



ISSN 2949-2483

Volume

1

Number

1

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 – Загретдинова 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, д. 42

Телефон: +7 (843) 231-92-90

Факс: +7 (843) 292-61-59

E-mail: lawjournal@ieml.ru

Сайт: <https://lawjournal.digital>

Телеграм: <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, д. 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, 2023.

Международный стандартный номер сериальных изданий: eISSN 2949-2483.

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 принятия – 20 февраля 2023 г. Дата онлайн-размещения на сайте <https://lawjournal.digital> – 28 февраля 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 – кандидат юридических наук, доцент, доцент кафедры предпринимательского права Уральского государственного юридического университета имени В. Ф. Яковлева (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, заведующий кафедрой информационного права и цифровых технологий Саратовской государственной юридической академии (Саратов, 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)

Харитоновая Юлия 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)

Гозстоный Гергели – 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 Тьяша – доктор наук, доцент кафедры гражданского, международного частного и сравнительного права Мариборского университета (Марибор, Республика Словения)

- Иоаннис Револидис** – доктор наук, преподаватель кафедры медиа права 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)
- Попович Душан** – доктор наук, профессор кафедры гражданского права Белградского университета, президент Сербского института разрешения споров о доменных именах (Белград, Республика Сербия)
- Прауди Юди** – доктор наук, профессор кафедры компьютерных наук и электроники Университета Гаджа Мада (Булакшумур, 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

Филипова И. А.

Создание метавселенной: последствия для экономики, социума и права..... **7**

Галлезе-Нобиле К.

Регулирование умных роботов и искусственного интеллекта в Европейском союзе **33**

Громова Е. А., Петренко С. А.

Квантовое право: начало **62**

Гуляева П. С.

Медицинские нанороботы в фокусе права..... **89**

Мурадян С. В.

Цифровые активы: правовое регулирование и оценка рисков **123**

Бурдова В. Д.

Правовая природа воспроизведения музейных предметов в цифровой форме NFT..... **152**

Рицу С., Мелипатаки Г., Мате Д. А.

Концепция труда: от традиционных социально-трудовых представлений к современным эффектам цифровой трансформации **175**

Василевский А. В.

Правовое регулирование отношений в сфере краудфандинга в Республике Беларусь **191**

Райеджиан А. М.

Цифровые тренды криминологии и уголовного правосудия XXI века **235**

Антонова Е. Ю.

Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию **251**

Дмитриева А. А., Пастухов П. С.

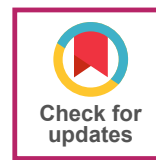
Концепция электронного доказательства в уголовном судопроизводстве..... **270**

Талапина Э. В., Жарова А. К.

Илларию Лаврентьевну Бачило – основоположника информационного права в России..... **296**



Научная статья
УДК 34:004:330.1:338
EDN: <https://elibrary.ru/lccojj>
DOI: <https://doi.org/10.21202/jdtl.2023.1>



Создание метавселенной: последствия для экономики, социума и права

Ирина Анатольевна Филипова 

Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского
г. Нижний Новгород, Российская Федерация

Ключевые слова

Виртуальная реальность, дополненная реальность, искусственный интеллект, киберпространство, метавселенная, нейроправа, права человека, право, цифровая платформа, цифровой аватар

Аннотация

Цель: определение степени влияния такого развивающегося технологического направления, как метавселенные, на различные сферы общества и выявление потребностей в реагировании со стороны права.

Методы: основным методом, используемым при проведении исследования, является системно-структурный метод, позволяющий установить связи между разными элементами общества как сложной системы, проанализировать закономерности, порождаемые распространением влияния прототипов метавселенных в одной сфере на другие. В качестве дополнительных применяются формально-логические, сравнительно-правовой, а также методы правового моделирования и прогнозирования.

Результаты: реализация концепции метавселенной на практике открывает новые возможности для людей, но будет сопровождаться серьезными изменениями в экономической подсистеме общества, в частности многократным ростом доли виртуальной экономики и структурными сдвигами в занятости. Изменения коснутся и социальной подсистемы: трансформируются социальные связи, модели обучения, появятся новые потребности личности. Перемены в экономической и социальной сферах повлекут необходимость адаптировать к ним право в целях сохранения эффективности правового регулирования общественных отношений. Необходимо учитывать и то, что метавселенная увеличит возможности не только людей, но и искусственного интеллекта, для которого виртуальная среда является практически «естественной». Нормы права должны обеспечить защиту человека в условиях увеличения виртуальной составляющей в жизни людей, сопряженной с интеллектуализацией среды.

Научная новизна: системно проанализированы изменения, происходящие в различных сферах современного общества в связи с развитием технологического направления метавселенных, выделены основные вопросы, возникающие из-за этого развития и требующие

© Филипова И. 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.

правовых решений как на уровне конституции, так и на уровне отраслевого законодательства, предложены необходимые изменения в правовом регулировании.

Практическая значимость: материалы исследования могут быть использованы в работе по подготовке предложений о внесении изменений и дополнений в действующее законодательство, а также в педагогической деятельности, в частности, при реализации учебных курсов или модулей, связанных с правом, в условиях цифровой трансформации общества.

Для цитирования

Филипова, И. А. (2023). Создание метавселенной: последствия для экономики, социума и права. *Journal of Digital Technologies and Law*, 1(1), 7–32. <https://doi.org/10.21202/jdtl.2023.1>

Содержание

Введение

1. Изменения в экономике

2. Влияние на социум

3. Потребность в конституционализации новых прав

4. Вопросы отраслевого регулирования

Выводы

Список литературы

Введение

В 2021 г. термин «метавселенная» получил широкую известность: если ранее его употребляли в основном разработчики компьютерных игр и философы, интересовавшиеся космологией, то после объявления о работе над созданием прототипов цифровых вселенных таких IT-гигантов, как Meta*, Google, Microsoft, Amazon, Nvidia, метавселенные стали технологическим трендом, к обсуждению которого подключаются все больше экономистов, социологов и правоведов из разных стран.

Метавселенная (параллельная цифровая вселенная) – виртуальный мир будущего, который будет существовать наряду с физическим миром, «населенный» цифровыми аватарами реальных людей. Пока существующие виртуальные миры фрагментарны, независимы и не связаны между собой, взаимодействуя лишь по необходимости¹. С появлением метавселенной повседневная жизнь людей

¹ Примерами виртуальных миров – интерактивной виртуальной 3D-среды – сегодня являются в первую очередь многопользовательские онлайн-игры, в которые одновременно могут играть сотни тысяч человек, создав личные аватары, способные участвовать в деятельности данного виртуального мира и общающиеся друг с другом (World of Warcraft, Star Wars: The Old Republic и т. д.).

перетечет в виртуальную среду. Предполагаемые сроки создания такой метавселенной – от пяти лет² до нескольких десятилетий³.

Метавселенная должна стать следующим поколением глобальной сети (Web 3.0), постоянно действующим виртуальным пространством, в котором люди смогут работать, общаться и отдыхать. Насколько это реально? Концепция метавселенной тесно связана с цифровыми технологиями: виртуальной и дополненной реальностью (VR/AR-технологиями), искусственным интеллектом, беспроводной связью, технологиями распределенного реестра (блокчейн) и т. д., их развитие делает создание «полноценной» метавселенной в пределах ближайших двух десятилетий весьма вероятным.

