инструментов и (или) требований, которые ранее не подлежали АРВ. Однако оценка фактического воздействия законодательных актов, пришедшая на смену экспертизы, осуществляется только в Российской Федерации, в соответствии с утвержденными Правительством Российской Федерации правилами ее проведения (см. табл. 1).

Таблица 1. Оценка действующих нормативных правовых актов в странах Содружества Независимых Государств

Страна	Вид оценки	Законодательство
Российская Федерация	Оценка фактического воздействия нормативных правовых актов, регулирующих правоотношения в сфере предпринимательской и иной экономической деятельности	Постановление Правительства Российской Федерации от 30 января 2015 г. № 83 «О проведении оценки фактического воздействия нормативных правовых актов, а также о внесении изменений в некоторые акты Правительства Российской Федерации»
Республика Кыргызстан	Оценка действующих нормативных правовых актов, регулирующих предпринимательскую деятельность	Закон Республики Кыргызстан от 5 апреля 2008 г. № 55 «Об оптимизации нормативной правовой базы регулирования предпринимательской деятельности»
Республика Узбекистан	Оценка по нормативным правовым актам, воздействующим на предпринимательскую деятельность, права, свободы и законные интересы граждан, а также на окружающую среду	Закон Республики Узбекистан от 20 апреля 2021 г. № ЗРУ-682 «О нормативно-правовых актах»
Республика Казахстан	Оценка соответствия действующих регуляторных инструментов и (или) требований установленным условиям их формирования (ст. 81-1 Предпринимательского кодекса Республики Казахстан)	Кодекс Республики Казахстан от 29 октября 2015 г. № 375-V «Предпринимательский кодекс Республики Казахстан»; Приказ министра национальной экономики Республики Казахстан от 30 ноября 2015 г. № 748 «Об утверждении Правил проведения и использования анализа регуляторного воздействия регуляторных инструментов и (или) требований»

Кроме того, в большинстве стран Содружества Независимых Государств предусмотрена сопровождающая (мониторинговая, on-going) оценка регулирующего воздействия нормативных правовых актов, позволяющая оперативно получить информацию, действительно ли регулирование достигает тех целевых групп, на которые было направлено, имеют ли место побочные эффекты, насколько справедливо и эффективно данное регулирование с точки зрения таких групп, что позволяет вносить необходимые коррективы в процессе реализации акта. Институт правового мониторинга (мониторинг правоприменения) получил свое активное развитие в Российской Федерации, Республике Казахстан, Республике Армения, Республике Узбекистан и др. В Республике Беларусь также формируются правовые основы данного вида мониторинга.

Исходя из анализа использования представленных юридических технологий, приходим к выводу, что в большей части стран Содружества Независимых Государств отсутствует комплексная, всесторонняя оценка регулирующего воздействия в виде единой процедуры, и в первую очередь недостаточное внимание уделяется ретроспективной оценке уже принятых нормативных правовых актов, что не совсем

оправданно, так как на стадии оценки проектов актов законодательства невозможно в полной мере учесть изменения внутренней и внешней среды, а также спрогнозировать все последствия регулирования в процессе реализации правовых норм. Кроме того, в условиях стремительного развития цифровых технологий и желания законодателя как можно быстрее реагировать на появление новых общественных отношений в экономической сфере, зачастую возникают ошибки уже на стадии разработки проектов, связанные со слабой и излишне поспешной их подготовкой, что, безусловно, отрицательно влияет на качество правоприменения, снижая эффективность реализации законодательства, создает серьезные препятствия для ведения бизнеса (Jakupec & Kelly, 2016). К примеру, Скотт Джейкобс, говоря о проблемах, связанных с низким качеством принятия законов, отмечает, что принятые в спешке законы – одна из главных причин мирового финансового кризиса. По мнению эксперта, такие непродуманные законы являются непосредственным источником коррупции и потерь крупнейших экономик. И если нельзя предугадать, какими будут законы, то невозможно построить качественный бизнес-план⁴.

Во избежание всевозможных рисков, вызванных в том числе низким качеством принятия законов, требуется осуществление всестороннего и прозрачного пересмотра всех действующих регуляций на цикличной, постоянной основе. Это обусловлено тем, что данный процесс представляет собой замкнутый непрерывный регуляторный цикл (разработка обязательных требований – оценка их действия – корректирование по результатам оценки). Таким образом, именно переход к полному циклу ОРВ, который предусматривает последовательное прохождение всех стадий оценки и пересмотра установленных правил, включая проведение качественной ретроспективной оценки, может стать залогом качественного нормативно-правового регулирования, без которого невозможно избежать определенных сложностей в решении вопросов, связанных с осуществлением предпринимательской деятельности. К сожалению, на фоне ускоряющихся процессов цифровизации и технологического прогресса в целом, государственная машина интенсивно разрабатывает все новые и новые требования к бизнесу. С течением времени некоторые из таких требований утрачивают свою актуальность, что приводит к определенным коллизиям в праве, создает законодательные завалы, предпосылки для неоправданных расходов со стороны бизнеса, ведет к серьезной зарегулированности отдельных отраслей экономики (Haidar, 2012). Несмотря на огромный потенциал уже апробированных юридических технологий (ОРВ, ОФВ и правового мониторинга), данные инструменты, даже в своей совокупности, учитывая цифровые преобразования, не могут обеспечить эффективный пересмотр всех обязательных требований, особенно в части анализа всех устаревших регуляций. Такого рода сложности в регулировании создают предпосылки для внедрения новых инновационных правовых механизмов оценки и оптимизации действующего законодательства при сохранении и улучшении работы уже имеющихся. Подход, предусматривающий проведение единой комплексной процедуры ОРВ, позволяет эффективно препятствовать необоснованному разрастанию нормативного поля. Кроме того, широкое использование целого спектра аналитических инструментов для оптимизации законодательства в условиях постоянного

⁴ Regulatory Impact Analysis : Best Practices in OECD Countries. OECD PUBLICATIONS, 2, rue Andr e-Pascal, 75775 PARIS.

расширения цифровых возможностей в экономической сфере стало своего рода трендом, актуальной практикой реформирования законодательства во многих странах (Дегтярев, 2022а). Выбор данного вектора в работе по совершенствованию системы обязательных требований и достижения стабильности в регулировании экономических отношений объясняется стремлением многих стран к формированию интегрированной регуляторной политики, объединяющей в себе различного рода регуляторные механизмы и технологии в единое целое.

В условиях цифрового развития и глобализации быстрому решению вопросов по сокращению обременительных регуляций и обеспечению правовой устойчивости способствовало внедрение эффективных механизмов дерегулирования, одним из которых выступает регуляторная гильотина, представляющая собой гибкий и простой правовой инструмент недифференцированного сокращения нормативного массива. Регуляторная гильотина может использоваться для проведения узких и широкомасштабных реформ, имеющих разовый или системный характер (Nosova, & Norkina, 2021).

Регуляторная гильотина позволяет оперативно за короткий промежуток времени пересмотреть большое количество правил, регламентирующих экономические отношения. Ключевая идея регуляторной гильотины – указать на системный характер проблемы зарегулированности предпринимательской деятельности, а также продемонстрировать возможность устранения избыточных требований в максимально короткие сроки, легким, разумным и мягким способом исправить сложившуюся ситуацию, не допустить очередного кризиса в экономической сфере, открыть более широкие возможности для внедрения и развития новых цифровых технологий и реализации инновационных проектов.

Определений понятия «регуляторная гильотина» в юридической литературе достаточно много. В широком понимании это прозрачное и доступное средство для подсчета и быстрого пересмотра большого количества правил через призму выработанных научных критериев надлежащего регулирования, согласно которым происходят оценка и устранение тех регуляций, которые больше не нужны.

Д. Б. Цыганков под регуляторной гильотиной понимает правовое средство для быстрого пересмотра большого количества нормативных актов (Любимов и др., 2019).

И. В. Сехин характеризует регуляторную гильотину как инструмент дерегулирования общественных отношений, основанный на критериальной оценке массива правовых норм и последующем прекращении действия избыточных обязательных требований (Дидикин, 2021).

Д. В. Новак в качестве ключевого принципа действия регуляторной гильотины определяет возможность пересмотра всех обязательных требований, на предмет их эффективности в системе действующего правового регулирования (Любимов и др., 2019).

Если придерживаться позиции М. В. Дегтярева, то регуляторная гильотина – масштабируемый и операционабельный интегральный инструмент упрощающего и/или трансформирующего пакетированного «прореживания» массивов нормативных правовых актов, продолжение регуляторного существования и действия которых не имеет уже более (или не имело изначально) веских оснований и оправданий с точки зрения законности, разумной рациональности, стратегии экономического развития, социально-экономической необходимости» (Дегтярев, 2022а).

С опорой на представленные дефиниции можно заключить, что сущность регуляторной гильотины вполне понятна и проста. Рассматриваемая регуляторная технология заключается в масштабном пересмотре действующих требований, содержащихся в нормативных правовых актах, в результате которого принимается одно из трех решений: оставление в силе, внесение изменений или ликвидация.

Вместе с тем, выступая в поддержку уже выверенных и реализуемых во многих странах инструментов улучшения регулирования, Д. Б. Цыганков справедливо отмечает, что там, где нормально и полноценно работает ОРВ, гильотина особо-то и не нужна, так как избыточные акты своевременно отменяются, что не дает им бесконтрольно разрастись⁵. Однако при наличии захламленности нормативно-правового массива невозможно обойтись без комплексного и масштабного реформирования законодательства. Особенно остро эта проблема проявляет себя в наиболее зарегулированных секторах экономики. Соответственно, такой инструмент быстрых реформ, как регуляторная гильотина, – это определенный шаг в сторону обеспечения стабильности регулирования и правовой безопасности бизнеса (Дегтярев, 2022b).

Таким образом, в решении вопросов по сокращению обременительных правил и обеспечению правовой устойчивости важно использовать интегрированный подход, включающий внедрение комплексной полноценной ОРВ наряду с использованием новейших регуляторных технологий, среди которых наибольшую популярность набирают механизмы правового дерегулирования.

2. Международный опыт реализации механизма регуляторной гильотины

2.1. Практика применения инструментов правового дерегулирования и их отдельных элементов в зарубежных странах

Впервые механизм регуляторной гильотины был применен в Европе. Первые ее проявления нашли свое отражение в ранних попытках дерегуляции в 1980-х гг., в ходе которых была разработана центральная микроэкономическая стратегия для стран, сталкивающихся с экономическим кризисом и ищущих быстрых реформ.

В 1984 г. программа «Регуляторная гильотина» была инициирована в Королевстве Швеция. Правительство этой страны обнаружило, что не в состоянии составить перечень действующих нормативных правовых актов, в связи с чем приняло решение создать четкую всеобъемлющую единую законодательную базу и поручило всем подчиненным ему органам в течение года составить реестры своих актов. При подготовке списков отбирались ненужные и устаревшие регуляции, которые затем были автоматически отменены, а все новые правила и изменения в действующие нормативные правовые акты стали вноситься в единый реестр в течение суток с момента принятия. Такой подход считался большим успехом. В ходе его использования удалось быстро комплексно пересмотреть нормативную базу и отменить все, что не прошло фильтрацию, т. е. было признано устаревшим, тормозящим, нецелесообразным, избыточным, влекущим необоснованные расходы, связанные со значительными рисками. Так, например, в сфере образования было отменено 90 % всех правил.

⁵ Голодникова, А. Е., Ефремов, А. А., Соболев Д. В., и др.; рук. авт. кол-ва Цыганков Д. Б. (2018). *Регуляторная политика в России: основные тенденции и архитектура будущего*. Москва: Национальный исследовательский университет «Высшая школа экономики».

В результате удачно проведенной реформы в Королевстве Швеция принцип регуляторной гильотины позаимствовала Венгрия, и в начале 1990-х гг. страна таким образом избавилась от всех норм, не отвечающих требованиям рыночной экономики. Первый этап предусматривал работу с нормативно-правовой базой, принятой до 30 июня 1990 г., а второй – с принятой после этой даты.

Затем успешным опытом оптимизации законодательства заинтересовалась Республика Корея, столкнувшаяся в 1997 г. с азиатским финансовым кризисом. С учетом предыдущих неудачных подходов к реформе регулирования по принципу «снизу вверх» в этот раз был выбран подход «сверху вниз». Программа реформы включала две ключевые инициативы: первая – по дерегулированию, вторая – устойчивая институциональная реформа. Таким образом, корейская гильотина была внедрена в более широкую стратегию проведения реформы. В итоге за 11 месяцев 1998 г. предварительно созданный Комитет по реформе регулирования (RRC) отменил 5 430 (48,8 %) и упростил 2 411 (21,7 %) из 11 125 пересмотренных им нормативных актов, что способствовало увеличению притока прямых иностранных инвестиций (FDI), сокращению административных издержек, снижению почти вдвое нормативной нагрузки на бизнес, созданию новых рабочих мест, расширению доступа к валютным рынкам и многолетнему экономическому росту страны (Артеменко, 2020).

Особое значение в ходе реализации регуляторной реформы в Республике Корея имело принятие на начальной стадии регуляторной гильотины исторического Закона об административном регулировании (Basic Act on Administrative Regulations – BAAR), который включал порядок создания и работы RRC (ст. 23–33 BAAR), нормы по разработке Комплексного плана по совершенствованию регулирования (ст. 20 BAAR) и впервые закреплял понятие оценки регулирующего воздействия (regulations impact analysis – RIA) и его критерии (ст. 2, 7 BAAR)⁶.

Однако необходимо отметить, что элементы дерегулирования, которые поспособствовали становлению современного механизма регуляторной гильотины, использовались в отдельных странах еще до 1980 г. Это было связано с переходом к концепции государства всеобщего благосостояния (welfare state), реализованной в большинстве экономически развитых стран мира начиная с 1970 г. Так, например, в отмеченный период экономика Соединенных Штатов Америки столкнулась с избыточным регулированием в социальной сфере. Зарегулированность экономических отношений обременяла бизнес и демонстрировала неэффективность регулирования предпринимательской деятельности. Желая эффективно решить проблему устранения возникших барьеров при ведении бизнеса и снизить социальные расходы, Соединенные Штаты Америки среди прочих мер ввели дополнительные требования по защите труда к предприятиям с опасным производством (Южаков и др., 2021). Необходимость введения новых норм была обусловлена сокращением специалистов по охране труда. Однако ужесточение правил имело негативный эффект и стало одной из причин массовых увольнений работников с таких предприятий.

⁶ Basic Act on Administrative Regulations (Act No. 5368, Aug. 22, 1997).

Аналогичных примеров чрезмерного регулирования в той или иной области можно привести достаточно много. Сложившаяся ситуация требовала быстрого пересмотра и устранения избыточных, разрушительных регуляций. В результате в конце 1970-х – начале 1980-х гг. в Соединенных Штатах Америки, Соединенном Королевстве Великобритании и Северной Ирландии и ряде иных стран начали вводить элементы дерегулирования (*deregulation, less regulation*) (Contractor et al., 2020).

Следует также отметить, что внедрению регуляторной гильотины и ее отдельных элементов предшествовали программы: 1) сокращения административных барьеров (*red tape cutting, simplification*); 2) временного регулирования (законодательства с самоистекающим сроком регуляторного действия), получившего название *sunset legislation*, или *sunsetting* (*Gesetzgebung auf Zeit* – в Федеративной Республике Германия, *tijdelijke wetgeving* – в Королевстве Нидерландов) – норм «заходящего солнца» («закатное законодательство», «самозавершающиеся» нормы), который был, к примеру, применен в Австралии (Дегтярев, 2021).

Так, в Австралии, согласно Закону о законодательных актах (*Legislative Instruments Act 2003, LIA*), любые регуляции в отношении бизнеса или некоммерческих организаций через 10 лет автоматически аннулировались, если не были приняты меры по их сохранению. Для продления действия тех или иных норм предусматривалась особая процедура, связанная с оценкой их регулирующего воздействия. Обозначенный закон обеспечивал обновление нормативного массива и поддержание его в актуальном состоянии.

Примером страны, где «закатное законодательство» используется довольно часто, также выступает Государство Израиль. Например, с 2000 по 2015 г. Кнессет (законодательный орган страны) принял 281 временный закон. В Соединенных Штатах Америки использование процедуры *sunset legislation* было связано с особенностями деятельности конгрессов штатов. С позиции М. В. Дегтярева, систему таких актов можно квалифицировать как временное законодательство (Дегтярев, 2022a).

Практика применения отдельных элементов дерегулирования в Австралии, Соединенном Королевстве Великобритании и Северной Ирландии, Королевстве Нидерландов, Соединенных Штатах Америки и иных странах, а также высокие результаты, полученные в ходе использования принципа регуляторной гильотины в Королевстве Швеция и Республике Корея, легли в основу современной регуляторной гильотины. Являясь новатором в вопросах, связанных с оценкой источников регуляторных проблем начиная с 2004 г., компания *Jacobs, Cordova & Associates (JC&A)* приняла активное участие в разработке и внедрении программ регуляторных реформ в Республике Хорватия, Социалистической Республике Вьетнам, Республике Кения, Арабской Республике Египет, Республике Молдова, Боснии и Герцеговине, Республике Сербия и других государствах, что продемонстрировало эффективность механизма регуляторной гильотины в том числе и в развивающихся странах.

Проведенное исследование также позволяет выделить одну из причин столь быстрого решения ряда стран внедрить механизм регуляторной гильотины и в оптимально короткие сроки провести инвентаризацию законодательства. В большинстве случаев это было обусловлено их желанием вступить в Европейский союз, что, в свою очередь, требовало гармонизации и координации национального нормативного массива с европейским законодательством. Процесс оптимизации законодательства с использованием механизма регуляторной гильотины, по мнению Д. Б. Цыганкова, послужил своего рода «окном возможностей» для борьбы с избыточными нормами (Любимов и др., 2019).

2.2. Примеры эффективных широкомасштабных регуляторных реформ с использованием современного механизма регуляторной гильотины

Наиболее классическим примером применения регуляторной гильотины выступает опыт Республики Хорватия (подала заявку на вступление в ЕС в 2003 г.). Проект регуляторной гильотины был запущен властями страны в январе 2006 г. Весь процесс внедрения и проведения реформы занял девять месяцев. Проект был известен под названием HITROREZ («Быстрое сокращение», «ХитроРез»).

Процедура оптимизации хорватского законодательства включала сбор, анализ и упорядочение правил, касающихся ведения бизнеса. Разработанный проект предусматривал тройной пересмотр всех требований: органами публичного управления, которые их издавали; специальным подразделением HITROREZ, а также компаниями и предпринимателями⁷.

Проведение реформы предполагало прохождение двух этапов.

Первый этап предусматривал подготовку органами исполнительной власти полного перечня требований, касающихся бизнеса, и представление его в специальное подразделение HITROREZ.

На втором этапе требования подлежали рассмотрению ведомствами на основе взаимодействия с заинтересованными сторонами бизнеса и установленных критериев. В ходе анализа в отношении регуляций, содержащихся в законодательных актах, принималось одно из следующих заключений: отменить, изменить или оставить так, как есть.

Сам план действий по реализации стратегии гильотины в Республике Хорватия состоял из 17 обязательных последовательных шагов и четкого графика, где первый шаг – это принятие решения со стороны органов власти запустить гильотину.

В результате реализации проекта HITROREZ были выработаны конкретные рекомендации по каждому нормативному акту, содержащему требования к бизнесу, и представлены в Правительство Республики Хорватия. Это позволило отменить около 27 % всех правил, касающихся бизнеса, а также упростить более 30 % норм. В соответствии с данными Всемирного банка, в ходе проведенной реформы на основе регуляторной гильотины экономике страны удалось сэкономить 65,6 млн долл. ежегодно (0,13 % от ВВП).

Проект HITROREZ также послужил первым шагом для начала реализации дальнейших общесистемных реформ в стране. К примеру, в период с 2006 по 2020 г. Республика Хорватия существенно улучшила свои показатели во всемирном рейтинге стран Doing Business, поднявшись со 118-й позиции на 51-ю.

Успех гильотины в Республике Хорватия был обеспечен следующими факторами:

- системным подходом к пересмотру законодательной базы и выделения финансирования на регуляторные расходы;
- установлением четких стандартов проекта, активным участием бизнес-сообщества в реализации проекта;
- желанием вступить в Европейский союз;

⁷ Jacobs, S., & Astrakhan, I. (2005). Effective and Sustainable Regulatory Reform: The Regulatory Guillotine in Three Transition and Developing Countries. *World Bank Conference Reforming the Business Environment: From Assessing Problems to Measuring Results*. 29 Nov. – 1 Dec. 2005, Cairo.

– внедрением нового программного обеспечения для повышения эффективности и прозрачности регулирования (Александров, 2019).