Это станет результатом эволюции Интернета. По словам главного аналитика компании Garthner⁴ Т. Нгуена, «переход к зрелой метавселенной будет аналогичен предыдущим технологическим сдвигам, таким как промышленная революция или эра мобильных устройств, в том смысле, что эта эволюция приведет к появлению нового набора технологических лидеров, потенциально вытеснив некоторых из предыдущей эпохи»⁵. Мир находится на первом (начальном) этапе формирования метавселенной, который продлится минимум до 2024 г., после чего начнется второй этап – «продвинутая» метавселенная, передовые решения для которой будут характеризоваться технологической конвергенцией, появлением новых технологий в целях удобной навигации по физическому и цифровому пространству, развитием технологий распознавания и картирования людей, мест, вещей и процессов (ориентировочно 2024–2027 гг.), переход к третьему этапу – «зрелой» метавселенной – может начаться после 2028 г. В итоге сформируется сеть взаимосвязанных виртуальных миров, где люди взаимодействуют с цифровым контентом и друг с другом, образуя экосистему, соединяющую цифровой и физический миры за счет комбинации дополненной и виртуальной реальностей, перехода от 2D-версии Интернета (с двухмерной компьютерной графикой) к общему 3D-пространству, Интернет в котором характеризуется интероперабельностью⁶ и синхронностью.

Созданию метавселенной будет сопутствовать целый ряд изменений во всех сферах жизнедеятельности общества: изменится экономическая система, преобразуются социальные связи, трансформируется право. Рассмотрим основные изменения.

² Newton, C. (2021, July 22). Mark in The Metaverse. Facebook's CEO on why the social network is becoming 'a metaverse company'. <https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview>

³ Ball, M. (2021, June 29). Framework for the Metaverse. 'The Metaverse Primer'. <https://www.matthewball.vc/all/forwardtothemetaverseprimer>

⁴ Одна из крупнейших в мире исследовательских и консалтинговых компаний, специализирующихся на рынке информационных технологий.

⁵ Nguyen, T. (2022, May 11). Here's how the metaverse will evolve. <https://www.techrepublic.com/article/heres-how-the-metaverse-will-evolve/>

⁶ Интероперабельность – это функциональная совместимость, способность взаимодействовать с другими системами без ограничения доступа.

1. Изменения в экономике

Еще в 2011 г. исследователь У. Брайан Артур из Стэнфорда указывал, что повседневные процессы в экономике уже тесно переплетены с цифровым миром: «В данный миг цифровая экономика не производит ничего осязаемого, но помогает архитекторам проектировать здания, отслеживает продажи, выполняет торговые и банковские операции, контролирует производственное оборудование, выставляет счета клиентам»⁷. Доля «невидимой» цифровой экономики с каждым годом растет. На современном этапе цифровой трансформации экономики – «Индустрии 4.0» – продолжается роботизация производства, происходит персонализация контента на основе анализа больших данных, совершенствуются технологии цифровых двойников (виртуальных моделей), что позволяет широко применять их в различных областях производства (Lv et al., 2022).

Создание метавселенной соответствует следующему этапу цифровой трансформации экономики – «Индустрии 5.0». Распространение интернета вещей влечет рост числа «умных» экосистем, отличающихся высокой степенью автоматизации, совершенствуются ИИ-ассистенты – программные агенты с элементами искусственного интеллекта, способные выполнять интеллектуальные задачи для пользователя. Появление метавселенной расширит область деятельности людей, позволит устранить пространственные, временные и ресурсные ограничения, налагаемые природой, и приведет к появлению новых продуктов, услуг, бизнес-моделей, новых профессий и форм занятости. «Метавселенная как глобальный тренд экономики может поспособствовать превращению хаоса цифровизации будущего в систему взаимодействия, стать платформой для экономических субъектов и успешным стратегическим проектом» (Алабина и др., 2022).

По мнению главы технологической компании Nvidia Дж. Хуанга, экономика виртуального мира в пределах десятилетия сможет превзойти экономику реального мира, тем самым экономика метавселенной превысит по размеру глобальный ВВП⁸. С ним не согласны специалисты международной консалтинговой компании Analysis Group, которые считают, что если метавселенная будет развиваться аналогично мобильным технологиям, то через 10 лет ее вклад в мировой ВВП составит всего 2,8 %. В то же время они отмечают, что преимуществом метавселенной является создание новых рынков, поэтому «форма и очертания метавселенной будут материализовываться сначала медленно, и только после того, как будет достигнута критическая масса, ее полный потенциал начнет приобретать более конкретные очертания»⁹. Аналитики одного из крупнейших банков – Citibank (Citi Global Insights) – прогнозируют

⁷ Brian Arthur, W. (2011, October 1). *The Second Economy*. <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-second-economy>

⁸ Kindig, B. (2022, February 18). *Nvidia on How the Metaverse Can Overtake the Current Economy*. <https://www.forbes.com/sites/bethkindig/2022/02/18/nvidia-on-how-the-metaverse-can-overtake-the-current-economy/?sh=5c3301a23614>

⁹ Christensen, L., Robinson, A. (2022, May 16). *The potential global economic impact of the metaverse*. <https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf>

высокие темпы роста и оценивают общий доступный рынок для экономики метавселенной примерно в 13 трлн долл. к 2030 г.¹⁰

С ростом доли виртуальной экономики метавселенная будет разрастаться, производственные и торговые корпорации уже «занимают места» в создаваемых прототипах метавселенных. Первыми «включившимися» отраслями стали индустрии развлечений, моды и криптовалюты. К примеру, дома моды Gucci, Ralph Lauren, Louis Vuitton, Paco Rabanne, Valentino и Burberry выпустили коллекции цифровой одежды. Все чаще проводятся эксперименты с рекламой: известные бренды используют видеоигры, технологии дополненной реальности, привлекая потребителей на цифровые платформы, приобщая к виртуальной среде все больше людей. Заявки на патенты, поданные Meta*, свидетельствуют о том, что реклама и спонсируемый контент станут важной частью стратегии развития метавселенной¹¹. Это повышает интерес к невзаимозаменяемым токенам (NFT) – цифровым сертификатам на основе блокчейна, подтверждающим право на владение виртуальным активом. Дома моды, аукционы и спортивные клубы уже продают NFT¹², что способствует формированию метавселенной, поощряя развитие цифровых торговых площадок.

Рынок меняется: множество офлайн-игроков активно развивают свои цифровые экосистемы и намерены создавать «супераппы» – приложения с расширенным набором функций. Цель, преследуемая лидерами направления, – создание виртуальной среды, в которой пользователь для решения своих задач захочет или будет вынужден оставаться постоянно.

Крупные работодатели, особенно высокотехнологичные компании, например Lenovo¹³, интересуются «подключением» к метавселенной. Количество заинтересованных компаний будет увеличиваться, ведь к настоящему моменту практически любая отрасль экономики переориентировала себя на мобильные рабочие процессы, поэтому тенденция охватывает не только высокотехнологичные, но и традиционные компании, в частности, McDonald's, Nike уже заявили о намерении адаптироваться к условиям метавселенной¹⁴.