Кроме того, важным элементом результативного применения регуляторной гильотины в Республике Хорватия явилось официальное утверждение соответствующих структур и институтов. В частности, постановлением Правительства Республики Хорватия от 28 июня 2007 г. «О создании Управления по координации системы оценки регулирующего воздействия» было создано Управление по координации системы оценки регулирующего воздействия. В его состав вошел отдел анализа и контроля за реализацией проекта HITROREZ.

Вслед за Республикой Хорватия по этому же принципу упрощения регулирования в 2005–2007 гг. была осуществлена оптимизация нормативной правовой базы для предпринимателей в Республике Молдова. Примечательно, что запуску радикальной реформы в Молдове предшествовало принятие в 2004 г. Закона об оптимизации нормативной базы регулирования предпринимательской деятельности (Закона о гильотине), что предполагало переход к более смелым и систематическим реформам (Молдова до 2005 г. уже имела опыт проведения общегосударственных регуляторных реформ). Отмеченный закон устанавливал новые стандарты качества регулирования и содержал перечень принципов по созданию актуальных, выполнимых, ясных, разумных правил, соответствующих уровню развития цифровых технологий:

- прозрачность и стабильность в регулировании бизнеса;
- никакое вмешательство в предпринимательскую деятельность и/или приостановление предпринимательской деятельности не допускается, за исключением случаев, прямо определенных в законе;
- разграничение контрольно-надзорных и регуляторных функций органов исполнительной власти;
- административные органы не должны требовать и взимать никаких дополнительных сборов за выдачу лицензий, разрешений и других сертификатов для ведения бизнеса, кроме тех, которые прямо определены в законах и постановлениях правительства или парламента, которые определяют вид услуг и плату, взимаемую за такие услуги;
- требовать и запрашивать какие-либо документы для выдачи лицензий, разрешений и других сертификатов для ведения бизнеса, которые прямо не оговорены в законах и постановлениях правительства или парламента, запрещено.

Недостатком представленных принципов выступала их сосредоточенность в основном на улучшении правового регулирования предпринимательской деятельности (правовой безопасности бизнеса) без уделения должного внимания экономической стороне вопроса. Тем не менее реформа в Республике Молдова была успешной, позволив впервые за многие годы составить всеобъемлющий прозрачный перечень правовых актов, регламентирующих вопросы ведения бизнеса. Созданная в целях реализации «регуляторной гильотины» Национальная рабочая группа за шесть месяцев пересмотрела 1 130 нормативных правовых актов, регулирующих предпринимательскую деятельность. В ходе проведенной реформы было выявлено, что лишь 426 актов соответствуют всем установленным критериям (были включены в электронный реестр), 285 актов (35 %) требовали внесения изменений и дополнений, 99 нормативных правовых актов (12 %) отменили (большинство из них были признаны незаконными). Использование механизма регуляторной гильотины в стране

также значительно укрепило центральные институты, ответственные за проведение реформ, повысило доверие к реформе и увеличило потенциал для проведения более масштабных реформ в будущем.

В целом несущая конструкция регуляторной гильотины имела универсальный характер, что позволяло использовать ее при проведении широкомасштабных реформ (пример Республики Хорватия, Республики Молдова), и секторных, направленных на упрощение регулирования в отдельных секторах экономики или сферах, например, совершенствования инвестиционных процессов, системы лицензирования и др. Среди стран, успешно реализовавших секторную реформу, можно назвать Республику Кения, Арабскую Республику Египет и др.

Так, в 2005 г. правительство Республики Кения приступило к реформе, направленной на сокращение растущего числа бизнес-лицензий и сборов и на снижение уровня коррупции, которая приобрела серьезные масштабы в связи с избыточностью таких лицензий. Реформа заняла 18 месяцев. Под руководством Министерства финансов был создан центральный комитет по реформированию регулирования и началась реализация общегосударственной программы по дерегулированию «Регуляторное поведение и усиление потенциала Республики Кения»⁸.

Всесторонняя инвентаризация, проведенная в рамках этой реформы, показала, что частный сектор сталкивался с более чем 1300 бизнес-лицензиями и соответствующими сборами, взимаемыми более чем 60 государственными учреждениями и 175 местными органами власти, а регулирующие органы постоянно вводили все новые и новые лицензии. Результатом стало то, что частный сектор был перегружен лицензиями, сборами и расходами. В ходе реформы многие лицензии были признаны ненужными, незаконными или неоправданно дорогостоящими. По состоянию на октябрь 2007 г. 315 лицензий были аннулированы и 379 упрощены. В общей сложности было сохранено 294. Из оставшихся примерно 300 были отложены из-за разрабатываемых новых законопроектов или уже принятых законодательных актов, а 25 переклассифицированы и не учитывались как лицензии⁹.

Примечательно, что правительство Республики Кения в ходе проведения реформы вышло за рамки предыдущих проектов, основанных на реформировании лицензий «по одной за один раз» (one in – one out), и адаптировало более широкий «гильотиновый подход», предусматривающий быстрое выявление, пересмотр и упорядочение всех лицензий при ведении бизнеса и связанных с ними сборов. Результаты реформы лицензирования внесли существенный вклад в повышение статуса Республики Кения как ведущего реформатора в рейтинге Всемирного банка Doing Business за 2008 г. По итогам «Мониторинга и оценки реформы бизнес-лицензирования правительства Республики Кения» в рамках программы «Регуляторное поведение и усиление потенциала Республики Кения» были отменены и упрощены отдельные виды лицензирования, что существенно уменьшило расходы на контрольно-надзорную деятельность, снизило риски для предпринимателей и инвесторов. Сокращение расходов бизнеса экспертами было оценено в 146 млн долл. в год.

⁸ Jacobs, S., Ladegaard, P., & Musau, B. (2007, October). *Kenya's Radical Licensing Reform*.

⁹ Jacobs S. (2005, December). *The Regulatory Guillotine Strategy. Preparing the Business Environment in Croatia for Competitiveness in Europe*.

Важным и принципиально новым результатом проведенной в Республике Кения реформы лицензирования выступило решение по созданию надлежащей институциональной основы для поддержки устойчивости реформ. В частности, правительством страны были одобрены институциональные инициативы: по формированию постоянно действующего регулирующего органа при Министерстве финансов, в задачи которого входила проверка новых правил ведения бизнеса, а также разработка и внедрение более масштабных программ реформ регулирования в будущем; создание электронного реестра нормативных правовых актов и реестра регулирующих органов.

Обзор реализации реформы лицензирования Республики Кения позволил выделить ее основные принципы:

- внедрение упорядоченного и прозрачного процесса подсчета лицензий во всех государственных органах, обладающих полномочиями выдачи лицензий;
- быстрый пересмотр и проверка лицензий на соответствие установленным критериям: законность, обоснованность, необходимость, удобство для бизнеса;
- бремя доказывания для сохранения тех или иных лицензий не лежит на реформаторах;
- полная прозрачность и широкое участие заинтересованных сторон в процессе реформирования;
- создание институциональной основы для проведения регуляторных реформ на системной основе.

Регуляторная реформа в Арабской Республике Египет также имела секторный характер и была направлена на упрощение инвестиционных процессов (2014 г.). Результатом реформы стало создание специальной структуры «Египетская регуляторная реформа и деятельность по развитию» (ERRADA). В рамках ее компетенции были осуществлены ревизия и совершенствование законодательства в сфере инвестиций, сведены к минимуму обременительные административные процедуры. В 2015 г. в целях укрепления доверия инвесторов, ослабления бюрократии и привлечения иностранных инвестиций был принят Закон Арабской Республики Египет АРЕ № 17/2015, который внес изменения в Закон Арабской Республики Египет АРЕ № 8/1997 «Об инвестициях». Данный закон предусматривал стандартизацию инвестиционных инициатив, упрощение для инвесторов прохождения всевозможных бюрократических процедур и другие мероприятия, что позволило сократить большое количество неэффективных и нецелесообразных правил в данной сфере.

Проект с использованием регуляторной гильотины был реализован и в Социалистической Республике Вьетнам. В 2007 г. был утвержден План по упрощению административных процедур в области государственного управления на период 2007–2010 гг.» (далее – План), который состоял из четырех основных этапов:

- инвентаризации, включающей в себя подготовку государственными органами исполнительной власти перечней административных процедур и информации о них на основе стандартизированных форм с последующим созданием реестров;
- самопроверки, в рамках которой органы исполнительной власти анализировали и оценивали процедуры на основе критериев законности, необходимости, приемлемости и разумности;
- сбора специальной рабочей группой указанной информации и обсуждения с представителями органов публичной власти с последующей разработкой концепции административных реформ;

– разработки рекомендаций в отношении каждой проверенной административной процедуры (Дегтярев, 2022а).

Экономическая выгода от проведенной регуляторной реформы в Социалистической Республике Вьетнам была существенной. Сокращение затрат бизнеса, связанных с регулированием, было оценено в 1,4 млрд долл. в год. Пересмотру подлежала 5 421 процедура на всех уровнях, из которых 8,8 % было отменено, 77 % – упрощено.

Современная регуляторная гильотина в свою очередь охватила большое количество развитых стран мира. Внедрение «регуляторных гильотин» в этих странах было обусловлено не только процессами цифровизации и разрастанием законодательного массива, но и целым рядом иных причин:

1. Выход из международных соглашений и союзов (например, Соединенное Королевство Великобритании и Северной Ирландии – отмена норм регулирования в связи с принятием Закона о выходе страны из Европейского союза, 2018 г.).

2. Упрощение регулирования трудовых отношений в целях повышения производительности труда (Французская Республика, 2017 г.).

3. Внедрение эффективных правовых институтов регулирования и практик (Австралия, Новая Зеландия, 2017 г.).

4. Создание упрощенных условий для ведения определенного бизнеса там, где это ранее делать было невозможно в целях экономического развития регионов, привлечения в них прямых инвестиций (Государство Япония, 2003 г.).

5. Участие в работе международных организаций (например, Организации экономического сотрудничества и развития – ОЭСР, включающей 38 государств и играющей ведущую роль в международном сообществе по продвижению реформы регулирования и внедрению разумной практики регулирования на основе общего государственного подхода).

Особого внимания в проведении регуляторной реформы среди развитых стран заслуживает опыт Японии, так как является уникальным примером территориального подхода к реформе регулирования. Благодаря программе специальных зон, основанной на законодательстве, утвержденном в 2002 г. (Закон «О специальных зонах, связанных со структурными реформами»), некоторые правила могли быть смягчены или отменены в географически ограниченных районах, выступающих в качестве испытательного полигона и первого шага для проведения реформ на национальном уровне. В стране территориальный подход, сочетающий реформу регулирования с элементами децентрализации, привел к инициативам, которые в противном случае могли бы занять намного больше времени¹⁰.

Многогранный международный опыт показал, что большинство реализованных регуляторных реформ имеют широкомасштабный характер и не ограничиваются только использованием механизма регуляторной гильотины, что абсолютно обоснованно. Процессы цифровизации создают основу для развития новейших регуляторных технологий, делая их более гибкими, высокоэффективными и низкзатратными (Beach et al., 2020). Если изначально целью регуляторной политики многих стран являлось стремление уменьшить количество нормативных правовых актов (дерегулирование), мешающих развитию бизнеса (политика по «уменьшению регулирования» – less regulation), то со временем регуляторные реформы приобрели комплексный,

¹⁰ OECD Reviews of regulatory reform: Japan. (1999).

сбалансированный и системный характер. Их основная цель заключалась не в сокращении количества регуляций, а в повышении их качества и результативности (концепция «качественного регулирования» – *better regulation*). В дальнейшем, с появлением новых инструментов регулирования (оценка регулирующего воздействия; измерение и уменьшение административного бремени; упрощение существующего законодательства, включая консолидацию, кодификацию; консультации с заинтересованными сторонами; оценка фактического воздействия; открытый доступ к законодательной базе и др.), произошла своего рода модернизация регулирования, что привело к смене концепции «качественного регулирования» на более современную концепцию «умного регулирования» (*smart regulation*). Однако, несмотря на эволюцию концепций регулирования, механизм регуляторной гильотины даже с учетом цифровых преобразований экономики остается актуальным и выступает одним из ключевых элементов при проведении как секторных, так и более масштабных реформ (Давыдова, 2020).

Регуляторная гильотина – это лишь один пример реформ, которые могут одновременно дать как краткосрочные результаты, так и заложить основу для устойчивых изменений в сфере регулирования предпринимательской деятельности. Регуляторная гильотина предполагает своего рода цикличность проведения инвентаризации законодательства и практически никогда не является завершением реформ. Зарубежный опыт показал, что регуляторные реформы, которые проводятся снизу вверх, а также бессистемные, разовые реформы не приводят к ожидаемому успеху, поскольку достижения улучшения регулирования вновь могут пойти на спад в результате принятия большого количества новых и утраты актуальности уже действующих требований. Такие случаи имеют место особенно тогда, когда в стране на протяжении многих лет формировались и укоренились достаточно сильные привычки правового регулирования, что стимулирует повторение тех же самых ошибок. Для успешной реализации стратегии гильотины необходим целый ряд условий, и в первую очередь важна политическая, административная и правовая поддержка реформы. Кроме того, любая реформа опирается на руководящие принципы, содержащие необходимые характеристики надлежащего регулирования. Принципами «регуляторной гильотины» являются: всеобщность пересмотра законодательной базы; быстрота и окончательность принятия решения о сохранении, упрощении или отмене правовых норм; отмена в пользу реформы бремени доказывания необходимости сохранения правовых норм (презумпция зарегулированности общественных отношений в сфере предпринимательской деятельности); универсальность критериев оценки правовых актов.

Анализ реформ также продемонстрировал, что не везде в мире применяют «регуляторную гильотину» в чистом виде, ряд стран разрабатывают свои собственные механизмы дерегулирования. Но суть их та же – сокращение избыточного регулирования при ведении бизнеса в целях обеспечения устойчивого экономического роста и социального благополучия страны.

2.3. Становление нового правового института обязательного требования в Российской Федерации

Экономическая политика большинства стран, в том числе и Российской Федерации, направлена на то, чтобы законодательство и регулирование были друзьями, а не врагами технологического прогресса. Однако регулирование порой приобретает избыточный характер, налагая слишком много нормативных требований, которые их адресаты должны соблюдать.

В России анализ существующих проблем в регулировании экономических отношений позволил определить значимые ориентиры и приоритетные направления совершенствования правового регулирования бизнеса. Серьезное внимание было уделено вопросам создания четких ориентиров, общих правил и приемов установления обязательных требований, построению эффективной системы требований, предъявляемых к бизнесу, с использованием перспективных регуляторных технологий, включающих в себя и инструмент правового дерегулирования – регуляторную гильотину.

Правительством Российской Федерации не раз отмечалось, что постоянство в законодательстве становится проблематичным. Избыточность требований, предъявляемых к бизнесу, препятствует принятию более эффективных решений, приводит к необходимости пересмотра нормативного массива. Кроме того, законодательство, которое с течением времени устаревает, ставит на карту доверие граждан и общества к способности установленных правил решать вопросы, ради которых они были приняты. Данная проблема стала наиболее очевидной в ходе высоких достижений технологического прогресса, охвативших в том числе и экономическую сферу. Огромное количество обязательных требований уже не соответствовало современным потребностям субъектов экономической деятельности, уровню технологического прогресса, изменениям, обусловленным процессами цифровизации.

Концепция эффективного регулирования заключается в постоянном и систематическом совершенствовании его качества. Необходимость перестройки нормативной правовой базы для целей успешного ведения бизнеса была отмечена еще в 2014 г. в ряде программных и стратегических документов Российской Федерации. Предпосылками для принятия кардинальных решений по устранению избыточного регулирования выступили:

- принятие большого количества законодательных актов, не предусмотренных заранее сформированным планом, а связанных с реакцией государства на различные события;
- автономность имеющихся процедур оценки законодательства, слабая взаимосвязь применяемых инструментов правовой диагностики;
- зарегулированность целого ряда сфер экономики;
- механическая отмена обязательных требований без проведения должного комплексного анализа, основанного на четких критериях;
- отсутствие доступной, исчерпывающей базы (реестра) обязательных требований по всем сферам регулирования предпринимательской и иной экономической деятельности;
- отсутствие плановости и цикличности в переоценке и пересмотре обязательных требований, предъявляемых к бизнесу и др.

Запуску регуляторной гильотины способствовало принятие Федерального закона «Об обязательных требованиях в Российской Федерации» (далее – Закон № 247-ФЗ)¹¹. Данный закон заложил фундамент для формирования нового правового института обязательного требования.

¹¹ Об обязательных требованиях в Российской Федерации. № 247-ФЗ от 31.07.2020. (2020). КонсультантПлюс.

Закон № 247-ФЗ позволил определить единые условия установления всех правил, предъявляемых к бизнесу, а именно: обозначил сферу применения его норм, определил объект, субъекты и предмет регулирования, источники, в которых должны содержаться данные нормы, и срок их действия, формы оценки применения обязательных требований. Необходимыми условиями установления обязательных требований были названы: анализ социально значимых рисков в соответствующей сфере общественных отношений; учет соответствия обязательных требований современной цифровой реальности.

Кроме того, Закон № 247-ФЗ закрепил основополагающие принципы – общие критерии, своего рода ограничения (требования к требованиям), на которых должна базироваться и строго им соответствовать вся система обязательных требований. Всего было выделено пять принципов: законность, правовая определенность и системность, обоснованность, открытость и предсказуемость, исполнимость обязательных требований.

Приведение в действие механизма регуляторной гильотины позволило быстро и эффективно осуществить пересмотр значительного объема действующих нормативных правовых актов, содержащих обязательные требования, с целью их актуализации и отмены всех устаревших и избыточных правил. Это способствовало существенному сокращению финансовых затрат для бизнеса как по всем направлениям предпринимательской деятельности, так и на уровне отдельных секторов экономики или сфер. Регуляторная гильотина выступила ценным инструментом для устранения неопределенности и рисков; рационализации процесса законотворчества; повышения качества законодательства и эффективности регулирования в условиях развития инноваций и новых цифровых возможностей.

Однако следует обратить внимание на ряд проблемных аспектов, обнаруженных в ходе внедрения нового правового регулятора.

Во-первых, регуляторная гильотина не является панацеей, способной устранить многочисленные сложности в регулировании, связанные с разрастанием нормативного поля и увеличением разрыва между правом и реальностью.

Во-вторых, чрезмерное использование механизма регуляторной гильотины зачастую не позволяет качественно провести содержательную оценку нормативных предписаний и может привести к бездумному массовому сокращению обязательных требований, создавая ситуацию правового вакуума. В связи с чем следует исходить из того, что регуляторная гильотина выступает всего лишь одним из действенных механизмов правового дерегулирования, широкий потенциал которого необходимо использовать в совокупности с иными регуляторными технологиями.

Несмотря на обозначенные риски, Закон № 247-ФЗ выступил структурообразующим в построении нового для РФ правового института обязательного требования, продемонстрировав единство, комплексность норм, регулирующих экономические отношения, позволил сформировать целостную систему правового регулирования, основанную на риск-ориентированном подходе, представляющую собой типовую матрицу для каждой сферы предпринимательской деятельности. Внедрение регуляторной гильотины значительно снизило регуляторную нагрузку на бизнес, сократило количество контрольных функций государственных органов.

Подводя итог вышесказанному, следует отметить, что в эпоху цифровых преобразований экономики и иных сфер жизнедеятельности стремление бороться с зарегулированностью, обусловленной устаревшим и излишним законодательством,

которое больше не соответствует темпам развития современного общества, путем недифференцированного сокращения нормативного массива все возрастает. Регулирование любого социального и технологического явления подразумевает понимание его характеристик и быстрое реагирование на возникающие сложности. Закон должен идти в ногу с «ускорением» и защищать возможности, открываемые технологическим развитием. Целесообразность использования механизма правового дерегулирования, основанного на одномоментном пересмотре и отсечении большого количества устаревших и неэффективных регуляций, в условиях глобальных цифровых трансформаций и турбуленций, является очевидным и выступает ярким примером, когда регулятивные меры становятся не только легкими, но и разумными, служат интересам общества и способствуют своевременному внедрению инноваций, открывая новые цифровые возможности. Данная регуляторная технология позволяет адаптировать регулирование к изменяющейся цифровой реальности и трансформационным процессам в экономике, пересмотреть весь «жизненный цикл» требований, предъявляемых к ведению бизнеса, избегая, таким образом, чрезмерного регулирования в той или иной сфере экономических отношений.

Выводы

1. Процессы цифровизации в экономической сфере привели наряду с открытием новых возможностей для бизнеса к проблеме, связанной с появлением значительного количества неактуальных, устаревших, формальных регуляторных правил, не отвечающих требованиям и принципам рыночной экономики. Такое положение дел стало причиной возникновения непреодолимых барьеров для ведения бизнеса и увеличило административную нагрузку на хозяйствующие субъекты, послужило основанием для поиска новых эффективных законодательных механизмов по устранению избыточного правового регулирования.