В недалеком будущем многим людям, скорее всего, придется проводить большую часть времени в виртуальной реальности, делая покупки в виртуальных торговых центрах, общаясь на виртуальных форумах и выполняя онлайн-задания по работе. Эти действия люди будут производить с помощью цифровых аватаров – своих виртуальных воплощений, отражающих образ конкретного человека и его индивидуальные особенности. Пока гаджеты для попадания в виртуальную среду стоят достаточно дорого, далеко не каждый может их себе позволить, но когда-то так было

¹⁰ Metaverse and Money. Decrypting the Future (2022, March). Citi GPS. <https://ir.citi.com/gps/x5%2BFQJT3BoHXVu9MsqVRoMdiws3RhL4yhF6Fr8us8oHaOe1W9smOy1%2B8aaAgT3SPuQVtwC5B2%2Fc%3D>

¹¹ Murphy, H. (2022, January 18). Facebook patents reveal how it intends to cash in on metaverse. <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647>

¹² Frank, A. (2022, June 21). Bella Hadid Arrives in the Metaverse with a New Line of NFTs. <https://www.vogue.com/article/bella-hadid-nft-metaverse-interview>

¹³ Lenovo Story Hub (2022, January 13). Enterprise Metaverse: Employees Are Ready, Can Organizations Deliver? [Press Release]. <https://news.lenovo.com/pressroom/press-releases/enterprise-metaverse-employees-ready-organizations-deliver/>

¹⁴ Kilzi, M. (2022, May 20). The New Virtual Economy of The Metaverse. <https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/20/the-new-virtual-economy-of-the-metaverse/?sh=78850cc546d8>

и с персональными компьютерами, смартфонами. По мере дальнейшего развития технологий стоимость продуктов на их основе снизится, и со временем приобретение VR/AR-устройств превратится в обыденность.

Метавселенная станет единой цифровой платформой, используемой для труда, образования, лечения, отдыха, т. е. для человеческого существования в целом. Сейчас экономика метавселенной находится в стадии строительства, крупные компании начали «виртуальный» захват пространства. Инновации, сопутствующие созданию метавселенной, скажутся и на реальной экономике, влияя на ее инфраструктуру и менеджмент. С развитием метавселенной становятся возможными экономия ресурсов и уменьшение объема отходов за счет сокращения физического потребления.

В сфере труда метавселенная расширит возможности платформ цифрового труда, которые уже активно функционируют. Возрастание доли платформенной занятости признается в докладе Международной организации труда «Перспективы занятости и социальной защиты в мире: роль платформ цифрового труда в трансформации сферы труда»¹⁵, опубликованном в 2021 г. Согласно докладу, с 2010 по 2020 г. число цифровых трудовых платформ увеличилось как минимум пятикратно, а мониторинг спроса и предложения рабочей силы на них свидетельствует о постоянном росте спроса и предложения. Современная платформенная экономика – это набросок экономики в метавселенной будущего¹⁶. Применительно к трудовым отношениям это означает, что:

- метавселенная станет «рабочим местом» для многих работников, включая всех, кто сегодня работает удаленно;
- работодатели приобретут удаленный доступ к рабочей силе потенциальных работников по всему миру, что позволит передавать все больше работы на аутсорсинг;
- алгоритмическое наблюдение, под которым нередко уже находятся удаленные работники, распространится еще шире;
- будет расти число людей, выполняющих работу по «обслуживанию» метавселенной.

Следствием изменений на рынке труда станет трансформация занятости населения, что вкупе с изменениями в отраслевой экономике и менеджменте, происходящими из-за увеличения доли виртуальной экономики, будет способствовать смене социального ландшафта.

Не стоит забывать и про маркетинговую политику. Для понимания путей развития метавселенной очень важно осознавать, что ее построение, как и построение любой цифровой платформы, не является благотворительностью, в основе лежит коммерческая заинтересованность: бизнес-модель основана на получении прибыли. Так как пользователи платформ, как правило, против платной подписки за доступ к цифровым сервисам, то свободный доступ открывается в обмен на рекламу. В этой модели изначально многое построено на отслеживании и профилировании поведения и интересов пользователей, т. е. пользователи – продукт, который покупается и продается, а не клиент, оплачивающий счета. Это заставляет «полагаться на определенный уровень государственного регулирования, чтобы предотвратить

¹⁵ *Перспективы занятости и социальной защиты в мире: роль платформ цифрового труда в трансформации сферы труда.* (2021). Группа технической поддержки по вопросам достойного труда и Бюро МОТ для стран Восточной Европы и Центральной Азии. Москва: МОТ.

¹⁶ De Stefano, V., Aloisi, A., Countouris, N. (2022, February 1). *The Metaverse is a Labour Issue*. <https://socialeurope.eu/the-metaverse-is-a-labour-issue>

эксплуатацию пользователей внутри метавселенной» (Rosenberg, 2022). Устройства для доступа в виртуальную реальность собирают много данных о пользователе, обмен такими данными между компаниями позволит использовать их для профилирования и показа персонализированной рекламы, обладающей более сильным воздействием на потребителя, чем современная реклама.

2. Влияние на социум

Итак, метавселенная как глобальная цифровая платформа становится новым витком развития киберпространства, объединяющего все цифровые каналы. Процесс создания метавселенной – часть эволюции Интернета: интернет-технологии непрерывно развиваются, а вместе с ними расширяется и взаимодействие людей с Сетью. В этом процессе можно выделить три стадии развития онлайн-сообществ: прошедшую стадию Web 1.0 (объединение пользователей на основе виртуальных сетей), текущую стадию Web 2.0 (создание онлайн-сообществ) и будущую или уже начинающуюся – Web 3.0 (формирование виртуального мира, принадлежащего сообществам) (Шкарупета, 2022).

Созданием метавселенных занят целый ряд компаний, означает ли это, что метавселенных будет несколько? Представляется, что конкуренция между создаваемыми прототипами метавселенных приведет к их слиянию или поглощению, в итоге «полноценная» метавселенная будет единой, но включающей множество виртуальных миров и сегментов, например «китайский», «российский» и т. д.

Метавселенная как следующая версия Интернета будет представлять собой коллаборативную открытую среду смешанной реальности, в которой взаимодействуют люди и интеллектуальные вещи в рамках многих виртуальных миров, создаваемых разными корпорациями на общей технологической, экономической и этической платформе¹⁷. Некоторые исследователи говорят о предопределенности (детерминированности) построения «децентрализованного общества» на этапе Web 3.0 (Weyl et al., 2022).

В любом случае прежняя социальная ткань, включающая различные социальные группы, в виртуальном мире во многом теряет свое значение. IT-гиганты стремятся трансформировать образ жизни людей и саму природу человека, реализуя идею метавселенной, переводящей жизнь в «цифровой формат»: важность онлайн-идентификации, профессионального и бытового онлайн-общения, цифровых активов сильно возрастет.

Обучение, совершенствование навыков также будут проходить в метавселенной, став доступным из любой точки мира. Как инструмент для образования метавселенная весьма привлекательна: можно посещать лекции лучших университетов, проводить тренировки в безопасной среде. Переход к пятому, а затем к шестому поколению мобильной связи (5G и 6G) позволит обеспечить голографическое присутствие удаленных пользователей в визуализированном пространстве и передачу тактильных ощущений с помощью сенсоров. Нейрофизиологи отмечают, что тренировка внимания и самоконтроля в условиях

¹⁷ Гопка, А. (2021, 14 сентября). Следующая версия интернета: как изменится жизнь в метавселенной. https://www.forbes.ru/tekhnologii/439893-sleduusa-versia-interneta-kak-izmenitsa-zizn-v-metavse_lennoj

объединения физического и цифрового миров даст лучшие результаты при меньших усилиях (Tang et al., 2022).

По мнению исследователей одного из крупнейших аналитических центров Brookings Institution, высказанному в докладе, посвященном воздействию метавселенной на образование, «образование отстает от цифровых скачков, технологии, а не преподаватели, определяют образовательные возможности»¹⁸. В докладе приводится пример: знакомство на уроке истории с культурой Древней Греции через виртуальное погружение похоже на путешествие в машине времени, где каждый ученик сможет использовать свой цифровой аватар, чтобы побыть археологом, оснащенным соответствующими виртуальными инструментами, или по-другому изучать античность.

Стратегия развития метавселенной ориентирована преимущественно на молодое поколение, которому привычны интерактивные компьютерные игры. Уже к настоящему моменту роль видеоигр в повседневной жизни человека увеличилась (особенно на мобильных платформах). Интерактивные игры все больше «встраиваются» в реальность и подстраивают ее под себя. Попытки создать игровые платформы с расширенной функциональностью вызывают одобрение пользовательской аудитории, поэтому число компаний-разработчиков растет.

Технических преград для «трансформации видеоигр в бесконечно обновляемые, генерирующие события интерактивные вселенные» (П. Е. Архипов, 2022) уже нет, просто технологии по экономическим характеристикам пока не подходят для массового использования. Необходимые для подключения к метавселенной гаджеты не являются комфортными для постоянного ношения, на решение этой проблемы направлены огромные ресурсы. С повышением комфортности устройств, через которые пользователи взаимодействуют с метавселенной, они станут неотъемлемой их частью, со временем возможно встроенной для удобства в тело человека.

Если ранее в виртуальной среде ощущалась разница с реальностью (в движении, в степени «прорисовки» аватара), то сегодня достигнут выход на уровень гиперреальности – симуляции, неотличимой от реального мира. Ранее создание такого контента было сложным и дорогостоящим процессом, сейчас искусственный интеллект может конструировать недорогой и очень реалистичный «синтетический контент». В ближайшие годы метавселенную будут развивать в направлении иммерсивного (с эффектом присутствия) опыта в гиперреальных виртуальных средах, населенных аватарами, которые выглядят и звучат точно так, как люди. Это позволит привлечь миллиарды людей в метавселенную: чем дальше, тем больше генерирующие модели искусственного интеллекта будут использовать данные из окружающего мира для визуализации впечатлений и объектов, масштабируя персонализированный контент для миллиардов людей¹⁹.

Социальная коммуникация поменяется: люди в метавселенной будут взаимодействовать не только с аватарами других людей, но и с аватарами-агентами, созданными искусственным интеллектом.

¹⁸ Hirsh-Pasek, K., Zosh, J. M., Shwe Hadani, H., Michnick Golinkoff, R., Clark, K., Donohue, Ch., & Wartella, E. (2022). *A whole new world: Education meets the metaverse*. Report: Policy brief. Washington, Brookings. https://www.brookings.edu/wp-content/uploads/2022/02/A-whole-new-world_Education-meets-the-metaverse-FINAL-021422.pdf

¹⁹ Graham, T. (2022, June 18). *Can humanity be recreated in the metaverse?* <https://venturebeat.com/2022/06/18/can-humanity-be-recreated-in-the-metaverse/>

Необходимо упомянуть о том, что возможности искусственного интеллекта в условиях метавселенной изменятся. Метавселенная будет идеальной средой для систем искусственного интеллекта (ИИ-систем), как виртуальных, так и киберфизических. В киберфизических системах искусственный интеллект заключен в физическую оболочку, являющуюся носителем искусственного интеллекта. Виртуальная ИИ-система не «привязана» к конкретному физическому объекту, но пользуется аппаратными средствами, через которые может влиять на физический мир, в том числе подчиняя себе более «слабую» киберфизическую ИИ-систему. Для виртуальной ИИ-системы виртуальный мир – это естественная среда. Киберфизические ИИ-системы, имеющие «тело» и поэтому обладающие преимуществами перед виртуальными системами в реальном мире, в условиях метавселенной теряют его. Тем не менее они сохраняют возможность подключаться к виртуальному миру и не нуждаются в специальных внешних устройствах в отличие от людей.

Современное общество уже раздвинуло пределы реального мира, вошло «в искусственно созданное виртуальное пространство и превратилось в гибридный социум» (Недзвецкая, Простаков, 2022). Со временем человек станет относиться к коммуникациям в цифровой среде как к реальной, перенося на цифровых аватаров возможность реальных человеческих взаимодействий (Федосеева, Егармин, 2022). Согласно результатам проведенных социологических исследований, дети нередко воспринимают контакты с виртуальными ИИ-ассистентами как с живыми существами (Bylieva et al., 2021). Впрочем, это касается не только детей, «искусственный интеллект все более становится социальным: агенты, изначально ориентированные на решение инструментальных задач, становятся средой и участниками человеческих взаимодействий» (Резаев и др., 2020). Речь идет о постепенном формировании «искусственной социальности». Создание «полноценной» метавселенной позволит пойти дальше и «погрузить умерших творцов в новую гибридную среду в качестве активных элементов» (Gurov, 2022), продолжающих создавать произведения науки, литературы и искусства. Социологи все чаще задаются вопросом: способна ли метавселенная, расширяющая границы взаимодействий и ощущений ее участников, претендовать на создание новой основной человеческой реальности? (Ваторопин и др., 2022).

Среди возникающих социальных проблем можно назвать:

- появление новых потребностей («виртуальные вещи» теперь будут востребованы не только любителями компьютерных игр, их использование станет общепринятой практикой);
- неравенство в доступе, которое будет проистекать из цены гаджетов, доступности глобальной сети, уровня цифровой грамотности;
- утрату конфиденциальности в жизни человека, ведь иммерсивные гарнитуры и виртуальные инструменты метавселенной будут фиксировать, куда человек идет, на что смотрит, как выражение его лица и модуляции голоса раскрывают эмоции;
- проблему идентичности индивида (люди будут создавать цифровые аватары для навигации по метавселенной, что добавляет возможностей в виртуальном мире выдавать себя за кого-то другого);
- увеличение проблем со здоровьем (киберзависимость, «сенсорный конфликт», проблемы от недостатка подвижности) (Денисов, 2019);
- деградацию моральных ценностей в виртуальной среде, что отразится и на физическом мире (Гуров, Конькова, 2022);

– обеспечение безопасности детей при «погружении» в метавселенную, ведь дети, несмотря на возрастные ограничения для пользователей, как правило, осваивают новые технологии быстрее, чем их родители; с точки зрения монетизации дети – высокодоходный сегмент, поэтому многие виртуальные миры ориентированы на них и т. д.

3. Потребность в конституционализации новых прав

Цифровые технологии сделали большие сообщества реальными, теперь эти сообщества делают технологии обязательными (Жуков, 2022). Виртуализация общества и перенос растущей части контактов в цифровую среду продолжится, следовательно, острота перечисленных выше социальных проблем будет расти, что вызывает необходимость адаптации права к новым условиям. Не исключено, что создание метавселенной как сложного многоаспектного явления потребует установления экспериментальных правовых режимов (Малашенко, Шестаков, 2022).