2. Существенную роль в решении вопросов по сокращению неэффективных правил и обеспечению правовой устойчивости играет активное внедрение комплексной полноценной ОРВ законодательных актов, содержащих обязательные требования (включая ретроспективную оценку), наряду с использованием новейших регуляторных технологий, среди которых наибольшую популярность набирают механизмы правового дерегулирования, такие как регуляторная гильотина, которая может использоваться не только для разовой и секторной корректировки законодательства (по отдельным отраслям (подотраслям) экономики), но и для проведения широкомасштабных реформ, предусматривающих системный характер.

3. Современная регуляторная гильотина рассматривается в юридической науке как механизм комплексного анализа и пересмотра действующего нормативного массива и необходимый элемент совершенствования системы обязательных требований. Данная регуляторная технология успешно выполняет функцию фильтра, устраняя именно те правила, действие которых становится обременительным для субъектов хозяйствования с точки зрения экономической необходимости, рациональности и законности.

4. Принципами «регуляторной гильотины» являются: всеобщность пересмотра законодательной базы; быстрота и окончательность принятия решения о сохранении, упрощении или отмене правовых норм; отмена в пользу реформы бремени доказывания необходимости сохранения правовых норм (презумпция зарегулированности экономических отношений); универсальность критериев оценки правовых актов.

5. Для успешного внедрения единой полноценной процедуры оценки регулирующего (регуляторного) воздействия в совокупности с иными регуляторными технологиями, включая гильотину, необходим целый ряд условий:

- государственная и правовая поддержка проведения полномасштабного пересмотра всех обязательных требований, предъявляемых к бизнесу;
- формирование специальных структур и институтов, ответственных за проведение регуляторных реформ;
- подход «сверху вниз» при проведении реформы, когда решения принимаются на самом высоком уровне;
- измерение существующей проблемы регулирования, определение ее масштабов, определение цели реформы;
- переход к полному циклу ОРВ, предусматривающему усиление действующего механизма ОРВ, объединение всех существующих аналитических инструментов регулирования в единую процедуру;
- точное определение области (сфер регулирования) для проведения инвентаризации законодательства;
- разработка единых общих научных критериев эффективного регулирования и устранения на их основании тех норм, которые утратили свою целесообразность;
- прозрачность и широкое участие заинтересованных сторон в процессе пересмотра действующей законодательной базы;
- наличие технических возможностей для поддержки и проведения реформ;
- создание всеобщего единого реестра требований в целях их систематизации и информирования заинтересованных лиц и др.

6. Зарубежный опыт показал, что проблема зарегулированности экономического поведения является системной, требующей проведения неоднократных регуляторных реформ. Это объясняется тем, что на этапе интенсивных цифровых преобразований экономики государство постоянно вводит все новые правила для ведения бизнеса, которые по прошествии времени могут терять свою актуальность, противоречить друг другу, создавая законодательные завалы, приводя к чрезмерному регулированию и неоправданным расходам для субъектов хозяйствования.

7. Правовой опыт Российской Федерации по повышению эффективности регулирования в экономической сфере продемонстрировал комплексный подход в решении вопросов по совершенствованию системы обязательных требований, предъявляемых к бизнесу. Внедрение нового самостоятельного правового института обязательного требования, включившего в себя регуляторную гильотину – перспективный инструмент недифференцированного сокращения избыточных требований, позволило сформировать четкий единый порядок разработки и оценки соблюдения обязательных требований, провести кардинальную регуляторную реформу законодательства, позволившую распутать сложные регуляторные узлы и масштабно пересмотреть действующие правила во всех сферах экономической деятельности.

Список литературы

- Александров, О. В. (2019). «Регуляторные гильотины»: международный опыт устранения препятствий для бизнеса и инвестирования. *Торговая политика*, 1(17), 107–119. EDN: <https://www.elibrary.ru/zauags>. DOI: <https://doi.org/10.17323/2499-9415-2019-1-17-107-119>
- Алексеев, С. С. (1966). *Механизм правового регулирования в социалистическом государстве*. Москва: Юридическая литература. <https://www.elibrary.ru/sifyfj>

- Артеменко, Е. А. (2020). Регуляторная гильотина как механизм дерегулирования и борьбы с коррупцией. *Вестник Томского государственного университета. Экономика*, 52, 7–31. EDN: <https://www.elibrary.ru/hixdez>. DOI: <https://doi.org/10.17223/19988648/52/1>
- Давыдова, М. Л. (2020). «Умное регулирование» как основа совершенствования современного правотворчества. *Журнал российского права*, 11, 14–29. EDN: <https://www.elibrary.ru/ynerpx>. DOI: <https://doi.org/10.12737/jrl.2020.130>
- Дегтярев, М. В. (2021). Новейшие регуляторные технологии и инструменты: дефиниция и классификация. *Право и государство: теория и практика*, 12(204), 180–183. EDN: <https://www.elibrary.ru/zcmmne>. DOI: https://doi.org/10.47643/1815-1337_2021_12_180
- Дегтярев, М. В. (2022a). *Новейшие регуляторные технологии и инструменты: Регуляторные эксперименты, песочницы, гильотины, экосистемы, платформы*. Москва: Буки-Веди.
- Дегтярев, М. В. (2022b). Новейшие регуляторные технологии и инструменты: резоны и предпочтения, риски и проблемы. *Право и государство: теория и практика*, 1(205), 179–183. EDN: <https://www.elibrary.ru/mpyvro>. DOI: https://doi.org/10.47643/1815-1337_2022_1_179
- Дидикин, А. Б. (2021). Обязательные требования и правовые средства их оценки в механизме регуляторной политики. *Мониторинг правоприменения*, 1(38), 4–9. EDN: <https://elibrary.ru/jxccxf>. DOI: <https://doi.org/10.21681/2226-0692-2021-1-4-9>
- Любимов, Ю. С., Новак, Д. В., Цыганков, Д. Б. (2019). Регуляторная гильотина. *Закон*, 2, 20–36. <https://www.elibrary.ru/yxaokl>
- Шаулова, Т. В. (2017). Оценка регулирующего воздействия: очередное увлечение или инструмент развития? *Научные труды Северо-Западного института управления РАНХиГС*, 8(1), 139–143. EDN: <https://www.elibrary.ru/ziwhxj>. DOI: <https://doi.org/10.2139/ssrn.3826436>
- Южаков, В. Н., Добролюбова, Е. И., Покида, А. Н., Зыбуновская, Н. В. (2021). Реформа госконтроля и «регуляторная гильотина»: что получилось с позиции бизнеса? *ЭКО*, 7(565), 151–170. EDN: <https://www.elibrary.ru/uskrhr>. DOI: <https://doi.org/10.30680/ECO0131-7652-2021-7-151-170>
- Beach, T. H., Hippolyte, J.-Laurent, & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. *Automation in Construction*, 118(12). <https://doi.org/10.1016/j.autcon.2020.103285>
- Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. *International Review of Financial Analysis*, 80(2), 1–14, 102023. <https://doi.org/10.1016/j.irfa.2022.102023>
- Contractor, F. J., Dangol, R., Nuruzzaman, N., & Raghunath, S. (2020). How do country regulations and business environment impact foreign direct investment (FDI) inflows? *International Business Review*, 29(2). <https://doi.org/10.1016/j.ibusrev.2019.101640>
- Grassi, L., & Lanfranchi, D. (2022). RegTech in public and private sectors: the nexus between data, technology and regulation. *Journal of Industrial and Business Economics*, 49(3), 441–479. <https://doi.org/10.1007/s40812-022-00226-0>
- Haidar, J. I. (2012). The impact of business regulatory reforms on economic growth. *Journal of the Japanese and International Economies*, 26(3), 285–307. <https://doi.org/10.1016/j.jjie.2012.05.004>
- Jakupец, V., & Kelly, M. (2016). Regulatory impact assessment: the forgotten agenda in ODA. *Assessing the Impact of Foreign Aid*, 95–106. <https://doi.org/10.1016/b978-0-12-803660-0.00007-6>
- Nosova, S., & Norkina, A. (2021). Digital technologies as a new component of the business process. *Procedia Computer Science*, 190, 651–656. EDN: <https://www.elibrary.ru/zryypb>. DOI: <https://doi.org/10.1016/j.procs.2021.06.076>
- Polemis, M. L., & Stengos, T. (2020). The impact of regulatory quality on business venturing: A semi-parametric approach. *Economic Analysis and Policy*, 67, 29–36. <https://doi.org/10.1016/j.eap.2020.05.005>
- Purnomo, A., Susanti, T., Rosyidah, E., Firdausi, N., & Idhom, M. (2022). Digital economy research: Thirty-five years insights of retrospective review. *Procedia Computer Science*, 197(13), 68–75. EDN: <https://www.elibrary.ru/zgdxjk>. DOI: <https://doi.org/10.1016/j.procs.2021.12.119>
- Rowthorn, V., Plum, A., & Zervos, J. (2017). Legal and Regulatory Barriers to Reverse Innovation. *Annals of Global Health*, 82(6), 991–1000. <https://doi.org/10.1016/j.aogh.2016.10.013>
- Youssef, A. B., Boubaker, S., Dedaj, B., & Carabregu-Vokshi, M. (2021). Digitalization of the economy and entrepreneurship intention. *Technological Forecasting and Social Change*, 164(5), 120043. <https://doi.org/10.1016/j.techfore.2020.120043>

Сведения об авторе



Минич Светлана Александровна – младший научный сотрудник отдела исследований в области гражданского, экологического и социального права Института правовых исследований, Национальный центр законодательства и правовых исследований Республики Беларусь

Адрес: 220030, Республика Беларусь, г. Минск, ул. Берсона, 1а

E-mail: ekabpils75@mail.ru

ORCID ID: <https://orcid.org/0000-0003-0713-3378>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/GWC-0287-2022>

Google Scholar ID: <https://scholar.google.ru/citations?user=iYsfRdIAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1022812

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.23.31 / Государственное регулирование предпринимательской деятельности

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 15 октября 2022 г.

Дата одобрения после рецензирования – 5 февраля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.34>

Improving the System of Mandatory Requirements to Business under the Digital Transformation of Economy

Svetlana A. Minich

National Centre for Legislation and Legal Research of the Republic of Belarus
Minsk, Republic of Belarus

Keywords

Business activity,
business,
deregulation,
digital technologies,
economy,
law,
legal regulation,
legislation,
mandatory requirements,
regulatory guillotine

Abstract

Objective: to elaborate scientifically substantiated proposals for improving the system of mandatory requirements in the sphere of business and other economic activity under formation of digital economy, taking into account the foreign experience of eliminating barriers for business and the available practice of legislation optimization in this sphere.

Methods: the research methodological basis consists of traditional general and specific methods of scientific cognition: dialectical, formal-logical, historical-comparative, systematic, terminological, general logic methods (analysis, synthesis, generalization, induction, deduction, etc.), as well as special methods: historical-legal, formal-legal, and method of comparative jurisprudence.

Results: the author investigated and systematized theoretical approaches and experience of improving the system of mandatory requirements in foreign countries and the Russian Federation; the possibilities of introducing the most successful innovative legal instruments and practices to improve the regulation of economic relations were considered. The role of a retrospective assessment of the regulatory impact of existing regulatory legal acts containing mandatory requirements in addressing issues of reducing burdensome rules and ensuring legal stability in the context of digital transformation of the economy was determined. The international experience of implementing the regulatory guillotine

© Minich S. A., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

mechanism was considered; its essence, purpose, tasks, basic principles, and algorithm of operation were revealed. The issues of establishing and evaluating the application of the requirements for business contained in regulatory legal acts were analyzed.

Scientific novelty: the author's comprehensive analysis of existing scientific developments on improving the system of mandatory requirements for business; systematization of scientific and theoretical approaches to the selection of innovative legal instruments to eliminate excessive legal regulation of economic relations; generalization of successful foreign practices in the implementation of "regulatory guillotine" measures.

Practical significance: recommendations were developed for effective reduction of burdensome requirements that negatively affect the development of business in the context of digital transformation of the economy. Conditions were determined for the implementation of a full-fledged regulatory impact assessment procedure and the successful implementation of regulatory reforms. The results of the study can be used in standard-setting activities and in the educational process when elaborating educational programs in Economics and Law.

For citation

Minich, S. A. (2023). Improving the System of Mandatory Requirements to Business under the Digital Transformation of Economy. *Journal of Digital Technologies and Law*, 1(3), 775–802. <https://doi.org/10.21202/jdtl.2023.34>

References

- Aleksandrov, O. V. (2019). Regulatory guillotines: international experience in removing barriers to business and investment. *Trade policy*, 1(17), 107–119. (In Russ.). <https://doi.org/10.17323/2499-9415-2019-1-17-107-119>
- Alekseev, S. S. (1966). *Mechanism of legal regulation in a Socialist state*. Moscow: Yuridicheskaya literatura. (In Russ.).
- Artemenko, E. A. (2020). The regulatory guillotine as a mechanism for deregulation and anti-corruption. *Tomsk State University Journal of Economics*, 52, 7–31. (In Russ.). <https://doi.org/10.17223/19988648/52/1>
- Beach, T. H., Hippolyte, J.-Laurent, & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. *Automation in Construction*, 118(12). <https://doi.org/10.1016/j.autcon.2020.103285>
- Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. *International Review of Financial Analysis*, 80(2), 1–14, 102023. <https://doi.org/10.1016/j.irfa.2022.102023>
- Contractor, F. J., Dangol, R., Nuruzzaman, N., & Raghunath, S. (2020). How do country regulations and business environment impact foreign direct investment (FDI) inflows? *International Business Review*, 29(2). <https://doi.org/10.1016/j.ibusrev.2019.101640>
- Davydova, M. L. (2020). Smart Regulation as the Basis for Improving Modern Law-Making. *Journal of Russian Law*, 11, 14–29. (In Russ.). <https://doi.org/10.12737/jrl.2020.130>
- Degtyarev, M. V. (2021). The latest regulatory technologies and tools: definition and classification. *Law and State: The Theory and Practice*, 12(204), 180–183. (In Russ.). https://doi.org/10.47643/1815-1337_2021_12_180
- Degtyarev, M. V. (2022a). The latest regulatory technologies and tools: reasons and preferences, risks and problems. *Law and State: The Theory and Practice*, 1(205), 179–183. (In Russ.). https://doi.org/10.47643/1815-1337_2022_1_179

- Degtyarev, M. V. (2022b). *The latest regulatory technologies and tools: regulatory experiments, sandboxes, guillotines, ecosystems, platforms*. Moscow: Buki-Vedi. (In Russ.).
- Didikin, A. B. (2021). Mandatory requirements and legal means for their assessment in the regulatory policy mechanism. *Monitoring of law enforcement*, 1(38), 4–9. (In Russ.). <https://doi.org/10.21681/2226-0692-2021-1-4-9>
- Grassi, L., & Lanfranchi, D. (2022). RegTech in public and private sectors: the nexus between data, technology and regulation. *Journal of Industrial and Business Economics*, 49(3), 441–479. <https://doi.org/10.1007/s40812-022-00226-0>
- Haidar, J. I. (2012). The impact of business regulatory reforms on economic growth. *Journal of the Japanese and International Economies*, 26(3), 285–307. <https://doi.org/10.1016/j.jjie.2012.05.004>
- Jakupec, V., & Kelly, M. (2016). Regulatory impact assessment: the forgotten agenda in ODA. *Assessing the Impact of Foreign Aid*, 95–106. <https://doi.org/10.1016/b978-0-12-803660-0.00007-6>
- Lyubimov, Yu. S., Novak, D. V., & Tsygankov, D. B. (2019). Regulatory guillotine. *Statute*, 2, 20–36. (In Russ.).
- Nosova, S., & Norkina, A. (2021). Digital technologies as a new component of the business process. *Procedia Computer Science*, 190, 651–656. <https://doi.org/10.1016/j.procs.2021.06.076>
- Polemis, M. L., & Stengos, T. (2020). The impact of regulatory quality on business venturing: A semi-parametric approach. *Economic Analysis and Policy*, 67, 29–36. <https://doi.org/10.1016/j.eap.2020.05.005>
- Purnomo, A., Susanti, T., Rosyidah, E., Firdausi, N., & Idhom, M. (2022). Digital economy research: Thirty-five years insights of retrospective review. *Procedia Computer Science*, 197(13), 68–75. <https://doi.org/10.1016/j.procs.2021.12.119>
- Rowthorn, V., Plum, A., & Zervos, J. (2017). Legal and Regulatory Barriers to Reverse Innovation. *Annals of Global Health*, 82(6), 991–1000. <https://doi.org/10.1016/j.aogh.2016.10.013>
- Shaulova, T. (2017). Regulatory Impact Assessment: Another Hobby or Development Tool? *Nauchnye trudy Severo-Zapadnogo instituta upravleniya RANKhIGS*, 8(1), 139–143. (In Russ.). <https://doi.org/10.2139/ssrn.3826436>
- Youssef, A. B., Boubaker, S., Dedaj, B., & Carabregu-Vokshi, M. (2021). Digitalization of the economy and entrepreneurship intention. *Technological Forecasting and Social Change*, 164(5), 120043. <https://doi.org/10.1016/j.techfore.2020.120043>
- Yughakov, B., Dobrolyubova, E., Pokida, A., & Zybunovskaya, H. (2021). The Law Enforcement Reform and Regulatory Guillotine: What's the Outcome from the Business Perspective. *ECO*, 7(565), 151–170. (In Russ.). <https://doi.org/10.30680/ECO0131-7652-2021-7-151-170>

Author information



Svetlana A. Minich – Junior Researcher of the Department of Research in the sphere of Civil, Environmental and Social Law, National Centre for Legislation and Legal Research of the Republic of Belarus

Address: 1a Berson Str., 220030 Minsk, Republic of Belarus

E-mail: ekabpils75@mail.ru

ORCID ID: <https://orcid.org/0000-0003-0713-3378>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/GWC-0287-2022>

Google Scholar ID: <https://scholar.google.ru/citations?user=iYsfRdIAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1022812

Conflict of interests

The authors declare no conflict of interests.

Funding

The research was not sponsored.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – October 15, 2023

Date of approval – February 5, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:349.44:004:352

EDN: <https://elibrary.ru/djkvsd>

DOI: <https://doi.org/10.21202/jdtl.2023.35>

«Умные города»: правовое регулирование и потенциал развития

Елена Юрьевна Тихалева

Среднерусский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
г. Орел, Российская Федерация

Ключевые слова

Законодательство,
местное самоуправление,
муниципальное
образование,
муниципальное право,
право,
правовое регулирование,
умный город,
цифровая платформа,
цифровизация,
цифровые технологии

Аннотация

Цель: исследование тенденций развития концепции «умных городов» и их правового регулирования.

Методы: в работе использовались общенаучные (индукция, дедукция) и специальные (системно-структурный, сравнительно-правовой анализ) методы. Кроме того, в исследовании применялись методы обзорного анализа, чтобы изучить статус-кво для «умных городов». До сих пор инновационные исследовательские подходы в рамках рассмотрения концепций «умного города» встречаются редко, как и перспективы, касающиеся целевого управления знаниями и сотрудничества соответствующих заинтересованных сторон. Если говорить о специальных методах исследования цифровых отношений, был использован контент-анализ (метод создания воспроизводимых и обоснованных выводов из текстов (или другого значимого материала) в контексте их использования). Поскольку результаты предыдущих исследований и концепций, касающиеся «умных городов», доступны, также применялся дедуктивный контент-анализ.

Результаты: дана характеристика общественных отношений, складывающихся в процессе развития концепции «умных городов». Обозначены ключевые правовые акты, принципы формирования и функционирования «умных городов» с учетом российского и зарубежного опыта. В связи с этим приведены примеры успешных практик из деятельности как российских, так и зарубежных муниципальных образований с учетом проводимых конкурсов, и рейтингов, определяемых центральными структурами. Обобщены популярные направления, широко внедряемые на местном уровне, и выделены возможные проблемы реализации данного проекта в нашем государстве.

© Тихалева Е. Ю., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: в статье осуществлен анализ имеющегося правового регулирования, а также результатов внедрения концепции «умных городов». Определены перспективные технологии и методы, необходимые для достижения целей реализации концепции. Выделены элементы, обеспечивающие устойчивость «умных городов», отвечающих требованиям будущего. Высказана авторская позиция о тесной взаимосвязи данного явления с институтом местного самоуправления в контексте возможного развития последнего с подключением искусственного интеллекта в процесс по принятию управленческих решений. Прежде всего речь идет об использовании потенциала интернета вещей. На практике возникает немалое количество проблем, связанных с реализацией нормативно закрепленных положений, что подразумевает необходимость проведения дальнейших научных исследований в анализируемой сфере.