Еще в статье 2013 г., анализируя влияние игровых виртуальных миров, исследователь из СПбГУ В. В. Архипов пришел к выводу, что виртуальные миры заслуживают пристального внимания юристов, являясь «принципиально новым и социально значимым явлением», они «могут использоваться как модели реального мира и как пространство для социального эксперимента» (Архипов, 2013). Позднее в другой статье он отмечает, что «в условиях цифровой трансформации общества актуализируется круг юридических проблем, связанных с пределами вмешательства реального права в виртуальное пространство» (Архипов, 2019).

Формирование метавселенной повлечет «перепрошивку» реального мира, который меняется с распространением цифровых технологий. Смена поколений – очередной шаг вперед, так как у тех, кто родился в эпоху цифровых гаджетов, технологическая толерантность выше, чем у предыдущего поколения.

Какие вопросы требуют внимания со стороны права?

Развитие кибердемократии способствует переносу процесса принятия политических решений в киберпространство. В действующем законодательстве уже предусмотрено электронное голосование, к примеру, в 2022 г. Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»²⁰ был дополнен ст. 64.1 о возможности проведения дистанционного электронного голосования. VR/AR-технологии способны сделать голосование доступным независимо от места нахождения лица с сохранением эффекта присутствия. Создание метавселенной устраняет недостаток современной кибердемократии – отсутствие места, в котором люди могут собираться для обсуждения и принятия коллективного решения, ощущая реальное присутствие друг друга (Williams, 2006).

Так как использование Интернета увеличивает вероятность участия граждан в голосовании (Mossberger et al., 2007), формирование метавселенной сделает возможной полноценную реализацию концепции цифрового гражданства, изменив привычные способы осуществления политических и иных прав. Это соответствует происходящей платформизации государственного управления, когда государство все

²⁰ Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации. № 67-ФЗ. (2022). *Собрание законодательства РФ*, 24, ст. 2253.

больше становится похожим на цифровую платформу по оказанию государственных услуг. Выборы и референдумы через государственные цифровые суперсервисы (доработанные «Госуслуги» или нечто подобное) – скорее всего, дело ближайшего будущего.

В то же время IT-гиганты все больше контролируют инфраструктуру публичного дискурса (Nemitz, 2018), эти корпорации уже захватили цифровую общественную сферу и, используя часто неосведомленное согласие пользователя, заменили закон условиями обслуживания компаний, над которыми государственные органы не всегда могут осуществлять контроль. Тем самым корпорации фактически взяли на себя множество функций, которые входят в компетенцию государств, и многие государства не могут оказать достаточного сопротивления (D'Cunha, 2021). С помощью цифровых технологий IT-гиганты и государства – мировые технологические лидеры приобретают возможности, позволяющие им сильно влиять на все мировое сообщество, о чем прямо говорится в докладе «Противостояние реальности в киберпространстве. Внешняя политика для фрагментированного Интернета», подготовленном в 2022 г. исследователями из ведущих научных и аналитических центров США, в частности Стэнфорда и Колумбийского университета (Fick et al., 2022).

Глобализация коммуникаций вступает в противоречие с суверенитетом государства как свободой от внешнего контроля, поэтому в условиях глобализации информационных процессов и распространения информационных войн возникают новые угрозы национальным интересам, что актуализирует обеспечение цифрового суверенитета (Zozulia et al., 2021) и требует изменений в законодательстве. Меры по обеспечению цифрового суверенитета включают разработку национальных операционных систем, инструментов работы с большими данными, национальных протоколов цифрового шифрования. Необходимость регулирования цифровых активов как критической инфраструктуры, защита цифрового гражданства, установление требований к алгоритмам, управляющим социальными взаимодействиями, расположение серверов и процессоров, осуществляющих обработку данных, на территории государства – эти меры активно обсуждаются в парламентах разных стран мира²¹.

Развитие метавселенных поднимает, с одной стороны, вопрос о создании правовых норм, нацеленных на недопустимость подрыва доверия к правительствам, с другой – вопрос о нормах, направленных на недопущение установления цифровой диктатуры. Ведь правительство сможет применить технологии метавселенной для наблюдения за гражданами, отслеживая их действия, передвижения с целью контроля над информационными потоками, управления ими с ограничением возможности людей выражать противоположные взгляды и создавать массовый консенсус (Akyeşilmen, 2021). Решение подобной задачи облегчается с развитием нейротехнологий, позволяющих использовать нейроинтерфейсы в качестве основных каналов доставки контента и обеспечивающих взаимодействие мозга человека с объектами, не существующими в реальности.

Стоит учесть, что базовой предпосылкой существования права является человеческое взаимодействие, основанное на эмоциях, желаниях и преследовании

²¹ Gak, M. (2021, December 9). *A ten-point manifesto for a Digital European Citizenship*. <https://www.opendemocracy.net/en/technology-and-democracy/a-ten-point-manifesto-for-a-digital-european-citizenship/>

определенных интересов. Право и доверие (межличностное, системное доверие) связаны друг с другом – это приводит к предположению, что право теряет свою актуальность с уменьшением релевантности доверия (Koos, 2022).

Таким образом, задачи конституционно-правового регулирования, вытекающие из цифровизации общества и формирования метавселенной, касаются устранения рисков:

- 1) дискриминации и цифрового неравенства;
- 2) утраты политических прав;
- 3) сокращения права на частную жизнь;
- 4) манипуляции сознанием человека.

Для минимизации перечисленных рисков следует закрепить в конституции права, необходимые человеку в условиях цифровизации всех сфер общества и растущей степени виртуализации среды.

Во-первых, признать право на свободный доступ в Интернет конституционным правом личности. Это базовое цифровое право требует фиксации в нормах конституции, что позволит обеспечить реализацию целой группы прав человека, потребность в которых появляется с развитием виртуальной среды (Рожкова, 2020). Кстати, Мексика уже признала такое право, с 2014 г. оно закреплено в ее конституции²². В законодательных органах Италии и Франции данный вопрос обсуждается. По мнению некоторых представителей Национальной ассамблеи Франции, реформа должна включать «основополагающее право, поощряющее свободный, равный и универсальный доступ к цифровым сетям» (La Raudière, 2018). Первый проект конституционного закона, касающегося этого вопроса²³, был внесен президентом Франции в Национальную ассамблею в 2018 г.

Во-вторых, вывести право на защиту персональных данных на уровень конституционного принципа. Например, через дополнение ст. 2 Конституции РФ, провозглашающей приоритет прав человека, второй частью. В настоящее время в Конституции РФ имеются ст. 23, 24 и 29, устанавливающие в общем виде право на неприкосновенность частной жизни, условия поиска и распространения информации, но следует учесть, что мониторинг в метавселенной выходит на новый уровень, а возможности для манипуляции возрастают многократно, ведь VR/AR-технологии изначально построены на обмане чувств. Последнее позволит выдавать необходимую информацию, используя полученные персональные данные для точного нацеливания на конкретных людей в нужное время. Искусственный интеллект, контактируя с человеком в целях убедить его, будет действовать с учетом данных о предыдущем поведении человека и о его реакциях на другой контент. Острота проблемы защиты персональных данных растет с увеличением их оцифрованного объема по мере «погружения» в метавселенную. Законодательство должно обеспечить максимальную прозрачность в отношении того, какие данные собираются и как они используются.