Практическая значимость: обусловлена недостаточной разработанностью данных об особенностях и перспективах внедрения идеи «умных городов». Положения проведенного исследования позволят осуществлять эффективную работу по совершенствованию механизмов правового регулирования рассматриваемой концепции и ее повсеместному распространению.

Для цитирования

Тихалева, Е. Ю. (2023). Умные города: правовое регулирование и потенциал развития. *Journal of Digital Technologies and Law*, 1(3), 803–824. <https://doi.org/10.21202/jdtl.2023.35>

Содержание

Введение

1. Правовое регулирование «умных городов»

2. Содержание концепции «умных городов»

3. Практика внедрения концепции «умных городов»

Выводы

Список литературы

Введение

В настоящее время значение городов как основных центров социально-экономической жизни возрастает. С одной стороны, они становятся основными местами, где селятся люди. Действительно, сегодня 55 % населения земного шара проживает в городах, а к 2050 г. эта доля достигнет 70 %. В Европейском союзе, в частности, эти показатели еще выше – 70 и 80 % соответственно.

Современные цифровые технологии привели к значительным изменениям в жизни различных государств и обществ, а также трансформировали принципы и методы организации управления. Эти процессы также затронули не только государственный, но и местный уровень.

Если в 90-е гг. XX в. речь шла о так называемых экогородах и низкоуглеродных городах, то в настоящее время все более перспективной становится идея появления так называемых умных городов с широким использованием информационных

и цифровых технологий, в том числе интернета вещей. Она захватывает умы политических деятелей всего мирового сообщества, в том числе и России, позволяет функционировать городу подобно единому организму.

Умный город – это город, который использует набор самых современных технологий, прежде всего информационных и коммуникационных, чтобы предоставлять более качественные услуги своим гражданам и пользователям. Это общее определение открывает двери для участия многих заинтересованных сторон в проектировании умных городов, таких как ученые-компьютерщики, инженеры-программисты, бизнес-менеджеры, городские девелоперы, градостроители и городские чиновники. Действительно, трудно создать единую структуру для «умных городов» и еще труднее измерить успех «умного города» в реализации его видения.

Современная концепция умных городов возникла из самых первых инициатив по созданию цифровых городов в 1990-х гг. Кроме того, с годами она превратилась в идею, использующую новые технологии интернета вещей для достижения стратегических целей «умного города».

«Умные города» могут стать фактором преодоления многих имеющихся социально-экономических проблем, а также способствовать экономическому росту. В основу идеи положена концепция возможности для самореализации каждого человека. Это пересечение цифровых технологий и интеллектуальных потенциалов систем управления. Данная концепция стала следствием феномена урбанизации, повышения экономического значения городов и растущего спроса на более стабильную жизнь (Attaran et al., 2022).

Ярким примером является опыт Индии. Здесь происходит появление новых городов между урбанистическими центрами с целью избегания перенаселения в крупных городах, привлекающих своими перспективами людей из глубинки. В качестве мотивации выступают заманчивые перспективы новых «умных городов» с передовой инфраструктурой, легкой и доступной в использовании (Стрельникова, Цуциев, 2017). В настоящее время здесь запущено сто «умных городов», и власти рассчитывают, что граждане будут использовать инновации с целью решения демографических и экономических проблем (Jothimani et al., 2022). Аналогично подобные веяния набирают обороты в Китае, цифровые платформы которого начинают распространяться в мировом пространстве (например, Alibaba's City Brain) (Caprotti & Liu, 2020).

1. Правовое регулирование «умных городов»

Еще в 2015 г. Европейский экономический и социальный комитет в своем решении указывал на возможность использования концепции «умных городов» для оперативного развития европейской промышленной экономики (European Economic and Social Committee, 2015). В 2016 г. на конференции Организации Объединенных Наций по жилью и устойчивому городскому развитию пристальное внимание также было уделено необходимости использования идеи «умного города».

В России «умный город» возник благодаря ведомственному проекту цифровизации городского хозяйства (объединяет Паспорта национальных проектов «Цифровая экономика» и «Жилье и городская среда») начиная с 2018 г.¹ Указанная строка расхо-

¹ Указ Президента РФ № 204 от 07.05.2018. (2018). *Собрание законодательства РФ*, 20, ст. 2817.

дов включена в федеральный бюджет. Список пилотных городов проекта включает 79 (изначально – 33) населенных пунктов (Ганин, Ганин, 2014).

Так, «Цифровая экономика» включает в себя следующие федеральные проекты: «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Цифровые технологии», «Цифровое государственное управление», «Искусственный интеллект»². В комплексе данные проекты подразумевают создание автоматизированной системы управления и контроля «умных городов».

Кроме того, были приняты «Национальная стратегия развития искусственного интеллекта на период до 2030 г.»³ и «Стратегическое направление в области цифровой трансформации строительной отрасли, городского и жилищно-коммунального хозяйства Российской Федерации до 2030 г.»⁴ в целях обеспечения ускорения развития искусственного интеллекта, развития роботизированных сервисов, а также повышения доступности предоставляемой информации. Несомненно, внедрение данных документов в практику жизнедеятельности населения оказывает влияние и на концепцию «умного города», способствуя повышению: эффективности планирования, прогнозирования и принятия управленческих решений; качества предоставляемых услуг, в первую очередь в политической и социальной сферах.

В 2019 г. разработке подверглась методика оценки IQ городов⁵, в которой выделены важные критерии оценки цифровизации муниципальных образований, например, наличие интеллектуальной системы социальных услуг, инвестиционный климат. В 2022 г. на ведомственном уровне сформулированы показатели цифровизации городского хозяйства, которые раскрывают возможности определения городов в качестве «умных» (обратная связь с гражданами, энергетика, безопасность и т. п. – 18 показателей среди базовых и дополнительных)⁶.

Детальное правовое регулирование на федеральном уровне получил соответствующий проект развития города Москвы⁷.

На международной арене еще в 2000 г. была принята Окинавская хартия глобального информационного общества, заложившая основы для последующего развития

² Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).

³ Указ Президента РФ № 490 от 10.10.2019. (2019). *Собрание законодательства Российской Федерации*, 41, 5700.

⁴ Распоряжение Правительства РФ № 3883-р от 27.12.2021. (2021). *Официальный интернет-портал правовой информации*. <http://www.pravo.gov.ru>

⁵ Приказ Минстроя России № 924/пр от 31.12.2019. (2019). *СПС «КонсультантПлюс»*. <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=379313#q40fMiTCYjxSO6p22>

⁶ Приказ Минстроя России № 357/пр от 11.05.2022. (2022). <https://docs.cntd.ru/document/350551073>

⁷ О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 19 Федерального закона «О персональных данных» № 123-ФЗ от 24.04.2020. *Собрание законодательства Российской Федерации*, 17, ст. 2701.

«умных городов»⁸. В 2017 г. созданы Азиломарские принципы искусственного интеллекта в рамках конференции, проводимой в США. В 2019 г. на Генеральной конференции ЮНЕСКО разработана резолюция о разработке этических норм в области искусственного интеллекта.

Модель «умного города», внедряемая в Европе с конца первого десятилетия XXI в., осуществлялась, прежде всего, на основе работы такой организации, как Европейское инновационное партнерство по «умным городам и сообществам» (EIP-SCC).

В 2020 г. была принята программа Организации экономического сотрудничества и развития (ОЭСР) по «умным городам» и инклюзивному росту, включающая большое разнообразие моделей, основанных на местных особенностях⁹. В программе выделено шесть ключевых параметров для измерения эффективности «умного города». Акцент сделан на рентабельность инвестиций в «умный город» и их окупаемость, а также приведение инвестиций в соответствие со стратегическими приоритетами города и потребностями граждан.

С 2021 г. действует Глобальная партнерская программа Всемирного банка «Умный город», направленная на определение приоритетности мер по устранению неравенства и цифрового разрыва в городах¹⁰.

Если говорить об отдельных государствах, то, например, во Франции издан Закон № 2016-1321 от 7 октября 2016 г. «О цифровой республике», подразумевающий открытость доступа к публичным данным, аккумулируемым государственными структурами¹¹.

Другим примером является Стратегия развития «умных городов», разработанная в Будапеште, которая демонстрирует смешанную картину подходов «сверху вниз» и «снизу вверх», главным образом из-за особого взгляда на стратегические рамки. Местное самоуправление Будапешта является ключевым фактором и участником деятельности по развитию «умных городов». Венгерское правительство реализует несколько проектов в пределах своей юрисдикции, в то время как ключевые государственные службы централизованы на национальном уровне, что оставляет городу мало места для планирования и реализации своих действий. Стратегия развития «умных городов» Будапешта сосредоточена на технологических подходах. Кроме того, деятельность по развитию «умных городов» охватывает большинство городских областей интегрированным образом; город хорошо вписывается в европейское понимание «умных городов», уделяя особое внимание экологически чистым решениям (Csukás & Szabó, 2022).

Аналогичная работа ведется на уровне межгосударственного взаимодействия. Так, в 2018 г. Министерством строительства и жилищно-коммунального хозяйства Российской Федерации (далее – Минстрой России) был подписан меморандум

⁸ Окинавская хартия глобального информационного общества от 22.07.2000. (2000, август). *Дипломатический вестник*, 8.

⁹ *The OECD Programme on Smart Cities and Inclusive Growth*. <https://www.oecd.org/cfe/cities/smart-cities.htm/>

¹⁰ Gunes Basat, Narae Choi. (July 09, 2021). 5 views: What makes a city 'smart'? <https://blogs.worldbank.org/sustainablecities/5-views-what-makes-city-smart/>

¹¹ LOI № 2016-1321 du 7 octobre 2016 pour une République numérique. (2016, 8 octobre). *Journal Officiel de la RÉPUBLIQUE FRANÇAISE*.

с Министерством земель, инфраструктуры, транспорта и туризма Японии¹². Данное государство активно занимается созданием и развитием «умных городов», в частности, к таким относятся: Цунасима, Аидзувакамацу (в городах предполагается широкое внедрение инновационных технологий); Фуджисава, Суйта (акцент сделан на экологическую составляющую) (Langendahl, 2021).

На подзаконном уровне в нашем государстве закреплена дефиниция «умный город», подразумевающая установленную парадигму развития города, активно внедряющего передовые цифровые технологии с целью улучшения уровня жизни граждан, качества поставляемых услуг и результативности процессов управления при необходимом обеспечении нужд населения¹³. Также обозначены базовые направления воплощения данного подхода в конкретных муниципальных образованиях:

- городская среда;
- безопасный город;
- цифровое городское управление;
- инвестиционный климат;
- благосостояние людей.

За рубежом выделяются такие направления smart city, как¹⁴:

- smart care (умное обслуживание, мониторинг);
- smart energy (умная энергетика);
- smart society (умное общество);
- smart office (умный офис);
- smart mobility (интеллектуальная мобильность);
- smart space (умное пространство);
- smart infrastructure (умная инфраструктура);
- smart transportation (умный транспорт);
- smart data (интеллектуальные данные).

Интеграция различных компонентов, перечисленных выше, может повысить успешность подобного проекта. По нашему мнению, связующим звеном здесь может выступать качество жизни горожан как одна из основных ценностей, гарантируемых в таком городе.

¹² Меморандум относительно развития взаимодействия в сферах строительства, жилищно-коммунального хозяйства и городской среды с целью создания «умных городов» между Министерством строительства и жилищно-коммунального хозяйства Российской Федерации и Министерством земель, инфраструктуры, транспорта и туризма Японии (подписан в г. Москве 26.05.2018). <https://minstroyrf.gov.ru/docs/16971/>

¹³ Приказ Минстроя России № 866/пр от 25.12.2020. <https://minstroyrf.gov.ru/docs/81884/>; Паспорт федерального проекта «Формирование комфортной городской среды» (утв. протоколом заседания проектного комитета по национальному проекту «Жилье и городская среда» от 21.12.2018 № 3). https://www.consultant.ru/document/cons_doc_LAW_319514/

¹⁴ Maddox, T. (2016, August 1). Smart cities: six essential technologies. <https://www.techrepublic.com/article/smart-cities-6-essential-technologies/>; Marr, B. (2020, July 2). The smart cities of the future: five ways technology is transforming our cities. <https://www.forbes.com/sites/bernardmarr/2020/07/02/the-smart-cities-of-the-future-5-ways-technology-is-transforming-our-cities/?sh=781277c673f8>

2. Содержание концепции «умных городов»

«Умные города» – это территории, где работают местные инновационные системы, получающие передовые возможности, что выражается в повышении конкурентоспособности, улучшении состояния окружающей среды, увеличении числа рабочих мест и благополучия граждан (Vukovic et al., 2021; Шкваря, Семенов, 2020).

Население города, квалифицированные сотрудники и инновационные предприятия – фундаментальные элементы, на которых строится подобная концепция (Fedorchenko & Karlyavina, 2021). В связи с этим важно уделять внимание росту уровня образования, поощрению инициатив и творческих активностей со стороны граждан, установлению партнерских отношений. В среде, где работают умные люди, акцент делается именно на человеческих ресурсах, управлении потенциалом, обработке и анализе данных самими людьми с целью принятия управленческих решений и осуществления производственных процессов.

Определяющими направлениями в развитии концепции «умного города» являются:

- 1) сравнение муниципалитетов между собой и выбор лучшего опыта;
- 2) понимание тенденций развития «умного города», их динамики, выявление недостатков и определение средств и ресурсов для их преодоления;
- 3) учет местных факторов, влияющих на развитие конкретного муниципалитета;
- 4) подготовка плана развития, включающего основные компоненты;
- 5) создание рабочей группы из представителей властных структур и общественности, осуществляющей контроль за реализацией проекта.

Используемые технологии могут сохранять жизни, предотвращать преступления, уменьшать отходы, экономить время, вырабатывать продуктивные для города решения. Другая цель – отвечать более эффективно и динамично вызовам, потребностям и желаниям жителей территории.

Основными принципами концепции «Умный город» являются:

- 1) ориентация на человека (данный принцип обусловлен приоритетом осуществления прав и свобод человека и гражданина, необходимостью обеспечения возможностей для реализации каждого индивида и решения его проблем по месту жительства через организацию системы обратной связи и адресное предоставление услуг, т. е. главная цель – повышение качества жизни граждан);

- 2) формирование устойчивой и безопасной среды (на первый план выходит безопасность жителей, обеспечение работы налаженных информационных сетей, комфортность городской среды, доступность социальной инфраструктуры; этот принцип предполагает активное развитие систем общественного наблюдения, общественной и экологической безопасности, интеллектуального городского освещения; повсеместное установление средств фото- и видеофиксации на дорогах, формирование интеллектуальных транспортных систем, стимулирование развития систем энергосбережения) (Низамиева, 2021; Куранов, 2020);

- 3) соблюдение баланса интересов, принципов развития и возможностей (указанный принцип подразумевает осуществление учета общественного мнения при принятии значимых решений, воздействующих на городскую среду (проведение голосований, опросов); вовлечение населения в формы самоорганизации на местном уровне, совместную реализацию общественных проектов; достижение консенсуса между интересами муниципалитета, предпринимательских структур и местных жителей) (Якушина, 2021);

4) доступность и удобство сервисов и услуг (выступает в качестве одного из преимуществ проживания в «умном городе»; внедрение принципа обеспечивается интернетизацией города, предоставлением многих услуг через электронные ресурсы (например, портал госуслуг, электронные приемные); при этом осуществляется учет потребностей разных групп населения в зависимости от возраста, пола, образования, профессии и т. п.) (Bekbolat et al., 2021);

5) интегрированность, взаимодействие и открытость (соответствующий принцип относится к механизму действия городских сервисов, предполагающему сбор и анализ всех необходимых данных, исключение их дублирования, предоставление заинтересованным лицам) (Белов, Смирнов 2018);

6) непрерывное совершенствование качества управления (принцип достигается за счет деятельности высокопрофессиональных служащих, в первую очередь менеджеров; анализа проблемных моментов; создания баз и реестров данных, отвечающих мировым стандартам; использования различных подсистем в формировании рационального управления) (Шарова, 2019);

7) акцент на экономической эффективности (этот принцип позволяет оценить инвестиционную привлекательность города, его инвестиционный климат (наличие бизнес-инкубаторов, технопарков и т. п.), что способствует созданию новых рабочих мест, повышению производительности труда; подразумевает необходимость обеспечения финансовой независимости города посредством активного развития ключевых направлений инвестиционной деятельности) (Голикова, 2020);

8) главенство долгосрочных решений над краткосрочными выгодами (данное направление обеспечивает экономический рост на перспективу, будущие поколения; позволяет избежать негативных последствий сиюминутных субъективных решений, поскольку именно качественные решения долгосрочного характера в дальнейшем оказывают непосредственное влияние на краткосрочные шаги) (Костко и др., 2022);

9) применение наилучших доступных технологий (принцип предполагает оценку технологии с точки зрения требований стоимости, сложности внедрения и обоснованности в конкретных условиях, необходимости минимизации негативных последствий; здесь возможно применение экспериментальных правовых режимов).

В зависимости от порядка и целей создания «умные города» могут быть, на наш взгляд, классифицированы следующим образом:

- новые города, которые искусственно создаются и изначально были построены для использования новых информационных технологий и привлечения бизнес-структур (Фудзисава в Японии, Неом в Саудовской Аравии, Рублево-Архангельское в Московской области);

- существующие города, имеющие богатую историю развития и переживающие на современном этапе процессы модернизации технологий как необходимое условие их дальнейшего развития и адаптации к складывающимся условиям (Лондон, Москва и др.);

- специализированные города, имеющие конкретную цель создания и в связи с этим применяющие процессы цифровизации в отношении выбранного направления развития (бизнес-инкубатор (Кремниевая долина в США), экогород (Масдар в ОАЭ, Неаполис на Кипре и т. п.).

Если говорить о зарубежном опыте внедрения концепции «умных городов», можно выделить следующие заслуживающие внимания моменты.

С 2019 г. Федеральное министерство транспорта, строительства и градостроительства Германии (BMWSB) продвигает немецкие города и муниципалитеты в отношении их планирования и реализации «цифровых стратегий для городов, пригодных для жизни», с финансированием под названием «Умные города, сделанные в Германии». В 2019 г. было профинансировано 13 городов или межмуниципальных проектов, в 2020 г. – еще 32, а в 2021 г. – еще 28. В дополнение к разработке и тестированию интегрированных подходов к «умному городу» целями этой программы финансирования являются сочетание устойчивости с цифровизацией, развитие облачных инфраструктур и сервисов нового поколения (Treude et al., 2022).

Италия фокусируется на внедрении приложений и интеллектуальных систем. Разработка приложений включает в себя строительные платформы, технологии с открытым исходным кодом и платформы городских данных. При разработке систем особое внимание уделяется проектированию вспомогательных систем, эффективности транспортных систем, содействию преобразования уязвимых территорий в «умные» и устойчивые районы.

Великобритания делает акцент на приложениях и управлении, включая разработку совместных инновационных платформ, безопасность данных и проекты транспортной инфраструктуры. Основная деятельность направлена на городских администраторов, развитие услуг, ориентированных на мобильные данные. В частности, планы Лондона состоят в том, чтобы стать глобальным городом – испытательным полигоном для инноваций, где лучшие идеи (например, из сектора искусственного интеллекта) разрабатываются с соблюдением самых высоких стандартов конфиденциальности и безопасности и распространяются по всему миру.

Таким образом, зеленые насаждения, возможность быстрого поиска работы, наличие школ и безопасность граждан являются основными факторами, определяющими европейские умные города. Политика в области «умных городов» на ближайшие годы учитывает основные компоненты их развития и является сквозной задачей в области цифровизации государственных и муниципальных услуг и углубленной реформы в области продвижения бизнес-моделей и продаж продуктов. Подключаемость и безопасность оцифрованных систем также будут формировать поведение населения через их склонность к цифровым компонентам, интеллектуальность, которая обеспечивает устойчивость, адаптивную и ориентированную на будущее оценку рисков (Apostu et al., 2022).

3. Практика внедрения концепции «умных городов»

В целях активизации использования современных цифровых технологий государства прибегают к проведению различных конкурсов, имеющих определенный призовой фонд.

В России ежегодно проводится конкурс «Лучшая муниципальная практика», в котором введена номинация, связанная с интеграцией цифровых технологий или платформенных решений в рамках совершенствования городского хозяйства, т. е. то, что составляет основу деятельности «умного города»¹⁵. Это способствует накоплению передового опыта лучших практик. Конкурс имеет по данной номинации призовой фонд в двести миллионов рублей.

¹⁵ Приказ Минстроя России от 09.07.2020 № 368/пр. (2020). Официальный интернет-портал правовой информации. <http://www.pravo.gov.ru>

Количество подаваемых заявок с каждым годом возрастает, что обеспечивает вовлечение в конкурс различных видов муниципальных образований (в 2020 г. подано 59 заявок из 28 субъектов Российской Федерации, в 2021 г. – 95 заявок из 39 регионов, а в 2022 г. поступила 101 заявка из 41 региона).

Для отбора заявок в конкурсе используется одновременно 58 критериев, в частности:

- перспективы воспроизводства в других муниципальных образованиях;
- возможности участия местного населения;
- степень внедрения передовых технологий;
- взаимосвязь между применением практики и ростом индекса IQ;
- соответствие действующим нормативным правовым актам в рассматриваемой сфере;
- способность разрешения имеющихся в муниципальном образовании проблем и т. д. (Антонова, 2020).

Например, в 2021 г. победителями в конкурсе были признаны Калуга (организация автоматической деятельности центрально-диспетчерской службы государственного унитарного предприятия «Калугаоблводоканал») и сельское поселение Стригуновское Борисовского района Белгородской области (внедрение единой интерактивной базы данных, включающей данные об имеющихся кладбищах, – «Мемориал»)¹⁶.

В целом распространенными тенденциями среди участников конкурса являются:

- формирование цифровых платформ или создание сервисов обратной связи с местными жителями в отраслях хозяйства, испытывающих наибольшие потребности в этом;
- модернизация деятельности сетей энерго-, тепло- и водоснабжения, что связано с вопросами местного значения, входящими в компетенцию органов местного самоуправления.

Если обратить внимание на конкурсы мирового масштаба, в первую очередь стоит отметить Intelligent Community Awards¹⁷ и AI City Challenge¹⁸.

Каждый год в рамках Intelligent Community Awards проходит награждение территориальных образований, интеллектуальных сообществ и партнеров из государственного и частного секторов, которые вносят в них свой вклад. Программа награждений преследует две цели: отметить достижения сообществ в развитии инклюзивного процветания на основе информационных и коммуникационных технологий и собрать данные для исследовательских программ ICF.

AI City Challenge был создан для стимулирования развития и использования искусственного интеллекта в городских условиях. Это проявляется, например, в улучшении транспортных результатов за счет повышения эффективности дорожного движения и безопасности дорог, совершенствовании процессов эксплуатации зданий за счет повышения их энергоэффективности, снижении коллапсов в розничной

¹⁶ Тихалева, Е. Ю. (2022). Применение цифровых технологий на современном этапе реформирования местного самоуправления. В сб. *Государственное и муниципальное управление в России: состояние, проблемы и перспективы: материалы Всероссийской научно-практической конференции* (с. 150). Пермь: Пермский филиал РАНХиГС.

¹⁷ Intelligent Community Forum. <https://www.intelligentcommunity.org/awards>

¹⁸ AI City Challenge. <https://www.aicitychallenge.org>

среде за счет ускорения движения на кассах и т. д. Общим для всех этих разнообразных решений является извлечение полезной информации из множества датчиков с помощью потоковой передачи в реальном времени и пакетной аналитики огромного объема (данных с камер).

Помимо проведения конкурсов, государства могут создавать сайты, содержащие перспективные решения в сфере внедрения цифровых технологий, которые конкретные города используют в любой удобной форме.

В Российской Федерации примером выступает интернет-ресурс «Банк решений умного города»¹⁹, включающий проекты по основным направлениям развития общественной жизни (жилищно-коммунальная, транспортная сферы и т. п.). Речь идет об упрощении процессов управления инфраструктурой (создание автоматизированного программного обеспечения), сокращении стоимости обслуживания городского хозяйства (автоматизация управления) или облегчении жизни граждан (умный пешеходный переход). На сайте размещены паспорта проектов, где можно увидеть содержание проекта: его план, включающий направления реализации, возможный результат использования (расчетный и реальный), требующиеся функциональные свойства, разработчик; период, необходимый для внедрения; финансовые затраты, интеграция проекта в конкретных структурах.

Лидером по реализации указанных технологий в Российской Федерации является Москва (в 2020 г. – по результатам глобального рейтинга «умных городов» – 56-е место; в рейтинге умных городов компании Z/Yen Group Limited (рейтинг деловой активности муниципальных образований) – 44-е место) (Есаян, Трунцевский, 2020). Это логично и отражает тенденции, складывающиеся в мировом сообществе. Очевидно, что самые передовые технологии концентрируются в столицах (примерами выступает развитие Лондона, Сеула (Lee & Nam, 2021)).

Так, в Лондоне в рамках развития концепции «умного города» поддерживаются такие проекты, как Barclays Cycle Hire (приложение, с помощью которого граждане могут получить информацию о наличии и возможностях использования велосипедов напрокат в городе), Listen London Platform (приложение для прослушивания в социальных сетях информации об актуальных проблемах города), Love Clean London (сервис, благодаря которому жители могут сообщить властям о недостатках, связанных с чистотой улиц и парков Лондона) и др.

Кроме того, каждый год Минстрой России формирует рейтинг IQ городов, предполагающий определение городов, достигших наибольших успехов в области цифровизации. При этом используются 47 показателей, разделенных на 10 групп. Отдельное внимание здесь уделяется именно сбалансированности показателей, так как высокие показатели в отдельной группе не всегда свидетельствуют об эффективности использования цифровых технологий в целом. Так, по итогам 2021 г. Москва получила наиболее высокий IQ в рамках крупнейших городов (более одного миллиона человек), а город Саров Нижегородской области – в муниципальных образованиях менее ста тысяч человек²⁰.

¹⁹ Умный город: ведомственный проект Минстроя России. <https://russiasmartcity.ru>

²⁰ Тихалева, Е. Ю. (2022). Применение цифровых технологий на современном этапе реформирования местного самоуправления. В сб. *Государственное и муниципальное управление в России: состояние, проблемы и перспективы: материалы Всероссийской научно-практической конференции* (с. 151). Пермь: Пермский филиал РАНХиГС.

Однако необходимо отметить, что в соответствии с федеративным устройством нашего государства Москва имеет статус города федерального значения, следовательно, исходя из Конституции Российской Федерации, это субъект Российской Федерации. В нашем случае акцент делается на анализ развития муниципальных образований, в первую очередь городских округов.

Если говорить о международных рейтингах, можно обратить внимание на рейтинг Smart City Index (создатели – Центр мировой конкурентоспособности IMD и Сингапурский университет технологии и дизайна), учитывающий как экономические, так и технологические показатели: мобильность, уровень безопасности, перспективы развития и т. п. (всего пять групп показателей, разбитых по соответствующим критериям). По результатам 2021 г. среди российских городов Москва заняла 54-е место, а Санкт-Петербург – 79-е²¹.

Рейтинг технологических городов будущего составляет аналитическое агентство fDi Intelligence, учитывающее развитие инфраструктуры и возможности привлечения инвестиций²².

Стратегическое и консалтинговое бюро Eden Strategy Institute ежегодно публикует рейтинг Top 50 Smart City Government (три группы оценки показателей: сфера, масштаб и интеграция)²³.

При реализации концепции «умного города» целесообразно использовать технологии бенчмаркинга (эталонной оценки), методы моделирования и рейтинговой оценки (Камолов и др., 2022).

Бенчмаркинг в последнее время получил заметное распространение. Данная технология базируется на сравнении значимых аспектов конкретного вида деятельности с результатами конкурентов, что весьма перспективно применительно к реализации инноваций в муниципальных образованиях. Здесь подразумеваются непрерывный поиск новых идей, их реальная адаптация и последующее использование на практике с целью улучшения собственных итогов работы. Бенчмаркинг можно также рассматривать как инструмент контроля (основные методы – оценивание и сопоставление, т. е. статистические) (Xu et al., 2022). При этом важно точно определить параметры, используемые для сравнения; объекты, подходящие для проведения анализа, а также возможности, имеющиеся на практике к адаптации, и желаемые результаты. В связи с этим различают сравнительный (ориентирует на планируемые изменения исходя из определения уровня развития муниципального образования по сравнению с лидерами в соответствующей сфере) и процессный (предполагает совершенствование деятельности в практической плоскости посредством выбора необходимого набора инструментов для достижения цели) бенчмаркинг (Moustaka et al., 2021).

Бенчмаркинг представляет собой последовательное выполнение ряда процедур, должен иметь систематический характер, поэтому он не может использоваться

²¹ Data shows effects of COVID-19 and climate change on citizens' perceptions of how 'smart' their cities are. (2021, October). IMD. <https://www.imd.org/news/updates/data-shows-effects-of-covid-and-climate-change-on-citizens-perceptions-of-how-smart-their-cities-are>

²² FDI Intelligence. <https://www.fdiintelligence.com>

²³ Eden Strategy Institute. <https://www.edenstrategyinstitute.com>

для какой-либо разовой ситуации. Чаще всего данная технология может включать в себя такие этапы, как:

- реинжиниринг (предполагает комплексный подход к решению имеющихся проблем на основе проводимого наблюдения, понимание необходимости переосмысления происходящих управленческих процессов и их качественной переориентации на конкретный результат) (Saragih et al., 2021);
- достижение определенного уровня характеристик конкурентоспособности муниципального образования;
- анализ и оценка различных вариантов развития муниципалитета на основе имеющегося положительного опыта конкурентов;
- выбор конкретного пути совершенствования муниципального образования с целью улучшения соответствующих показателей.

Благодаря моделированию можно объективно оценить текущее состояние муниципального образования с целью удовлетворения потребностей его жителей, спрогнозировать использование имеющегося потенциала для достижения цели. Моделирование позволяет использовать инновации в совокупности с цифровыми технологиями при условии, что поступающая информация применяется в полном объеме, систематизированно, а технологии внедряются исходя из специфики деятельности конкретного города.

Метод рейтинговой оценки применительно к развитию «умных городов» подразумевает возможность объективно осуществлять оценку деятельности всех элементов «умного города», выявлять имеющиеся недостатки и находить варианты их устранения. Применение такого метода непосредственно направлено на повышение рейтинга соответствующего муниципалитета среди «умных городов». В связи с этим возможно привлечение экспертов и аналитиков для проведения подобных работ, что, к сожалению, может быть сложно реализуемо на местном уровне из-за ограниченности ресурсов. Поэтому речь может идти о работе таких специалистов на общественных началах.

Еще одним важным показателем эффективного внедрения концепции «умных городов», отвечающей требованиям будущего, является, на наш взгляд, их устойчивость, которая включает:

1. Текущее социально-экономическое развитие, определяемое дорожной картой сообщества для местного устойчивого развития и разумной политики, способствующей инвестиционным инициативам и интегрированным центрам для местного роста, со стратегической точки зрения.

2. Поддержку столпов развития, которые используют специфику, аутентичность и потенциал развития. Так, не все отрасли в достаточной степени применяют природный и антропогенный потенциал и повышают ценность существующего человеческого капитала и демографической поддержки как за счет увеличения местного населения, так и мобильности людей (внутренняя мобильность или иммигранты).

3. Поощрение иностранных инвестиций для завершения/диверсификации экономической и социальной деятельности, а также для сохранения и развития местной квалифицированной рабочей силы.

4. Надлежащее управление на местном уровне должно включать, по крайней мере, три компонента: цифровизацию; разумное развитие общественных служб, транспорта и связи, а также качество жизни.

5. Сеть здравоохранения, за которую отвечает местное сообщество, должна сосредоточиться на услугах для повышения качества жизни в мегаполисе и районах

регионального влияния, специализирующихся на риске зональных медицинских заболеваний, с целью содействия государственно-частному и муниципальному партнерству в сфере профилактических, лечебных и восстановительных медицинских услуг, с тем чтобы дополнять сеть служб здравоохранения, представляющих национальный или международный интерес.

6. Образовательная сеть призвана поддерживать высокое качество образования в областях специализации, требуемых местными и региональными рынками труда, чтобы удержать молодое поколение с помощью привлекательных рабочих мест в качестве альтернативы внешней миграции – будь то временная работа или постоянная. Университетское образование и услуги непрерывного образования должны обеспечивать интеграцию в национальную образовательную сеть в качестве центра передового опыта в области профессиональной подготовки или специализации. Сектор образования должен способствовать установлению связей между образовательными учреждениями и бизнесом посредством стипендий, стажировок и предварительной подготовки к трудоустройству и надлежащего управления структурным спросом на рынке труда.

Очевидно, что параллельно с функционированием муниципальных программ по формированию «умных городов» необходима реализация программ по энергосбережению и повышению энергетической эффективности, формированию современной городской среды²⁴.

К сожалению, идеальные решения в большинстве случаев сложно воплощаются в практику. Соответственно внедрение концепции «умного города» сопряжено с проблемами, возникающими при получении определенных результатов.

Если говорить о препятствиях, стоящих на пути развития «умных городов» в Российском государстве, сюда можно отнести (Абрамов, Андреев, 2022):

- дотационность большинства муниципальных образований (Шныренков, 2019);
- нехватку квалифицированных кадров на местах;
- пассивность местного населения и органов власти, нежелание внедрять инновации;
- существующий разрыв (неравенство) между крупными городами и небольшими муниципальными образованиями, не позволяющий последним использовать в полном объеме достижения научно-технического прогресса в силу отсутствия возможности непосредственного доступа к цифровым технологиям (Молчанова, 2019);
- недооценку комплексного подхода к реализации целей формирования «умных городов», отсутствие необходимой координации действий, изолированность используемых интеллектуальных систем (Malchenko, 2020);
- долгосрочность реализуемых проектов.

Выводы

«Умные города» подразумевают создание определенной индустрии в сфере информации и коммуникационных технологий, механизм взаимоотношений между властными структурами и населением, применение современных цифровых технологий в ежедневной городской жизни.

²⁴ Худжатов, М. Б. (2022). Муниципальные программы. СПС «КонсультантПлюс».

«Умный город» может порождать разнообразные частные инициативы и партнерства, но обычно он функционирует под эгидой муниципалитета. Городские власти являются главной движущей силой деятельности «умного города», при этом между ними и частными технологическими корпорациями существуют тесные отношения. Инновации «умного города» в конечном счете служат государственному управлению как надстройки для местного самоуправления: облегчают работу муниципальной администрации, предоставление государственных и муниципальных услуг и отношения между чиновниками и гражданами. Поэтому передовые формы непосредственного осуществления местного самоуправления (инициативные проекты, краудфандинг) могут стать подспорьем в развитии исследуемого феномена.

Таким образом, «умный город» выступает в роли некой экосистемы, определяющей как комфортные, так и безопасные условия для проживания людей. «Умный город» можно рассматривать как город, эффективно работающий в перспективных направлениях экономики, управления, транспортной мобильности, экологии, построенный на разумном сочетании регулирующих решений властей и деятельности активных и осведомленных о проблемах своего города граждан.

Тем самым основной целью реализации рассматриваемых идей является повышение качества жизни населения (достигается посредством обеспечения непрерывного взаимодействия местных властей и населения с вовлечением последнего в решение насущных проблем по месту жительства в режиме реального времени, максимального предоставления услуг населению) и качества управления городами (обеспечивается посредством внедрения передовых цифровых и инженерных решений, оптимизации использования имеющихся ресурсов).

Сегодня «умные города» предлагают заманчивые перспективы, стратегию и актуальный взгляд в будущее, оперативно отслеживают и интегрируют состояние своих важнейших систем инфраструктуры.

Проведя анализ базовых правовых актов, определяющих сущность концепции «умных городов», можно заключить, что большинство из них имеют подзаконный и разрозненный характер, включают основные критерии отнесения тех или иных территориальных образований к «умным городам». В связи с этим видится необходимым принятие в Российской Федерации единого федерального закона, устанавливающего комплексный подход и стандарты регулирования «умных городов» (закрепление ключевых понятий, целей и сфер развития, компетенции властных структур на всех уровнях).

Концепция проекта «умный город», на наш взгляд, является перспективным направлением совершенствования института местного самоуправления, способствующего претворению в жизнь таких его базовых принципов, как народовластие и независимость от иных властных структур. Также это может повысить уровень авторитета органов власти через открытость своей работы для граждан, что в настоящее время представляется необходимым для проведения исследований в области как конституционного, так и муниципального права.

Императив благополучия и улучшения качества жизни в контексте «умных городов» может быть достигнут только в том случае, если интеллектуальные услуги, занимающие столь важное место в концепции «умных городов», соответствуют потребностям, ожиданиям и навыкам жителей городов. Учитывая, что интернет вещей генерирует и открывает точки доступа в режиме реального времени к огромным объемам данных, относящихся к благосостоянию и качеству жизни, таким как

мнения граждан, а также к последним событиям, связанным с нормативно-правовой базой, дебатами, политическими решениями и разработкой не только федеральной, но и муниципальной политики, перспективными направлениями выступают: трансформация непосредственных форм осуществления местного самоуправления в электронный формат; использование потенциала, заложенного в этой системе для повышения эффективности управления, осуществляемого в «умных городах», в масштабах целого государства.

Список литературы

- Абрамов, В., Андреев, В. (2022). Проблемы и перспективы цифровой трансформации государственного и муниципального управления в регионе (на примере Кемеровской области). *Ars Administrandi (Искусство управления)*, 14(4), 667–700. EDN: <https://elibrary.ru/ctwmyg>. DOI: <https://doi.org/10.17072/2218-9173-2022-4-667-700>
- Антонова, А. В. (2020). Развитие методики оценки города по критериям «умного» города. *Вопросы управления*, 6(67), 122–141. EDN: <https://elibrary.ru/ugsecz>. DOI: <https://doi.org/10.22394/2304-3369-2020-6-122-141>
- Белов, В. И., Смирнов, И. И. (2018). Управление жизнедеятельностью городов посредством реализации концепции «Умный город». *Синергия Наук*, 24, 439–445. <https://elibrary.ru/usruiy>
- Ганин, О. Б., Ганин, И. О. (2014). «Умный город»: перспективы и тенденции развития. *Ars administrandi (Искусство управления)*, 1, 124–135.
- Голикова, Ю. Б. (2020). Экономика и управление инновациями в городах и регионах как основа формирования концепции будущего «Умный город». *Современные аспекты экономики*, 3-2(271), 18–27. <https://elibrary.ru/vovkmj>
- Есаян, А. К., Трунцевский, Ю. В. (2020). Общие подходы к нормативному правовому регулированию технологий в сфере «Умный город». *Международное публичное и частное право*, 1, 36–41. <https://doi.org/10.18572/1812-3910-2020-1-36-41>
- Камолов, С. Г., Глазьева, С. С., Тажиева, С. К. (2022). Умные города ЕАЭС как перспектива российского регионального технологического лидерства. *Российский экономический журнал*, 5, 64–82. EDN: <https://elibrary.ru/bdbkqd>. DOI: <https://doi.org/10.33983/0130-9757-2022-5-64-82>
- Костко, Н. А., Печеркина, И. Ф., Попкова, А. А. (2022). Модели реализации концепции «Умный город» в стратегиях социально-экономического развития крупных городов Российской Федерации. *Вопросы государственного и муниципального управления*, 4, 197–223. EDN: <https://elibrary.ru/uolfky>. DOI: <https://doi.org/10.17323/1999-5431-2022-0-4-197-223>
- Куранов, А. С. (2020). «Умный город» как «благополучный город». *Образование и наука в России и за рубежом*, 4(68), 191–194. <https://elibrary.ru/nzrlcj>
- Молчанова, В. И. (2019). От умного города к городу справедливому: проблемы устойчивого развития в условиях цифровой экономики. *Journal of Creative Economy*, 13(12), 2371–2386. EDN: <https://elibrary.ru/yeysk>. DOI: <https://doi.org/10.18334/ce.13.12.41379>
- Низамиева, Э. Р. (2021). Внедрение принципов умного города как драйвер к реорганизации и повышению эффективности существующих городов. *Вестник Томского государственного архитектурно-строительного университета*, 23(6), 19–27. EDN: <https://elibrary.ru/xcwmmwn>. DOI: <https://doi.org/10.31675/1607-1859-2021-23-6-19-27>
- Стрельникова, С. А., Цуциев, М. А. (2017). Пространственное развитие России: вопросы стратегии (интервью с П. А. Чистяковым, вице-президентом Центра экономики инфраструктуры). *Бюджет*, 2, 76–79.
- Шарова, А. А. (2019). Проект «Умный город» как комплексное решение повышения качества управления городами и уровня жизни в них. *Научный электронный журнал Меридиан*, 14(32), 3–5. <https://elibrary.ru/urppbj>
- Шкваря, Л. В., Семенов, А. (2020). Smart Cities: Necessity and Development Strategies. *Информация и Инновации*, 15(2), 52–58. EDN: <https://elibrary.ru/uzffyx>. DOI: <https://doi.org/10.31432/1994-2443-2020-15-2-52-58>
- Шныренков, Е. А. (2019). Экономические проблемы развития проекта «Умный город» в российских городах. *Экономика и предпринимательство*, 4(105), 304–307. <https://elibrary.ru/jwaqgd>
- Якушина, О. И. (2021). Организация социального пространства современных городов в свете концепций «открытого» и «умного» города. *Теория и практика общественного развития*, 4(158), 33–42. EDN: <https://elibrary.ru/kkughg>. DOI: <https://doi.org/10.24158/tipor.2021.4.5>