²² *Digital government toolkit. Digital government strategies: good practices. Mexico: Legal Framework for the National Digital Strategy.* (2014). <https://www.oecd.org/gov/mexico-legal-framework.pdf>

²³ *Projet de loi constitutionnelle "Pour une démocratie plus représentative, responsable et efficace".* (2021, Août 23). <https://www.gouvernement.fr/action/projet-de-loi-constitutionnelle-pour-une-democratie-plus-representative-responsable-et>

В-третьих, в качестве гарантий неприкосновенности частной жизни, исключающих возможность подвергнуться незаконному надзору со стороны государственных органов или частных корпораций, необходимо задуматься над включением в конституцию новой группы прав человека, так называемых нейроправ: права на психическую неприкосновенность, права на психическую целостность и права на интеллектуальное самоопределение (когнитивную свободу) (Ienca & Andorno, 2017). Первым в мире государством, включившим нейроправа в свою конституцию, стала Республика Чили, а обсуждение темы нейроправ как новой группы прав на уровне Парламентской ассамблеи Совета Европы²⁴, начавшееся в 2020 г., подчеркивает важность вопроса (Филипова, 2022).

Гарантии прав человека усилит и закрепление в Конституции принципа открытости алгоритмов в целях прозрачности работы искусственного интеллекта. Требование о прозрачности включает право знать о причинах решения, вынесенного искусственным интеллектом, право знать об искусственной или естественной природе субъекта, с которым вступает в контакт человек, и право на решение, основанное не только на автоматизированной обработке.

4. Вопросы отраслевого регулирования

С развитием метавселенной повышается значение цифрового профилирования. Отсутствие правовых ограничений на формирование цифровых профилей снижает неприкосновенность частной жизни, ущемляет право на человеческое достоинство и облегчает изготовление дипфейков злоумышленниками, применяющими искусственный интеллект. «Несмотря на то, что в настоящее время цифровые профили граждан представляют собой только свод официальной информации, содержащейся в некоторых государственных информационных системах и публичных реестрах, в будущем... данная инфраструктура может быть использована для профилирования людей, углубленного анализа, мониторинга и прогнозирования их поведения, как это делается уже сегодня некоторыми государственными и негосударственными организациями» (Мочалов, 2021).

Необходимо утвердить перечень сведений, которые не могут входить в состав цифрового профиля гражданина, перечень недопустимых целей использования цифровых профилей, кроме того, закрепить обязанность операторов в доступной форме доводить до субъектов информацию о фактах и юридических последствиях профилирования. Создание сверхточных цифровых профилей должно быть запрещено во избежание дискриминации граждан, а сбор таких психофизиологических параметров, как частота сердечных сокращений, разрешен лишь в медицинских целях. Все вышеперечисленное требует включения соответствующих норм в источники конституционного и административного права.

Нормами административного и гражданского права должна быть предусмотрена «защита прав граждан при осуществлении сбора, оценки и использования данных в рамках цифрового профилирования» с применением систем искусственного

²⁴ Парламентская ассамблея Совета Европы. (2022). Документы, принятые Ассамблеей 12–13 и 22–23 октября 2020 г. Предварительное издание. Страсбург. <https://rm.coe.int/adoptedtextscp-oct-20-ru/1680a043a6>

интеллекта «на базе дискриминационных алгоритмов по тому или иному социальному критерию» (Минбалеев, 2022).

С распространением цифровых аватаров возникает вопрос об их правовом режиме. Они «соотносятся с виртуальными мирами как часть и целое, вследствие чего могут рассматриваться как предмет правоотношений в области интеллектуальной собственности», с другой стороны, аватары являются способом самопрезентации пользователей, выражения их идентичности, их «цифровым телом», что позволяет правоведам «соотносить аватаров с категориями персональных данных и нематериальных благ» (В. В. Архипов, 2022).

Цифровой аватар – это «виртуальное воплощение человека, отражающее его образ и наиболее существенные черты характера, особенности индивидуальных цифровых ритуалов» (Федорченко, 2020). Аватар как средство самопрезентации человека в виртуальной среде нередко отражает его страхи, желания, психические отклонения, «связь аватара и личности обусловлена теорией проекции, которую предложила А. Фрейд» (Заславский, 2021). Смогут ли цифровые аватары иметь свою собственную правовую идентичность или они останутся лишь проекцией личности человека, контролирующего их? А если аватар создаст и будет контролировать система искусственного интеллекта? Необходимы правовые нормы, содержащие требование об обязательном отличии искусственных агентов в метавселенной от реальных людей.

Исследователем из Сингапурского университета Б. Ч. Чонгом высказывается мнение о необходимости признания субъектами права цифровых аватаров. Рассуждая об этом в своей статье «Аватары в метавселенной: возможные юридические проблемы и средства правовой защиты», он пишет: «Пользователи будут ожидать, что права их аватаров будут защищены в метавселенной... одним из способов решения проблемы было бы признание аватара ответственным за свои действия» (Cheong, 2022). Предположим, аватар украдет цифровую «сумку Gucci», соответственно, эффективным наказанием станет применение санкции в метавселенной к данному аватару. Это тем более разумно, если аватар создан и управляется искусственным интеллектом, а не человеком. По мнению Б. Ч. Чонга, даже аватара, созданного человеком, если он дополнен искусственным интеллектом и постоянно учится у своего хозяина-человека, как принимать решения, самостоятельно взаимодействуя с иными субъектами в метавселенной, можно было бы признать субъектом права в условиях метавселенной. Это выводит на новый уровень спор о признании/непризнании правосубъектности искусственного интеллекта, в который включается все больше юристов (Наумов, 2020).

Еще одной проблемой, нуждающейся в правовом решении, является технологическая возможность одного лица создать множество аватаров в метавселенной, как следствие, необходимым становится наличие административно-правовых норм, регулирующих этот момент. То же самое можно сказать и о возможности изменения или замены аватара, ведь это влияет на прозрачность социального поведения. «Правовая защита аватара должна быть согласована с надлежащим юридическим контролем возможности злоупотребления аватаром» (Dwivedi et al., 2022).

Уголовному законодательству придется учесть рост киберпреступности, особенно хищений криптовалюты и персональных данных, в том числе биометрической информации. Кстати, криминологи раньше других заинтересовались этой тематикой в разрезе «виртуальных преступлений» (Brenner, 2008), еще применительно к онлайн-играм, потому как последствия ситуаций внутри игры могут оказывать влияние на реальность, что выступает одновременно причиной и условием

вторжения права в виртуальную среду (Степанов, Филатова, 2021). Сегодня исследователи нередко ссылаются на «тест магического круга», разработанный Б. Т. Дюранске (Duranske, 2008), смысл которого в том, что виртуальное пространство отделено «магическим кругом» от реальности, и вторая не должна испытывать негативных последствий от происходящего в первом. Правовое регулирование не требуется, пока все разворачивается только внутри игры и подчиняется ее правилам (Adrian, 2010), если же происходит выход за пределы «магического круга», ситуация меняется. Например, захватив учетную запись, некто использует чужой аватар, выдавая себя за другого человека, и совершает деяние, влекущее юридические последствия, в том числе привлечение к ответственности этого человека.