- Apostu, S., Vasile, V., Vasile, R., & Rosak-Szyrocka, J. (2022). Do Smart Cities Represent the Key to Urban Resilience? Rethinking Urban Resilience. *International Journal of Environmental Research and Public Health*, 19(22), 15410. <https://doi.org/10.3390/ijerph192215410>
- Attaran, H., Kheibari, N. A., & Bahrepour, D. (2022). Toward Integrated Smart City: a New Model for Implementation and Design Challenges. *GeoJournal*, 87(S4), 511–526. <https://doi.org/10.1007/s10708-021-10560-w>
- Bekbolat B. M., Mahatov N. B., & Damysbek B. D. (2021). The Convenience of Smart Technologies for Cities. *Молодой ученый*, 9(351), 36–38. <https://elibrary.ru/izvhbr>
- Caprotti, F., & Liu, D. (2020). Platform Urbanism and the Chinese Smart City: the Coproduction and Territorialisation of Hangzhou City Brain. *GeoJournal*, 87(3), 1559–1573. <https://doi.org/10.1007/s10708-020-10320-2>
- Csukás, M., & Szabó, R. Z. (2022). What are the conditions to become smart? *Informacios Tarsadalom*, 22(2), 9–26. <https://doi.org/10.22503/inftars.xxii.2022.2.1>
- European Economic and Social Committee. (2015). Opinion of the European Economic and Social Committee on «Smart cities as drivers for development of a new European industrial policy» (own-initiative opinion). *Official Journal of the European Union*, 58, 24–33.
- Fedorchenko, S. N., & Karlyavina, E. (2021). Smart City: the arrival of a New Democracy or Digital Totalitarianism? *Journal of Political Research*, 5(1), 3–22. EDN: <https://elibrary.ru/cpmywd>. DOI: <https://doi.org/10.12737/2587-6295-2021-5-1-3-22>
- Jothimani, P., Chenniappan, P., & Chidambaranathan, V. (2022). Factors Impinge on the Development of a Smart City: a Field Study. *Environmental Science and Pollution Research*, 29(57), 86298–86307. <https://doi.org/10.1007/s11356-021-17930-4>
- Langendahl, P. (2021). The Politics of Smart Farming Expectations in Urban Environments. *Frontiers in Sustainable Cities*, 3, 1–8. <https://doi.org/10.3389/frsc.2021.691951>
- Lee, J. P., & Nam, J. H. (2021). Analysis of Regional Characteristics and Deficiency Areas of Smart City Living Service : Focused on the Seoul. *Journal of Korea Planning Association*, 56(5), 30–43. <https://doi.org/10.17208/jkpa.2021.10.56.5.30>
- Malchenko, Yu. A. (2020). From Digital Divide to Consumer Adoption of Smart City Solutions: a Systematic Literature Review and Bibliometric Analysis. *Vestnik of Saint Petersburg University. Mathematics*, 3, 316–335. <https://elibrary.ru/txeveg>
- Moustaka, V., Maitis, A., Vakali, A., & Anthopoulos, L. (2021). Urban Data Dynamics: A Systematic Benchmarking Framework to Integrate Crowdsourcing and Smart Cities' Standardization. *Sustainability*, 13(15), 8553. <https://doi.org/10.3390/su13158553>
- Saragih, L. R., Dachyar, M., & Zagloel, T. Y. M. (2021). Business Process Reengineering at ICT Operations, In Managing Smart Cities as New Customers (Non-Human). *International Journal of Technology*, 12(2), 378-389. <https://doi.org/10.14716/ijtech.v12i2.4418>
- Treude, M., Schüle, R., & Haake, H. (2022). Smart Sustainable Cities—Case Study Südwestfalen Germany. *Sustainability*, 14(10), 5957. <https://doi.org/10.3390/su14105957>
- Vukovic N. A., Larionova V. A., & Morganti P. (2021). Smart Sustainable Cities: Smart Approaches and Analysis. *Экономика региона*, 17(3), 1004–1013. EDN: <https://elibrary.ru/yqyxyu>. DOI: <https://doi.org/10.17059/ekon.reg.2021-3-20>
- Xu, J., Song, R., & Zhu, H. (2022). Evaluation of Smart City Sustainable Development Prospects Based on Fuzzy Comprehensive Evaluation Method. *Computational Intelligence and Neuroscience*, 1–11. <https://doi.org/10.1155/2022/5744415>

Сведения об авторе



Тихалева Елена Юрьевна – кандидат юридических наук, доцент, доцент кафедры конституционного, административного и уголовного права, Среднерусский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

Адрес: 302028, Российская Федерация, г. Орел, ул. Октябрьская, 12

E-mail: columbijka@mail.ru

ORCID ID: <https://orcid.org/0000-0003-4612-4722>

Google Scholar ID: <https://scholar.google.com/citations?user=Rt1gtkoAAAAJ>

ПИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=852559

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.19.25 / Правовой режим информации, информационных систем и сетей

Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 9 сентября 2022 г.

Дата одобрения после рецензирования – 15 февраля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.35>

"Smart Cities": Legal Regulation and Potential of Development

Elena Yu. Tikhaleva

Middle Russia Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration
Orel, Russian Federation

Keywords

Digital platform,
digital technologies,
digitalization,
law,
legal regulation,
legislation,
local self-government,
municipal entity,
municipal law,
smart city

Abstract

Objective: to research the trends of development of the "smart cities" concept and their legal regulation.

Methods: general scientific (induction, deduction) and special (systemic-structural, comparative-legal analysis) methods were used. Also, review analysis was applied to analyze the status quo of "smart cities". Innovative research approaches are still rare in considering the "smart cities" concept, as well as the prospects referring to targeted knowledge management and cooperation between the respective stakeholders. As for the special research methods for studying digital relations, we used content analysis (the method of creating reproducible and substantiated conclusions from texts (or other meaningful materials) in the context of their use). As the results of previous research and concepts referring to "smart cities" are available, we also used deductive content analysis.

Results: a characteristic is given to public relations formed within the process of development of "smart cities" concept. The key legal acts, principles of formation and functioning of "smart cities" are identified, taking into account the Russian and foreign experience. In this connection, the examples of successful practices are given, of the activities of both Russian and foreign municipal entities, taking into account the competitions held and rankings determined by the central structures. The popular directions are summarized, which are broadly introduced at the local level, and the probable problems are identified in the sphere of implementation of this project in our state.

© Tikhaleva E. Yu., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: the article carries out an analysis of the current legal regulation and the results of introducing the “smart cities” concept. The promising technologies and methods are identified, which are necessary to achieve the tasks of the concept implementation. The elements are specified, which ensure sustainability of “smart cities” complying with the future demands. An author’s position is expressed regarding a close interrelation of this phenomenon with the institute of local self-government in the context of possible development of the latter into the process of making managerial decisions involving artificial intelligence. This concerns, first of all, using the potential of the Internet of Things. In practice, a lot of problems occur, associated with the implementation of normatively stipulated provisions, which implies the need to perform further research in the sphere under study.

Practical significance: is due to the insufficient development of data about the features and prospects of introducing the idea of “smart cities”. The provisions of the research performed will allow effectively improving the mechanisms of legal regulation and broad implementation of the concept under study.

For citation

Tikhaleva, E. Yu. (2023). “Smart Cities”: Legal Regulation and Potential of Development. *Journal of Digital Technologies and Law*, 1(3), 803–824. <https://doi.org/10.21202/jdtl.2023.35>

References

- Abramov, V., & Andreev, V. (2022). Problems and prospects of digital transformation of state and municipal governance in a region (the case of the Kemerovo region). *Ars Administrandi*, 14(4), 667–700. (In Russ.). <https://doi.org/10.17072/2218-9173-2022-4-667-700>
- Antonova, A. V. (2020). Development of the city assessment technique by the criteria of a “smart” city. *Management Issues*, 6(67), 122–141. (In Russ.). <https://doi.org/10.22394/2304-3369-2020-6-122-141>
- Apostu, S., Vasile, V., Vasile, R., & Rosak-Szyrocka, J. (2022). Do Smart Cities Represent the Key to Urban Resilience? Rethinking Urban Resilience. *International Journal of Environmental Research and Public Health*, 19(22), 15410. <https://doi.org/10.3390/ijerph192215410>
- Attaran, H., Kheibari, N. A., & Bahrepour, D. (2022). Toward Integrated Smart City: a New Model for Implementation and Design Challenges. *GeoJournal*, 87(S4), 511–526. <https://doi.org/10.1007/s10708-021-10560-w>
- Bekbolat B. M., Mahatov N. B., & Damysbek B. D. (2021). The Convenience of Smart Technologies for Cities. *Molodoy ucheniy*, 9(351), 36–38.
- Belov, V. I., & Smirnov, I. I. (2018). Managing cities’ life activity through implementation of the “Smart city” concept. *Sinergiya Nauk*, 24, 439–445. (In Russ.).
- Caprotti, F., & Liu, D. (2020). Platform Urbanism and the Chinese Smart City: the Coproduction and Territorialisation of Hangzhou City Brain. *GeoJournal*, 87(3), 1559–1573. <https://doi.org/10.1007/s10708-020-10320-2>
- Csukás, M., & Szabó, R. Z. (2022). What are the conditions to become smart? *Informacios Tarsadalom*, 22(2), 9–26. <https://doi.org/10.22503/inftars.xxii.2022.2.1>
- Esayan, A. K., & Truntsevskiy, Yu. V. (2020). Common approaches to the legal regulation of technologies in the smart city area. *Public International and Private International Law*, 1, 36–41. (In Russ.).
- European Economic and Social Committee. (2015). Opinion of the European Economic and Social Committee on “Smart cities as drivers for development of a new European industrial policy” (own-initiative opinion). *Official Journal of the European Union*, 58, 24–33.
- Fedorchenko, S. N., & Karlyavina, E. (2021). Smart City: the arrival of a New Democracy or Digital Totalitarianism? *Journal of Political Research*, 5(1), 3–22. <https://doi.org/10.12737/2587-6295-2021-5-1-3-22>

- Ganin, O., & Ganin, I. (2014). "Smart City": Development Prospects and Trends. *Ars Administrandi*, 1, 124–135. (In Russ.).
- Golikova, Yu. B. (2020). Economics and innovation management in cities and regions as a basis for forming the concept of the future "Smart city". *Sovremennye aspekty ekonomiki*, 3–2(271), 18–27. (In Russ.).
- Jothimani, P., Chenniappan, P., & Chidambaranathan, V. (2022). Factors Impinge on the Development of a Smart City: a Field Study. *Environmental Science and Pollution Research*, 29(57), 86298–86307. <https://doi.org/10.1007/s11356-021-17930-4>
- Kamolov, S., Glazyeva, S. S., & Tazhiyeva, S. K. (2020). Smart cities in Eurasian economic union: outlook for Russian regional technological leadership. *Russian Economic Journal*, 5, 64–82. (In Russ.). <https://doi.org/10.33983/0130-9757-2022-5-64-82>
- Kostko, N., Pecherkina, I., & Popkova, A. (2022). Implementation models for the "smart city" concept in the strategies for socio-economic development of large cities in the Russian Federation. *Public Administration Issues*, 4, 197–223. (In Russ.). <https://doi.org/10.17323/1999-5431-2022-0-4-197-223>
- Kuranov, A. S. (2020). "Smart city" as "safe city". *Obrazovaniye i nauka v Rossii i za rubezhom*, 4(68), 191–194. (In Russ.).
- Langendahl, P. (2021). The Politics of Smart Farming Expectations in Urban Environments. *Frontiers in Sustainable Cities*, 3, 1–8. <https://doi.org/10.3389/frsc.2021.691951>
- Lee, J. P., & Nam, J. H. (2021). Analysis of Regional Characteristics and Deficiency Areas of Smart City Living Service : Focused on the Seoul. *Journal of Korea Planning Association*, 56(5), 30–43. <https://doi.org/10.17208/jkpa.2021.10.56.5.30>
- Malchenko, Yu. A. (2020). From Digital Divide to Consumer Adoption of Smart City Solutions: a Systematic Literature Review and Bibliometric Analysis. *Vestnik of Saint Petersburg University. Mathematics*, 3, 316–335.
- Molchanova, V. A. (2019). From a smart city to a just city: problems of sustainable development under digital economy. *Kreativnaya ekonomika*, 13(12), 2371–2386. (In Russ.). <https://doi.org/10.18334/ce.13.12.41379>
- Moustaka, V., Maitis, A., Vakali, A., & Anthopoulos, L. (2021). Urban Data Dynamics: A Systematic Benchmarking Framework to Integrate Crowdsourcing and Smart Cities' Standardization. *Sustainability*, 13(15), 8553. <https://doi.org/10.3390/su13158553>
- Nizamieva, E. B. (2021). Smart city development as a driver of efficiency reorganization and improvement of cities. *Vestnik Tomskogo gosudarstvennogo arkhitekturno-stroitel'nogo universiteta. Journal of Construction and Architecture*, 23(6), 19–27. (In Russ.). <https://doi.org/10.31675/1607-1859-2021-23-6-19-27>
- Saragih, L. R., Dachyar, M., & Zagloel, T. Y. M. (2021). Business Process Reengineering at ICT Operations, In Managing Smart Cities as New Customers (Non-Human). *International Journal of Technology*, 12(2), 378–389. <https://doi.org/10.14716/ijtech.v12i2.4418>
- Sharova, A. A. (2019). "Smart city" project as a complex solution to improve the quality of managing cities and standard of living in them. *Meridian-journal*, 14(32), 3–5. (In Russ.).
- Shkvarya, L. V., & Semenov, A. S. (2020). Smart cities: necessity and development strategies. *Informatsiya i Innovatsii*, 15(2), 52–58. (In Russ.). <https://doi.org/10.31432/1994-2443-2020-15-2-52-58>
- Shnyrenkov, E. A. (2019). Economic problems of "Smart city" project development in Russian cities. *Ekonomika i predprinimatel'stvo*, 4(105), 304–307. (In Russ.).
- Strelnikova, S. A., & Tsutsiev, M. A. (2017). Spatial development of Russia: issues of strategy (interview with P. A. Chistyakov, Vice President of the Center for infrastructure economics). *Byudzheth*, 2, 76–79. (In Russ.).
- Treude, M., Schüle, R., & Haake, H. (2022). Smart Sustainable Cities – Case Study Südwestfalen Germany. *Sustainability*, 14(10), 5957. <https://doi.org/10.3390/su14105957>
- Vukovic N. A., Larionova V. A., & Morganti P. (2021). Smart Sustainable Cities: Smart Approaches and Analysis. *Ekonomika regiona*, 17(3), 1004–1013. <https://doi.org/10.17059/ekon.reg.2021-3-20>
- Xu, J., Song, R., & Zhu, H. (2022). Evaluation of Smart City Sustainable Development Prospects Based on Fuzzy Comprehensive Evaluation Method. *Computational Intelligence and Neuroscience*, 2022, 1–11. <https://doi.org/10.1155/2022/5744415>
- Yakushina, O. I. (2021). Organizing public space in the contemporary city within "open" and "smart" city framework. *Theory and Practice of Social Development*, 4 (158), 33–42. (In Russ.). <https://doi.org/10.24158/tpor.2021.4.5>

Author information



Elena Yu. Tikhaleva – Candidate of Juridical Sciences, Associate Professor, Department of Constitutional, Administrative and Criminal Law, Middle Russia Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration

Address: 12 Oktyabrskaya Str., 302028 Orel, Russian Federation

E-mail: columbijka@mail.ru

ORCID ID: <https://orcid.org/0000-0003-4612-4722>

Google Scholar ID: <https://scholar.google.com/citations?user=Rt1gtkoAAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=852559

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – September 9, 2023

Date of approval – February 15, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023



Научная статья

УДК 34:342.721:004:004.8

EDN: <https://elibrary.ru/drgddj>

DOI: <https://doi.org/10.21202/jdtl.2023.36>

Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования

Дана Утеген ✉

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Бауржан Жанатович Рахметов

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Ключевые слова

Безопасность,
биометрическая
аутентификация,
биометрические данные,
идентификация,
неприкосновенность
частной жизни,
персональные данные,
право,
правовое регулирование,
технологии распознавания
лиц,
цифровые технологии

Аннотация

Цель: выявление моделей правового регулирования в сфере биометрической идентификации и аутентификации технологией распознавания физических лиц для выработки рекомендаций по повышению информационной безопасности человека и государственно-правовой охраны его права на неприкосновенность частной жизни.

Методы: рискориентированный подход в праве и такие специально-юридические методы познания, как методы сравнительно-правового анализа и юридического прогнозирования, имеют для исследуемой проблематики определяющее значение и позволяют сопоставить применяемые в зарубежных странах и их объединениях модели правового регулирования в сфере биометрической идентификации и аутентификации системами распознавания физических лиц, спрогнозировать возможные риски для безопасности биометрических данных с учетом перспективы дальнейшего распространения современной технологии распознавания лиц, сформулировать рекомендации по правовой охране биометрических данных.

✉ Контактное лицо

© Утеген Д., Рахметов Б. Ж., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Результаты: предложены пути дальнейшего совершенствования законодательства Республики Казахстан и иных стран, находящихся в процессе развития правового регулирования биометрических данных, в части определения допустимых критериев использования технологии распознавания лиц, разработки категоризации биометрических систем с высоким и низким уровнем риска (по примеру опыта регулирования искусственного интеллекта в Европейском союзе), необходимости введения системы запретов массовой и неизбирательной слежки за человеком с помощью систем видеонаблюдения и др.

Научная новизна: заключается в выявлении положительного зарубежного передового опыта по развитию правового регулирования в сфере распознавания физических лиц на основе биометрии (Европейский союз, Соединенные Штаты Америки, Соединенное Королевство Великобритании, Северная Ирландия), который может быть использован для дальнейшего совершенствования национального законодательства в целях создания наиболее эффективных механизмов правовой защиты персональных данных, включая биометрическую информацию.

Практическая значимость: основанное на рискориентированном подходе и компаративистском анализе исследование позволяет выработать меры по усилению правовой охраны биометрических данных, обеспечению эффективной защиты гражданских прав и свобод на неприкосновенность частной жизни на основе прогноза дальнейшего распространения современной технологии распознавания лиц.

Для цитирования

Утеген, Д., Рахметов, Б. Ж. (2023). Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования. *Journal of Digital Technologies and Law*, 1(3), 825–844. <https://doi.org/10.21202/jdtl.2023.36>

Содержание

Введение

1. Соединенные Штаты Америки: внедрение и регулирование технологии распознавания лиц
2. Европейский союз: рискориентированный подход в правовом регулировании
3. Республика Казахстан: на пути к регулированию биометрических данных

Выводы

Список литературы

Введение

Большинство развитых государств вкладывают значительные финансовые средства для использования технологии распознавания лиц. Это технология, которая сравнивает и анализирует два или более изображений лиц, идентифицирует их при помощи биометрических данных и определяет, кому принадлежат данные на основе

имеющихся баз¹ (Gill, 1997). Биометрические данные, используемые для распознавания лица, хранятся в системе биометрической аутентификации (Sarabdeen, 2022). Система биометрической аутентификации – это информационная система, позволяющая идентифицировать человека на основе некоторых его основных физиологических и поведенческих характеристик². К примерам биометрических признаков можно отнести отпечатки пальцев, лицо, радужную оболочку, отпечаток ладони, сетчатку, геометрию руки, голос, подпись и походку³. В ее основе содержатся аппаратные системы сбора данных, интегрирующие программные компоненты, позволяющие с помощью математических алгоритмов выполнять анализ данных и идентифицировать личность человека⁴.

Рассматривая различные группы правовых отношений в правоприменительной и правоохранительной деятельности органов исполнительной власти, выбранных в данной работе для сравнительного анализа государств, в реализации которых применимы технологии распознавания лиц, следует выделить следующие объекты, отнесенные к уязвимым:

- 1) категория объекта, уязвимого в террористическом отношении;
- 2) особо важные государственные объекты;
- 3) стратегические объекты отраслей экономики, имеющих стратегическое значение;
- 4) опасные производственные объекты;
- 5) объекты массового скопления людей и др.

Наиболее часто технология распознавания лиц используется правоохранительными органами для идентификации подозреваемых в совершении преступлений лиц. Анализ и идентификация происходят путем получения фото, видеоизображений, водительских прав, видеозаписи с камер общественного наблюдения, изображения из социальных сетей и др.⁵ Несмотря на то, что системы распознавания лиц применяются, в частности, для охраны правопорядка и обеспечения общественной безопасности, зачастую граждане находятся под наблюдением, даже не подозревая об этом, потому как уведомление о наблюдении отсутствует. Использование системы распознавания лиц силовыми структурами было отмечено критическими замечаниями и высказываниями о предвзятости, дискриминации и отсутствии прозрачности данных систем.

Международное сообщество в целом поддерживает инициативу по обеспечению безопасности при помощи цифровых технологий. Согласно Резолюции Совета Безопасности Организации Объединенных Наций (далее – ООН), государства-члены призывают активно предпринимать действия по противодействию угрозе терроризма

¹ Все про технологию распознавания лиц. *Www.cloudav.ru*. <https://www.cloudav.ru/mediacenter/technology/facial-recognition-technology/>; TAdviser – портал выбора технологий и поставщиков. (2020). *TAdviser.ru*. <https://www.tadviser.ru/index.php/>

² QUII. (2018). Biometric Recognition: definition, challenge and opportunities of biometric recognition systems. *IQUII*. <https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209>

³ Jain, A. (2008). Biometric authentication. *Scholarpedia*, 3(6), 3716. <https://doi.org/10.4249/scholarpedia.3716>

⁴ Там же, 2.

⁵ Резолюции Совета Безопасности ООН/RES/2396(2017). <https://www.un.org/securitycouncil/ru/content/sres23962017>

и мер в области предупреждения преступности⁶. В связи с участвовавшей практикой, связанной с мошенничеством, фальсификацией и подделкой документов, удостоверяющих личность, рекомендации органа ООН, отвечающего за обеспечение международного мира и безопасности, государствам касались внедрения систем биометрической идентификации данных в целях наблюдения за террористами или лицами, подозреваемыми в террористической деятельности⁷.

Помимо целей обеспечения безопасности, следует также отметить влияние пандемии COVID-19, поспособствовавшей ускорению применения систем распознавания лиц в борьбе с распространением инфекции и контроля за перемещением граждан в период карантинных ограничений. Алгоритмы систем распознавания лиц применялись для контроля за перемещением граждан, ношением масок, измерения температуры тела в целях управления мерами обеспечения общественного здравоохранения (Chen & Wang, 2023; Johnson et al., 2022; Shore, 2022).

В этой связи представляет интерес опыт правового регулирования стран, которые на данном этапе активно применяют систему биометрических баз данных, нацеленную на упрощение процедур уголовного расследования и контроля за перемещением на границах.

1. Соединенные Штаты Америки: внедрение и регулирование технологии распознавания лиц

На примере Соединенных Штатов Америки стоит сразу отметить практику использования камер с функцией распознавания лиц в контексте контртеррористических мер после событий 11 сентября 2001 г. На основании принятого Конгрессом США Закона о защите государственных границ были внедрены биометрические удостоверения личности⁸. С 2004 г. в стране была введена система снятия отпечатков пальцев и включения в базу изображения лиц, прибывающих в Америку. Проверка биометрических данных лиц по государственным базам данных направлена на выявление подозреваемых в терроризме лиц, разыскиваемых преступников или нарушивших ранее иммиграционное законодательство США. Таким образом, меньше чем за полгода была собрана биометрическая база данных более пяти миллионов человек. Кроме того, органы безопасности США приняли меры в отношении 3800 иностранцев на основании информации, полученной в ходе процесса биометрического скрининга при посещении США⁹. Меры были связаны с задержанием подозреваемых лиц на основании ордера об аресте, отказе в приеме на границе либо возвращении в страну последнего пребывания.

⁶ Там же.

⁷ Резолюция 2396 (2017), принятая Советом Безопасности на его 8148-м заседании 21 декабря 2017 года. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/27/PDF/N1746027.pdf?OpenElement>

⁸ Markey, E. J. (2021, June 15). Text: S.2052 – 117th Congress (2021–2022): Facial Recognition and Biometric Technology Moratorium Act of 2021. <https://www.congress.gov/bill/117th-congress/senate-bill/2052/text>

⁹ Federal Register, Vol. 73, Iss. 245. (2008, December 19). <https://www.govinfo.gov/content/pkg/FR-2008-12-19/html/E8-30095.htm>

Однако трагические события, связанные с террористическим актом 2001 г., не повлияли на возникновение, а лишь способствовали развитию уже существовавшей ранее системы идентификации по отпечаткам пальцев.

В США и других развитых странах в 1960–1970-х гг. системы распознавания лиц и анализа выражения лица начали разрабатываться в исследовательских лабораториях, финансируемых Министерством обороны и разведывательными службами. В 1990 г. были созданы новые компании для коммерциализации технологии, которые искали рынки сбыта, в особенности среди учреждений, использующих собственные компьютерные сети, таких как финансовая индустрия, бизнес, крупномасштабные системы идентификации, паспортные службы, государственные департаменты, правоохранительные и пенитенциарные системы (Schweber, 2014). В 1999 г. Федеральное бюро расследований США разработало и внедрило автоматизированные системы идентификации отпечатков пальцев. Данная система объединяет записи отпечатков пальцев, собранных федеральными правоохранительными органами. Она предоставляет возможности автоматизированного поиска отпечатков пальцев, электронного хранения изображений и электронного обмена отпечатками пальцев. В 2008 г. данная система обрабатывала в среднем более 63 000 отпечатков пальцев в день, 91 % из которых сканируются в систему в цифровом виде, остальная часть может храниться на бумажном носителе¹⁰.

За последние годы в практике США накопилось достаточное количество дел, связанных с рассмотрением процессов обработки, хранения и использования биометрических данных (Stepney, 2019). В этой связи наиболее важным представляются изучение и анализ отдельных решений для формирования данной категории проблемных вопросов с целью совершенствования законодательства Республики Казахстан.

В 2021 г. в США было рассмотрено дело Роберта Уильямса, чернокожего мужчины, который был арестован в 2020 г. за кражу часов из магазина в городе Детройт (штат Мичиган). Несмотря на то, что он не посещал данный магазин уже несколько лет, его задержали в присутствии двух его дочерей по подозрению в краже имущества. В случае Уильямса департамент полиции Детройта использовал технологию распознавания лиц, чтобы идентифицировать подозреваемого по изображению с камер наблюдения. Таким образом, была применена база данных изображений водительских прав департамента полиции штата Мичиган. Однако при идентификации произошла погрешность в идентификации лица, повлиявшая на последствия в виде задержания под стражей невиновного лица в течение 30 часов¹¹.

К сожалению, данный случай не является единственным – практика привлечения невиновных лиц участилась (Bowyer, 2004). В связи с применением технологии распознавания лиц было проведено исследование Национального института стандартов и технологий США¹². Данное исследование выявило, что при идентификации

¹⁰ FIRS IAFIS (Federal Bureau of Investigation). <https://www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-information-privacy-act/departments-of-justice-fbi-privacy-impact-assessments/firs-iafis>

¹¹ Harwell, D. (2021, April 13). Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match. *Washington Post*. <https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/>

¹² NIST (National Institute of Standards and Technology) (2000). <https://www.nist.gov/>

лица чаще всего происходит дискриминация по цвету кожи. Также технология распознавания лиц обширно применялась правоохранительными органами для идентификации лиц при проведении митингов и демонстраций, расследования мелких правонарушений и ареста людей без каких-либо доказательств вины (Buresh, 2021). В результате постоянно возрастает количество людей, которые стали жертвами нерегулируемой системы наблюдения и мониторинга¹³.

В итоге после ряда последствий обнаружения погрешностей при идентификации лиц гражданским обществом США и международными неправительственными организациями были сформированы петиции с призывом к массовому запрету технологий биометрического распознавания, обеспечивающих массовое и дискриминационное наблюдение¹⁴. В некоторых штатах США был инициирован Мораторий по запрету применения технологии распознавания лиц. В последующем в США был предложен к принятию законопроект о распознавании лиц, ограничивающий применение данной технологии и ее неэтичного использования¹⁵. В данном документе содержится перечень ограничений по части применения технологии распознавания лиц. К таким ограничениям отнесены:

- иммиграционный контроль,
- мирные протесты,
- установление личности подозреваемого в совершении преступления.

Согласно законопроекту, правоохранительным органам выставлено требование по осуществлению тестирования системы распознавания лиц и предоставлению ежегодных отчетов об эффективности практики их применения. Одним из важных критериев является удаление из баз данных изображений несовершеннолетних лиц, оправданных или освобожденных без предъявления обвинений¹⁶.

Несмотря на то, что большинство штатов инициировало внедрение и регулирование технологии распознавания лиц, следует отметить опыт штата Калифорния, который стал первым штатом в США, запретившим использование технологии распознавания лиц правоохранительными органами. В последующем практика Калифорнии повлияла на введение запрета на использование технологии распознавания лиц не только для правоохранительных органов, но и для частных организаций¹⁷.

¹³ Rauen Zahn, B., Chung, J., & Kaufman, A. (2021, March 20). Facing Bias in Facial Recognition Technology. *The Regulatory Review*. <https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/#:~:text=According%20to%20the%20researchers%2C%20facial>

¹⁴ The Computer Got It Wrong: Why We're Taking the Detroit Police to Court over a Faulty Face Recognition "Match". (2021, April 13). *American Civil Liberties Union*. <https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match>

¹⁵ Paul, K. (2019, May 15). San Francisco Is First US City to Ban Police Use of Facial Recognition Tech. *The Guardian*. <https://www.theguardian.com/us-news/2019/may/14/san-francisco-facial-recognition-police-ban>

¹⁶ Ban Biometric Surveillance. Access Now. <https://www.accessnow.org/ban-biometric-surveillance/>

¹⁷ California Law Enforcement Prohibited from Using Facial Recognition Technology in Body Cameras under Ting Bill Signed by the Governor. Assemblymember Phil Ting Representing the 19th California Assembly District. <https://a19.asmdc.org/press-releases/20191008-california-law-enforcement-prohibited-using-facial-recognition-technology>

На примере Калифорнии по применению ограничительных мер использования технологии распознавания лиц правоохранительными органами были включены основания по части предоставления ордера на обыск и требование по приведению достаточных доказательств совершения преступления. Кроме того, ограничительные меры правоохранительных органов касались использования технологии распознавания лиц во время протестов и митингов для идентификации участников в целях недопущения нарушений гражданских свобод и прав человека. Данный законопроект получил широкую поддержку со стороны международных неправительственных организаций по контролю за деятельностью правительства, групп по защите гражданских свобод, а также самих же представителей правоохранительных органов¹⁸. Особой поддержкой со стороны крупных компаний, таких как IBM, Amazon и Microsoft, стало решение о приостановлении продажи инструментов распознавания лиц правительствам¹⁹.

В результате принятый закон о распознавании лиц запрещает, чтобы совпадение было единственным доказательством, устанавливающим достаточные основания для ареста, как наиболее адекватная мера защиты, предотвращающая ошибки в постановлении о привлечении к ответственности (Gates, 2002).

Также в штате Иллинойс был принят закон о регулировании систем распознавания лиц, к примеру Закон о приватности биометрической информации Иллинойса²⁰ (Zuo et al., 2019). В данном законе прописаны положения о запрете на обмен, передачу без согласия, торговлю или извлечение финансовой выгоды от продажи биометрических данных²¹ (Hill et al., 2022).

На основании проведенного анализа в различных штатах США следует отметить некоторую фрагментарность подходов. Так как не все штаты ограничили применение камер с функцией распознавания лиц, большинство штатов приняли законы, регулирующие ограничение применения таких камер правоохранительными органами²². Не все граждане и иностранные граждане, проживающие на территории США, могут рассчитывать на безопасность в случаях погрешности при идентификации. Данный законопроект лишь обеспечивает базовую защиту для американцев, позволяя гражданскому обществу продвигать инициативы по ограничению бесконтрольного применения данных систем.

По мнению авторов законопроекта, сформированный подход по ограничению применения функции распознавания лиц и регулированию сбора и обработки данных

¹⁸ В США ограничат использование полицией систем распознавания лиц. (2022, September 30). ForkLog. <https://forklog.com/news/v-ssha-ogranichat-ispolzovanie-politsiej-sistem-raspoznavaniya-lits>

¹⁹ Муравьев, Д. (2020, June 19). Почему IT-компании отказались от технологии распознавания лиц и при чем тут протесты в Америке. *Теплица социальных технологий*. <https://te-st.ru/2020/06/19/why-it-companies-against-facial-recognition/>

²⁰ 740 ILCS 14/ Biometric Information Privacy Act. *Www.ilga.gov*. www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

²¹ Приближается крайний срок подачи иска в многомиллионном урегулировании процесса со Snapchat. (2022, October 13). *Chicago24online*. <https://chicago24online.com/news/prilizhaetsya-krajnij-srok-podachi-iska-v-mnogomillionnom-uregulirovanii-processa-so-snapchat/> ; Thornley v. Clearview AI, Inc., No. 20-3249 (7th Cir. 2021). *Justia Law*. <https://law.justia.com/cases/federal/appellate-courts/ca7/20-3249/20-3249-2021-01-14.html>

²² Face Off: Law Enforcement Use of Face Recognition Technology. (2018, February 23). *Electronic Frontier Foundation*. <https://www EFF.org/wp/law-enforcement-use-face-recognition>

позволит снизить вероятность злоупотребления мониторингом в дискриминационном характере, а также обеспечит меры по защите неприкосновенности частной жизни²³.

Тем самым следует сделать вывод, что технологии распознавания лиц и наблюдения допускают погрешности, способствуют дискриминации, в особенности в тех случаях, когда правоохранительные органы продолжают принимать решения об аресте и задержании лиц без дополнительных способов расследования преступлений (Givens et al., 2004). В случае принятия ограничительных мер система распознавания лиц будет использоваться лишь в необходимых и оправданных целях, а также ограничит широкие дискреционные полномочия правоохранительных органов (Nissenbaum, 2004). К тому же усилит право на возможность удаления информации о себе в случае оправдательного приговора. Инициатива законодателей по ограничению системы распознавания лиц также обусловлена защитой неприкосновенности частной жизни, недопущения предвзятости и дискриминации граждан по цвету кожи и расовой принадлежности.

2. Европейский союз: рискориентированный подход в правовом регулировании

Рассматривая практику Европейского союза (далее – ЕС), следует обратить внимание на принятие законодательства, ограничивающего использование систем распознавания лиц в реальном времени. Кроме злоупотреблений со стороны правоохранительных органов в части задержания ряда граждан без явных на то оснований, выяснилось, что инструменты применения искусственного интеллекта и систем распознавания лиц могут быть использованы для слежки за мигрантами, религиозными группами или представителями меньшинств²⁴. Выработанная позиция представителей европейского парламента ассоциирует методы слежки с опасностью для неприкосновенности частной жизни и гражданских свобод, а также способствующей проявлению предвзятости и дискриминационных технологий.

Предпосылками к принятию ограничительных мер стала обширная практика использования полицией технологии автоматического распознавания лиц для поиска людей в общественных местах. Технологии распознавания лиц, установленные на уличных камерах в целях обеспечения общественной безопасности, вызывали возмущения со стороны активистов, гражданского общества, которые в свою очередь требовали отчет о реальных фактах предотвращения преступлений при помощи установления наблюдения (Кутейников и др., 2022). В высказанных протестах правозащитным сообществом подчеркивались свобода слова и право на мирные собрания, которые являются важнейшими гражданскими свободами. Подчеркнуто, что использование правительством системы распознавания лиц препятствует выражению мнения, наносит ущерб целым сообществам и нарушает индивидуальные свободы²⁵.

²³ Turner, N. L., & Chin, C. (2022, April 7). Police Surveillance and Facial Recognition: Why Data Privacy Is an Imperative for Communities of Color. *Brookings*. <https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>

²⁴ Обзор решений ЕСПЧ за сентябрь 2018 года (2018, 14 сентября). Помощь для желающих обратиться в Европейский суд по правам человека в Страсбурге. <https://european-court-help.ru/obzor-reshenii-espch-za-sentiabr-2018-goda/> ; Face off Report. (2018). *Big Brother Watch*. bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/

²⁵ Guariglia, Paige Collings, & Matthew. (2022, September 26). Ban Government Use of Face Recognition in the UK. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk>

Примечательным делом, рассмотренным высоким судом в Кардиффе, был иск Эда Бриджеса при поддержке правозащитной организации Liberty. Бриджес заявил, что использование полицией технологии распознавания лиц во время его похода в магазин, а затем на мирной акции протеста против торговли оружием нарушает его право на неприкосновенность частной жизни и участие в мирных собраниях.

В постановлении высокого суда в Кардиффе было отмечено, что, несмотря на то, что система массового наблюдения нарушает права на частную жизнь тех, кого сканируют камеры наблюдения, судьи пришли к выводу, что, автоматизированное распознавание лиц несет в себе законные основания²⁶ (Бегишев, Хисамова, 2018).

В 2022 г. законодательные инициативы в Соединенном Королевстве Великобритании и Северной Ирландии (далее – Великобритания) об ограничении систем распознавания лиц были пересмотрены²⁷. Согласно Акту о защите данных Великобритании от 2018 г., обозначено, что биометрические и медицинские данные являются чувствительными данными, соответственно, сбор или обработка этих данных должны осуществляться только после получения явного согласия²⁸. Управление комиссара по информации Великобритании также выступило с уведомлением о проведении расследования в отношении тех организаций, которые внедряют системы распознавания лиц, несущих риск использования алгоритма анализа эмоций.

Технологии анализа эмоций обрабатывают такие данные, как отслеживание взгляда, анализ настроения, движения лица, анализ походки, сердцебиение, выражение лица²⁹ (Бегишев, Хисамова, 2018).

Анализ эмоций предполагает сбор, хранение и обработку целого ряда персональных данных, включая подсознательные поведенческие или эмоциональные реакции. Такое использование данных гораздо более рискованно, чем традиционные биометрические технологии, которые используются для идентификации лица (Sprokkereef, 2007).

Возникшие проблемы применения систем идентификации повлияли на проведение тщательного анализа правового регулирования биометрических систем аутентификации в Европейском союзе. В апреле 2021 г. Европейский орган по надзору за защитой данных, проанализировав текущие риски и опасения по части применения систем с функцией распознавания лиц, призвал запретить использование искусственного интеллекта для автоматического определения лиц в общественных местах. Аналогичным образом, в январе 2021 г. Совет Европы призвал к строгому регулированию технологий и отметил в своем новом руководстве, что технологии распознавания лиц должны быть запрещены, если они используются исключительно

²⁶ Bowcott, O. (2019, September 4). Police Use of Facial Recognition Is Legal, Cardiff High Court Rules. *The Guardian*. <https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules>

²⁷ Каминский, Б. (2022, 27 июля). В Британии потребовали запретить распознавание лиц в магазинах. *ForkLog*. <https://forklog.com/news/v-britanii-potrebovali-zapretit-raspoznavanie-lits-v-magazinah>

²⁸ Data Protection Act. "Data Protection Act 2018. (2018). *Legislation.gov.uk*. <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

²⁹ "Immature Biometric Technologies Could Be Discriminating against People" says ICO in Warning to Organisations. (2022, October 27). *Ico.org.uk*. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations/>

для определения цвета кожи, религиозных или иных убеждений, пола, расового или этнического происхождения, возраста, состояния здоровья или социального статуса человека. Группы гражданских свобод также призвали ЕС запретить биометрическое наблюдение на основании несоответствия правам человека³⁰.

Европейская комиссия включила в Закон ЕС об искусственном интеллекте ограничения использования системы распознавания лиц в общественных местах и для частных компаний, тем не менее оставила возможность применения в исключительных целях для правоохранительных органов. Органы обеспечения безопасности могут использовать эту технологию в таких случаях, как поиск пропавших детей, предотвращение террористических атак или обнаружение вооруженных и опасных преступников.

Законопроект ЕС об искусственном интеллекте, представленный в апреле 2021 г., направлен на ограничение использования биометрических систем идентификации, включая технологию распознавания лиц. В рамках проекта предлагается ввести новые требования, регулирующие применение технологии в зависимости от критериев – «высокого риска» или «низкого риска»³¹.

К системам высокого риска искусственного интеллекта будут отнесены:

- критически важные объекты, которые могут подвергнуть риску жизнь и здоровье граждан;
- биометрическая идентификация и категоризация физических лиц;
- образование и профессиональная подготовка (например, подсчет баллов на экзаменах);
- компоненты безопасности продукции (например, применение искусственного интеллекта в роботизированной хирургии);
- трудоустройство, управление персоналом и доступ к самозанятости (например, программное обеспечение для сортировки резюме при приеме на работу);
- доступ к основным частным и государственным услугам и льготам (система кредитования по баллам, ограничивающая граждан в возможности получить кредит);
- данные правоохранительных органов;
- данные миграционных и пограничных служб (проверка подлинности проездных документов);
- данные институтов отправления правосудия и демократических процессов (применение закона к конкретному набору доказательств)³².