В метавселенной может быть совершено практически любое преступление, возможное в реальном мире: кража, уничтожение имущества, нанесение телесных повреждений, убийство и т. д. Телесные повреждения или убийство могут касаться как цифрового аватара, так и реального человека, ведь теоретически возможно нанесение телесных повреждений разной степени тяжести пользователю, получившему доступ к метавселенной, с помощью тактильного костюма. Но и «убийство» аватара может причинить серьезный вред человеку, к примеру, войдя в метавселенную для работы, он обнаруживает, что хакер уничтожил его цифровой аватар – тщательно сконструированное «цифровое тело», на создание которого было потрачено немало средств – его нельзя восстановить, поэтому пропускается важная виртуальная встреча, за что работник лишается работодателем определенных благ. Кто компенсирует потери и будет ли наказан злоумышленник?²⁵

Применительно к гражданскому праву актуальным становится вопрос о «связывании» физической собственности с ее цифровым эквивалентом: что произойдет, если владение физическим объектом и эквивалентом NFT будут отдельными, что изменится, если физический объект будет потерян, украден или уничтожен?²⁶

Изменения в гражданском законодательстве коснутся положений об интеллектуальной собственности. Среди проблем, которые возникнут в сфере авторского права, можно назвать:

- рост числа споров по использованию объектов авторских прав в виртуальном пространстве (метавселенная повышает риск создания контента с использованием плодов чужого интеллектуального труда, поэтому защиту авторских прав придется совершенствовать);

- определение правовой судьбы виртуальных объектов, созданных искусственным интеллектом внутри метавселенной (Тимшин, 2022).

Получение прав на образ человека (живого или умершего) может быть предметом авторских прав, с развитием метавселенной у этого направления появляются новые перспективы. «При заселении метавселенной персонажами на основе людей необходимо получить права на использование имени человека, внешнего вида, поведения и артефактов. С живыми людьми это делается через лицензионное соглашение, которое должно быть максимально подробно расписано. Для использования образа и имени умершего человека проводится процедура «очистки

²⁵ McCollum, C. (2022, January 24). *Metalaw: The Law of the Metaverse*. <https://www.iotforall.com/metalaw-law-of-metaverse>

²⁶ Abraham, A. (2022, April 4). *Law & Order in the Metaverse*. <https://www.finextra.com/the-long-read/376/law--order-in-the-metaverse>

прав» (Добрякова, Близнец, 2022). Принципиально важным и пока не урегулированным становится то, что формирование метавселенной и развитие искусственного интеллекта со временем позволят «продолжить» создавать новые произведения умершим в реальности творцам, «воскрешенным» внутри метавселенной и получившим «цифровое бессмертие».

Имеющихся норм права будет недостаточно и для регулирования трудовых отношений между миллионами работников и работодателями. Пока трудовое законодательство как в России, так и в зарубежных странах не адаптировано к цифровой трансформации. В настоящее время на повестке дня проблема регулирования платформенной занятости. В условиях формирования метавселенной законодателю придется ответить на целый ряд новых вопросов:

- Что будет считаться рабочим временем, будет ли в него засчитываться онлайн-присутствие аватара в метавселенной?
- Должен ли аватар работника соответствовать реальному человеку?
- Обязаны ли аватары соблюдать дресс-код на рабочем месте?
- По каким правилам должен осуществляться наем работника через виртуальную реальность?
- Может ли работодатель устанавливать меры стимулирующего характера для тех работников, которые более лояльны к переходу в виртуальную среду?
- Какова будет ответственность работодателей за правонарушения своих работников в метавселенной?
- Какую ответственность понесет работодатель в случае киберзапугивания аватара работника?
- Каков будет статус аватаров, выполняющих функции работников, но созданных искусственным интеллектом?

Если эти вопросы не будут урегулированы законодательно, работодатель примет решение по каждому из них самостоятельно, не учитывая интересы работников. Кроме того, в мире растет трудовая миграция, в том числе за счет предложений работы на цифровых платформах. Такая виртуальная миграция не требует физического перемещения работников, с созданием метавселенной процесс выйдет на новый уровень (Глуценко, 2021).

Изменения потребуются и в процессуальном законодательстве, которое должно будет предусмотреть как опцию рассмотрение споров с участием аватаров, проведение виртуальных заседаний суда с эффектом реального присутствия и т. д. Международное право не сможет остаться в стороне как минимум потому, что возникают вопросы, связанные с разрешением трансграничных споров в условиях метавселенной.

Отдельные юристы настаивают на своевременности формирования права метавселенной²⁷, ведь ее создание открывает недоступные ранее возможности для развития общества, с одной стороны, и поднимает фундаментальные вопросы, связанные с частной жизнью, информационной безопасностью, интеллектуальной собственностью, с другой. «Вопросы группируются вокруг одной основополагающей дилеммы: кто за что отвечает? Трудности только усугубляются возрастающей сложностью и взаимозависимостью ИИ-систем... Становится все труднее возлагать юридическую ответственность на владельцев аватаров, разработчиков программного

²⁷ Metaverse Policy Institute. <https://www.metaversepolicy.org/>

обеспечения и операторов метавселенной, каждый из которых может иметь разную степень контроля над ИИ-системами» (Mostert & Yeoh, 2022). По мнению сторонников формирования права метавселенной, все вышеперечисленное требует нового типа правовой инфраструктуры, частью которой и станет новая группа норм, регулирующих общественные отношения в условиях метавселенной. Данное мнение не находит поддержки у большинства правоведов в первую очередь в связи с тем, что пока общество находится на начальной стадии создания метавселенной. Некоторые юристы считают, что выделение права метавселенной в ближайшие годы возможно, но только внутри другой общности норм – киберправа.

Можно согласиться с исследователем из Georgian Institute of Public Affairs (GIPA) Л. Нанобашвили, что, несмотря на существующую неопределенность, ясны как минимум две вещи: во-первых, метавселенная, исходя из динамики развития событий, будет формироваться дальше, становясь реальностью, и, во-вторых, создание метавселенной поднимает ряд вопросов правового характера. «Эти вопросы требуют юридического анализа, который может занять юристов и законодателей на долгие годы», причем «вероятно, метавселенная будет развиваться быстрее, чем будет создано ее правовое регулирование» (Nanobashvili, 2022).

Выводы

Развитие технологического направления метавселенных ведет к дальнейшей виртуализации экономики, провоцируя трансформации в структуре производства, управлении, маркетинговой политике и экономике труда. Меняются условия занятости на глобальном рынке труда, запросы потребителей. Увеличивается доля производителей и продавцов товаров, переключающихся на развитие цифровых экосистем и создающих приложения с расширенным набором функций для удобства использования в виртуальной среде.

Социальная ткань общества также меняется, повседневная жизнь людей включает все больше виртуальной составляющей: онлайн-общение, онлайн-обучение, онлайн-услуги, удаленная работа и т. д., следствием этого становится смена привычек, бытовых и культурных предпочтений.

Европейская парламентская исследовательская служба (EPRS) 24 июня 2022 г. опубликовала пресс-релиз «Метавселенная: возможности, риски и последствия для политики», в котором подчеркивается, что создание метавселенной окажет серьезное влияние на «конкуренцию, защиту данных, обязательства, финансовые транзакции, кибербезопасность, здоровье, а также доступность и инклюзивность»²⁸. Европейский парламент призвал Европейскую комиссию обеспечить соблюдение требований компаниями, которые станут функционировать в метавселенной, для чего обновить действующий с 2018 г. Общий регламент по защите данных (GDPR)²⁹. Таким образом, задачу поиска путей оптимального регулирования в условиях метавселенной перед правоведами начинают ставить уже законодательные органы.