Системы высокого риска будут запрещены для использования без цели или должны будут соответствовать строгим правилам надзорных органов, также применяться в серьезных случаях обеспечения безопасности. Широкий спектр технологий распознавания лиц, используемых в правоохранительных целях, при пограничном контроле, в общественных местах, образовательных учреждениях, общественном транспорте, может быть разрешен только при условии оценки соответствия и соблюдения требований безопасности (Sprökkereef, 2007). Технологии

³⁰ Там же, 20.

³¹ Каспарянц, Д. (2021, 7 октября). Стандартизация искусственного интеллекта в ЕС. Научно-технический центр ФГУП "ГРЧЦ". <https://rdc.grfc.ru/2021/10/ai-standards/>

³² Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. (2021, April 21). European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

распознавания лиц, используемые по категории низкого риска, будут ограничены критериями прозрачности и требований к правилам хранения и обработки информации³³.

Вне зависимости от представленных проектов регулирования искусственного интеллекта в Европе до сих пор существуют серьезные опасения касательно применения такого рода категоризации и регулирования без надлежащего общественного контроля. Большинство из государств – участников ЕС все же выступают за более строгие правила, включая полный запрет на использование таких технологий. В частности, система удаленной биометрической идентификации и технология распознавания лиц отнесены к системам высокого риска (Firc, 2023). Одним из главных требований обозначен четкий запрет на применение в общественных местах в правоохранных целях.

3. Республика Казахстан: на пути к регулированию биометрических данных

В Республике Казахстане отмечается тенденция к применению опыта зарубежных стран по биометрической аутентификации в различных сферах, таких как государственные, банковские, медицинские, правоохранные, образовательные и др.

В действующее законодательство о защите персональных данных был внесен ряд поправок³⁴, включено определение биометрических данных, утверждены правила процессов обработки и хранения биометрических данных при оказании государственных услуг. В положениях данных правил указаны процессы обработки биометрических данных при оказании государственных услуг, сбор которых осуществляется на добровольной основе, и собранная информация может быть в любой момент удалена из базы данных по письменному заявлению субъекта данных³⁵.

В соответствии с Законом «О персональных данных и их защите», понятие биометрических данных определено в качестве категории персональных данных, которые характеризуют физиологические и биологические особенности субъекта, на основе которых можно установить его личность³⁶.

Понятие определяет принадлежность биометрических данных к персональным данным, а процесс идентификации биометрических данных квалифицируется как «биометрическая аутентификация». Согласно Закону об информатизации,

³³ Филипова, И. А. (2022). *Правовое регулирование искусственного интеллекта: учебное пособие* (2-е изд., обновл. и доп.). Нижний Новгород: Нижегородский госуниверситет. https://www.researchgate.net/publication/359194516_Legal_Regulation_of_Artificial_Intelligence/citation/download; Madiaga, T., & Mildebrath, H. (2021, September). *In-Depth Analysis*. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)

³⁴ О персональных данных и их защите. ИПС «Әділет». <https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm>

³⁵ Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг. ИПС «Әділет». <https://adilet.zan.kz/rus/docs/V2000021547#z14>

³⁶ Там же, 22.

биометрическая аутентификация определена как комплекс мер, идентифицирующих личность на основании физиологических и биологических неизменных признаков³⁷.

Кроме указанных определений, в Республике Казахстан принят Закон о дактилоскопической и геномной регистрации. Цели закона обусловлены требованиями по обязательному сбору отпечатков пальцев для создания единой базы биометрических данных. База отпечатков данных будет применяться при пограничном контроле, мерам по противодействию терроризму, раскрытию уголовных преступлений, обеспечению правопорядка и безопасности³⁸.

По части процессов обработки данных также в 2022 г. была разработана Программа развития национальной платежной системы в Республике Казахстан до 2025 г.³⁹ В данной программе предусмотрено введение биометрической аутентификации при платежных операциях, в рамках инициативы ее реализации указано, что она нацелена на повышение обеспечения безопасности персональных данных за счет внедрения механизма получения цифрового согласия со стороны субъектов на обработку данных. В результате субъект должен видеть процедуру своего обращения за получением государственной услуги, цели обращения и с возможностью предоставления или отзыва согласия на доступ к его данным⁴⁰.

Кроме процедур повсеместного применения биометрических данных, в Программе развития Алматы до 2025 и 2030 гг. заявлено об установке камер видеонаблюдения с функцией распознавания лиц⁴¹. На 2027 г. запланировано расширение систем видеонаблюдения путем установки камер на всех уязвимых в террористическом плане объектах и во дворах многоквартирных жилых комплексов⁴². Актуальность установки камер наблюдения возросла после массовых беспорядков, произошедших в январе 2022 г., когда в нескольких крупных городах Республики Казахстан, в особенности в Алматы, правоохранительные органы и безопасности не могли контролировать массовые беспорядки, мародерство и нарушения общественного порядка⁴³.

Инициативы по установке видеокамер с функцией распознавания лиц определены законопроектом о регулировании цифровых технологий, согласно которому были

³⁷ Закон Республики Казахстан № 418-V от 24 ноября 2015 г. «Об информатизации» (с изменениями и дополнениями по состоянию на 03.09.2022). Информационная система ПАРАГРАФ. https://online.zakon.kz/document/?doc_id=33885902

³⁸ Раисова, З. (2021, 6 января). Обязательная дактилоскопия казахстанцев: зачем она нужна и как это работает? CABAR.asia. <https://cabar.asia/ru/zachem-vvoditsya-obyazatel'naya-daktiloskopiya-kazahstantsev>

³⁹ Об утверждении Национального плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан: Указ Президента Республики Казахстан № 636 от 15 февраля 2018 г. ИПС «Әділет». <https://adilet.zan.kz/rus/docs/U1800000636>

⁴⁰ Об утверждении Программы создания Национальной платформы цифровой биометрической идентификации на 2021–2024 годы (2021). Открытые НПА. <https://legalacts.egov.kz/npa/view?id=13895562>

⁴¹ Программа развития Алматы до 2030 г. социально ориентирована. (2022, 28 июня). <https://www.gov.kz/memleket/entities/almaty/press/news/details/394216?lang=ru>

⁴² Алхабаев, Ш. (2022, 12 сентября). Систему распознавания лиц внедрят в Алматы. Tengrinews.kz. https://tengrinews.kz/kazakhstan_news/sistemu-raspoznavaniya-lits-vnedryat-v-almaty-477602

⁴³ Казахстан: жертвы январских протестов не находят правосудия. (2022, May 9). Human Rights Watch. <https://www.hrw.org/ru/news/2022/05/09/kazakhstan-no-justice-january-protest-victims>

внесены поправки и изменения в действующий Закон об информатизации⁴⁴. В целях обеспечения национальной безопасности и общественного правопорядка планируется внедрение национальной системы видеомониторинга как совокупности программных и технических средств, осуществляющих сбор, обработку и хранение базы видеоизображений⁴⁵.

Между тем проанализированные документы и нормативные правовые акты, касающиеся защиты персональных данных в Республике Казахстан, на данный момент лишь частично соответствуют международным стандартам защиты прав человека. Кроме того, наличие законов не дает весомую гарантию их защиты. Отдельного внимания требуют правила сбора, обработки, хранения биометрических данных⁴⁶.

Применение камер с функцией распознавания лиц и сбор отпечатков пальцев граждан может допустить вмешательство в частную жизнь. Поэтому при правовом регулировании биометрических данных следует тщательно изучить международный опыт государств, которые уже реализуют практику сбора биометрических данных, во избежание рисков, связанных с утечкой персональных данных (Raissova & Mukhamejanova, 2021).

В работе правоохранительных органов, в процессе обработки биометрических данных рекомендуется придерживаться предложенных способов применения технологий распознавания лиц в правоприменительной и правоохранительной деятельности, исключающих или существенно снижающих возможность нарушения неприкосновенности частной жизни, прав и свобод человека:

Применение системы распознавания лиц должно быть соответствующим законной цели и оправданно необходимым.

Применение системы распознавания лиц должно иметь открытый и транспарентный характер, что включает отчетность перед гражданами в виде статистических данных, представление материалов о раскрытии преступлений при помощи технологии распознавания лиц.

Возможность для обращения в уполномоченные органы при наличии жалоб и обращений, а также получения интересующей информации.

Наличие четких правил, политики и процедур сохранности биометрических данных и процессов их обработки.

Соблюдение правил по минимизации сбора биометрических данных.

Ограничение доступа третьих лиц, не имеющих отношения к процессу обработки и наблюдения.

Соответствие требованиям законов и мерам безопасности для защиты от несанкционированного доступа и использования биометрических данных.

На регулярной основе проведение плановых и внеплановых проверок для обеспечения качества защиты биометрических данных и исключения от неправомерного использования, и предоставления доступа к ним.

⁴⁴ О проекте Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий»: Постановление Правительства Республики Казахстан № 1001 от 28.12.2019. ИПС «Әділет». <https://adilet.zan.kz/rus/docs/P1900001001>

⁴⁵ Об утверждении Правил функционирования Национальной системы видеомониторинга. ИПС «Әділет». <https://adilet.zan.kz/rus/docs/V2000021693>

⁴⁶ Исследование возможных экономических, социальных и правовых последствий закона РК «О дактилоскопической и геномной регистрации». (2021, June 23). Soros Kazakhstan Foundation. www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/

Выводы

В данном исследовании рассмотрен опыт применения технологий распознавания лиц и биометрической идентификации в качестве инструмента обеспечения безопасности. При помощи описания ограничений со стороны государств сформированы подходы к правовому регулированию рассматриваемой сферы, преимуществ и рисков их применения.

В целях недопущения любых нарушений неприкосновенности частной жизни, дискриминации, ограничений прав и свобод со стороны правительства или частных организаций необходимо на основе проанализированного опыта государств, реализовавших национальные проекты по регулированию биометрических данных, выявить гарантии и повышение степени государственно-правовой защиты. Анализ опыта государств продемонстрировал, что принятие соответствующих законов, регулирующих защиту биометрических данных, неизбежно, поскольку действующее законодательство недостаточно отвечает критериям безопасного использования технологии распознавания лиц правительственными и частными организациями.

По итогам проведенного анализа и изученного опыта зарубежных стран следует выделить следующие важные предложения для дальнейшего совершенствования законодательства в Республике Казахстан:

- дополнить действующее законодательство в части определения допустимых критериев использования технологии распознавания лиц;
- внести запрет массовой и избирательной слежки за человеком с помощью систем видеонаблюдения;
- запретить использование изображений граждан Республики Казахстан, взятых из общедоступных источников в целях пополнения баз биометрических данных;
- разработать категоризацию биометрических систем с высоким и низким уровнями риска на примере опыта регулирования искусственного интеллекта в Европейском союзе;
- установить запрет на использование системы биометрической идентификации в реальном времени любыми пользователями, кроме правоохранительных органов.

На основе изученного опыта ЕС и США указанные рекомендации могут быть приняты во внимание как в Республике Казахстан, так и в других государствах, находящихся на пути процесса развития и правового регулирования биометрических данных. При применении систем распознавания лиц на практике государственным органам следует способствовать соблюдению принципов прозрачности, законности и необходимости, а также сформировать политику обработки данных третьих лиц.

Список литературы

- Бегишев, И. Р., Хисамова, З. И. (2018). Криминологические риски применения искусственного интеллекта. *Всероссийский криминологический журнал*, 12(6), 767–775. [https://doi.org/10.17150/2500-4255.2018.12\(6\).767-775](https://doi.org/10.17150/2500-4255.2018.12(6).767-775)
- Кутейников, Д. Л., Ижаев, О. А., Зенин, С. С. (2022). Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности. *Lex Russica*, 75(2), 121–131. <https://doi.org/10.17803/1729-5920.2022.183.2.121-131>
- Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, 23(1), 9–19. <https://doi.org/10.1109/mtas.2004.1273467>

- Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?. *Santa Clara High Technology Law Journal*, 38(1). <https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2>
- Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, 47(2), 102482. <https://doi.org/10.1016/j.telpol.2022.102482>
- Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, 9(4), e15090. <https://doi.org/10.1016/j.heliyon.2023.e15090>
- Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, 3(2), 235–238. <https://doi.org/10.1177/152747640200300217>
- Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, 14(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161
- Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. <https://doi.org/10.1109/cvpr.2004.1315189>
- Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, 24(3), 325–335. <https://doi.org/10.1177/14613557221089558>
- Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, 39(4), 101753. <https://doi.org/10.1016/j.giq.2022.101753>
- Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, 22(4), 777. <https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6>
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 119. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>
- Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, 2(3), 140–150. <https://doi.org/10.48165/sajssh.2021.2309>
- Ring T. (2016). Privacy in peril: is facial recognition going too far too fast?, *Biometric Technology Today*, 7–8, 7–11. [https://doi.org/10.1016/S0969-4765\(16\)30123-0](https://doi.org/10.1016/S0969-4765(16)30123-0)
- Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3), e09086. <https://doi.org/10.1016/j.heliyon.2022.e09086>
- Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, 39(1), 242–274. <https://doi.org/10.1111/lsi.12062>
- Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, 70, 101815. <https://doi.org/10.1016/j.tele.2022.101815>
- Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19
- Stepney, Ch. (2019). Actual Harm Means it is too Late: How *Rosenbach v. Six Flags* Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, 40(1). <https://digitalcommons.lmu.edu/elr/vol40/iss1/2>
- Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, 143(6), 1298e–1306e. <https://doi.org/10.1097/prs.0000000000005673>

Сведения об авторах



Утеген Дана – заместитель директора, старший преподаватель Высшей школы права, Университет КАЗГЮУ имени М. С. Нарикбаева

Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8

E-mail: d_utegen@kazguu.kz

ORCID ID: <https://orcid.org/0000-0001-5296-7916>



Рахметов Бауржан Жанатович – PhD в области политики и международных отношений, ассистент-профессор Международной школы экономики, Университет КАЗГЮУ имени М. С. Нарикбаева

Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8

E-mail: b_rakhmetov@kazguu.kz

ORCID ID: <https://orcid.org/0000-0003-3948-9977>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/32537389>

Google Scholar ID: <https://scholar.google.com/citations?user=hanfRwoAAAAJ>

Вклад авторов

Д. Утеген осуществляла составление черновика рукописи и его критический пересмотр с внесением ценных замечаний интеллектуального содержания; разработку дизайна методологии; проведение сравнительного анализа; сбор литературы; анализ законодательства Соединенных Штатов Америки и Республики Казахстан; подготовку и редактирование текста статьи; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.

Б. Ж. Рахметов осуществлял формулирование идеи, исследовательских целей и задач; участие в научном дизайне; анализ и обобщение литературы; анализ законодательства Европейского союза и Республики Казахстан; интерпретацию частных результатов исследования; критический пересмотр и редактирование текста рукописи; интерпретацию общих результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Б. Ж. Рахметов является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.19.61 Правовое регулирование информационной безопасности

Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 7 ноября 2022 г.

Дата одобрения после рецензирования – 23 апреля 2023 г.

Дата принятия к опубликованию – 15 августа 2023 г.

Дата онлайн-размещения – 20 августа 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.36>

Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models

Dana Utegen ✉

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Baurzhan Zh. Rakhmetov

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Keywords

Biometric authentication,
biometric data,
digital technologies,
facial recognition,
technologies,
identification,
law,
legal regulation,
personal data,
privacy,
security

Abstract

Objective: to specify the models of legal regulation in the sphere of biometric identification and authentication with facial recognition technology in order to elaborate recommendations for increasing information security of persons and state-legal protection of their right to privacy.

Methods: risk-oriented approach in law and specific legal methods of cognition, such as comparative-legal analysis and juridical forecasting, are significant for the studied topic and allow comparing the legal regulation models used in foreign countries and their unions in the sphere of biometric identification and authentication with facial recognition systems, forecasting the possible risks for the security of biometric data, taking into account the prospects of further dissemination of the modern facial recognition technology, and to shape recommendations on legal protection of biometric data.

✉ Corresponding author

© Utegen D., Rakhmetov B. Zh., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Results: the ways are proposed to further improve legislation of the Republic of Kazakhstan and other countries currently developing the legal regulation of biometric data, regarding the admissible criteria for using the facial recognition technology, the elaboration of categorization of biometric systems with a high and low risk levels (by the example of the experience of artificial intelligence regulation in the European Union), and the necessity to introduce a system of prohibitions of mass and unselective surveillance of humans with video surveillance systems, etc.

Scientific novelty: consists in identifying a positive advanced foreign experience of developing legal regulation in the sphere of facial recognition based on biometry (European Union, the United States of America, the United Kingdom of Great Britain and Northern Ireland), which can be used for further improvement of the national legislation in order to create more effective mechanisms of legal protection of personal data, including biometric information.

Practical significance: based on risk-oriented approach and comparative analysis, the research allows elaborating measures for enhancing the legal protection of biometric data and ensuring effective protection of civil rights and freedoms by forecasting further expansion of the modern facial recognition technology.

For citation

Utegen, D., Rakhmetov, B. (2023). Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. *Journal of Digital Technologies and Law*, 1(3), 825–844. <https://doi.org/10.21202/jdtl.2023.36>

References

- Begishev, I. R., & Khisamova, Z. I. (2018). Criminological risks of using artificial intelligence. *Russian Journal of Criminology*, 12(6), 767–775. (In Russ.). [https://doi.org/10.17150/2500-4255.2018.12\(6\).767-775](https://doi.org/10.17150/2500-4255.2018.12(6).767-775)
- Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, 23(1), 9–19. <https://doi.org/10.1109/mtas.2004.1273467>
- Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws? *Santa Clara High Technology Law Journal*, 38(1). <https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2>
- Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, 47(2), 102482. <https://doi.org/10.1016/j.telpol.2022.102482>
- Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, 9(4), e15090. <https://doi.org/10.1016/j.heliyon.2023.e15090>
- Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, 3(2), 235–238. <https://doi.org/10.1177/152747640200300217>
- Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, 14(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

- Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. <https://doi.org/10.1109/cvpr.2004.1315189>
- Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, 24(3), 325–335. <https://doi.org/10.1177/14613557221089558>
- Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, 39(4), 101753. <https://doi.org/10.1016/j.giq.2022.101753>
- Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, 22(4), 777. <https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6>
- Kuteynikov, D. L., Izhaev, O. A., Lebedev, V. A., & Zenin, S. S. (2022). Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex Russica*, 75(2), 121–131. (In Russ.). <https://doi.org/10.17803/1729-5920.2022.183.2.121-131>
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 119. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>
- Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, 2(3), 140–150. <https://doi.org/10.48165/sajssh.2021.2309>
- Ring T. (2016) Privacy in peril: is facial recognition going too far too fast?, *Biometric Technology Today*, 7–8, 7–11. [https://doi.org/10.1016/S0969-4765\(16\)30123-0](https://doi.org/10.1016/S0969-4765(16)30123-0)
- Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3), e09086. <https://doi.org/10.1016/j.heliyon.2022.e09086>
- Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, 39(1), 242–274. <https://doi.org/10.1111/lsi.12062>
- Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, 70, 101815. <https://doi.org/10.1016/j.tele.2022.101815>
- Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19
- Stepney, Ch. (2019). Actual Harm Means it is too Late: How *Rosenbach v. Six Flags* Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, 40(1). <https://digitalcommons.lmu.edu/elr/vol40/iss1/2>
- Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, 143(6), 1298e–1306e. <https://doi.org/10.1097/prs.0000000000005673>

Authors information



Dana Utegen – Deputy Director, Senior Lecturer of KAZGUU Law School, KAZGUU University Astana

Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan

E-mail: d_utegen@kazguu.kz

ORCID ID: <https://orcid.org/0000-0001-5296-7916>



Baurzhan Zh. Rakhmetov – PhD in Politics and International Relations, Assistant Professor of International School of Economics, KAZGUU University Astana

Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan

E-mail: b_rakhmetov@kazguu.kz

ORCID ID: <https://orcid.org/0000-0003-3948-9977>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/32537389>

Google Scholar ID: <https://scholar.google.com/citations?user=hanfRwoAAAAJ>

Authors' contributions

Dana Utegen made the manuscript draft and critically reviewed it, inserting valuable comments of intellectual content; developed the methodology design; performed comparative analysis; collected literature; analyzed legislation of the United States of America and the Republic of Kazakhstan; prepared and edited the manuscript; formulated the key conclusions, proposals and recommendations; formatted the manuscript.

Baurzhan Zh. Rakhmetov formulated the research idea, goals and tasks; participated in research design; analyzed and summarized literature; analyzed legislation of the European Union and the Republic of Kazakhstan; interpreted the specific research results; critically reviewed and edited the manuscript; interpreted the general research results; approved the final version of the article.

Conflict of interest

Rakhmetov B. Zh. is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

ASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – November 7, 2023

Date of approval – April 23, 2023

Date of acceptance – August 15, 2023

Date of online placement – August 20, 2023