²⁸ EU: EPRS reports on opportunities, risks, and policy implications of the metaverse. (2022, June 27). <https://www.dataguidance.com/news/eu-eprs-reports-opportunities-risks-and-policy>

²⁹ Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Развитие ситуации позволяет сделать вывод, что работа над созданием норм права, учитывающих происходящие изменения, связанные с виртуализацией среды, становится неизбежной в ближайшие годы, причем поиск правовых решений не ограничится рамками одной отрасли права, а вызовет необходимость комплексного подхода и межотраслевого взаимодействия.

Представляется необходимой конституционализация цифровых прав в публично-правовом понимании термина. Наличие в ст. 23, 24 и 29 Конституции РФ общих положений о праве на неприкосновенность частной жизни и о распространении информации не является достаточным для защиты прав граждан в условиях развития технологий метавселенной и их реализации на практике. Требуется как минимум закрепление на конституционном уровне права на свободный доступ в Интернет и права на защиту персональных данных в качестве важнейшего конституционного принципа.

В связи с развитием нейротехнологий встает вопрос о включении в конституцию нейроправ, призванных защитить человека от несанкционированного воздействия на мозг. Угроза такого воздействия будет расти вследствие применения нейрогаджетов как устройств для доступа к метавселенной, когда нейроинтерфейсы станут основными каналами доставки контента в мозг человека, а считывание ритмов мозговой активности через нейронаушники – привычным для пользователей.

Недостаточно перечислить новые права в конституции, нужно включить детализирующие положения в отраслевое законодательство, дополнив рядом норм гражданское, уголовное, административное, трудовое и иные отрасли права, тем самым адаптируя правовую материю к новым условиям в целях сохранения эффективности правового регулирования и обеспечения антропоцентризма в обществе, вступающем в эпоху искусственного интеллекта.

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

Список литературы

- Алабина, Т. А., Дзангиева, Х. С., Юшковская, А. А. (2022). Метавселенная как глобальный тренд экономики. *Экономика. Профессия. Бизнес*, 1, 5–12. EDN: <https://elibrary.ru/lyhnip>. DOI: <https://doi.org/10.14258/epb202201>
- Архипов, В. В. (2013). Виртуальное право: основные проблемы нового направления юридических исследований. *Известия высших учебных заведений. Правоведение*, 2, 93–114. <https://elibrary.ru/qbkcff>
- Архипов, В. В. (2019). Действие правовых норм в цифровом медиапространстве и семантические пределы права. *Правоведение*, 1, 8–27. EDN: <https://elibrary.ru/ynkvva>. DOI: <https://doi.org/10.21638/spbu25.2019.101>
- Архипов, В. В. (2022). Персонажи (аватары) в многопользовательских компьютерных играх: вопросы правовой квалификации в свете междисциплинарных исследований. *Закон*, 3, 58–74. EDN: <https://elibrary.ru/lnqrtj>. DOI: <https://doi.org/10.37239/0869-4400-2022-18-3-58-74>
- Архипов, П. Е. (2022). Отождествление человека с его игровым аватаром в рамках игровых метавселенных. Повседневные практики в видеоиграх. *Знак: проблемное поле медиаобразования*, 1(43), 53–61. EDN: <https://elibrary.ru/qseysc>. DOI: <https://doi.org/10.47475/2070-0695-2022-10106>
- Ваторопин, А. С., Ваторопин, С. А., Тепляков, И. И., Чевтаева, Н. Г. (2022). Метавселенная: перспективы создания и социальные последствия. *Теория и практика общественного развития*, 4, 19–25. EDN: <https://elibrary.ru/xhrwef>. DOI: <https://doi.org/10.24158/tipor.2022.4.2>
- Глущенко, Г. И. (2021). Развитие виртуальной миграции в контексте цифровизации. *ДЕМИС. Демографические исследования*, 2, 57–64. EDN: <https://elibrary.ru/gdmvre>. DOI: <https://doi.org/10.19181/demis.2021.1.2.4>

- Гуров, О. Н., Конькова, Т. А. (2022). Метавселенные для человека или человек для метавселенных. *Искусственные общества*, 17(1). EDN: <https://elibrary.ru/nuucyx>. DOI: <https://doi.org/10.18254/S207751800019011-1>
- Денисов, Э. И. (2019). Роботы, искусственный интеллект, дополненная и виртуальная реальность: этические, правовые и гигиенические проблемы. *Гигиена и санитария*, 98(1), 5–10. EDN: <https://elibrary.ru/vtgtgb>. DOI: <https://doi.org/10.18821/0016-9900-2019-98-1-5-10>
- Добрякова, Г., Блинец, И. (2022). Цифровые вселенные (метаверсы) – права на образ аватара и NPC. *Интеллектуальная собственность. Авторское право и смежные права*, 2, 54–58. <https://elibrary.ru/cxfcmg>
- Жуков, В. А. (2022). Право и этика метавселенной. *Закон*, 7, 148–164. EDN: <https://elibrary.ru/yjyuch>. DOI: <https://doi.org/10.37239/0869-4400-2022-19-7-148-164>
- Заславский, Д. А. (2021). Аватар как средство самопрезентации личности в виртуальной среде. *Инновации. Наука. Образование*, 48, 1909–1914. <https://elibrary.ru/ruevsy>
- Малашенко, Г. Т., Шестаков, Д. Ю. (2022). Национальная экономическая безопасность в эпоху метавселенных. *Вестник Московского университета МВД России*, 3, 339–343. EDN: <https://elibrary.ru/brxtdn>. DOI: <https://doi.org/10.24412/2073-0454-2022-3-339-343>
- Минбалеев, А. В. (2022). Проблемы гражданско-правовой защиты личных неимущественных прав в процессе цифрового профилирования граждан. *Гражданское право*, 2, 9–11. EDN: <https://elibrary.ru/tqolti>. DOI: <https://doi.org/10.18572/2070-2140-2022-2-9-11>
- Мочалов, А. Н. (2021). Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности. *Lex russica*, 74(9), 88–101. EDN: <https://elibrary.ru/qfedzo>. DOI: <https://doi.org/10.17803/1729-5920.2021.178.9.088-101>
- Наумов, В. Б. (ред.). (2020). *Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития: монография*. Санкт-Петербург.: НП-Принт. <https://elibrary.ru/rkhlue>
- Недзвецкая, Н. П., Простаков, И. И. (2022). Виртуальная реальность цифрового социума. *Философия хозяйства*, 3(141), 208–217. <https://elibrary.ru/zyxbjl>
- Резаев, А. В., Стариков, В. С., Трегубова, Н. Д. (2020). Социология в эпоху «искусственной социальности»: поиск новых оснований. *Социологические исследования*, 2, 3–12. EDN: <https://elibrary.ru/zmuozb>. DOI: <https://doi.org/10.31857/S013216250008489-0>
- Рожкова, М. А. (2020). Цифровые права: публично-правовая концепция и понятие в российском гражданском праве. *Хозяйство и право*, 10, 3–12. <https://elibrary.ru/psbnmh>
- Степанов, П. П., Филатова, М. А. (2021). Проблемы уголовно-правовой охраны виртуального игрового имущества. *Всероссийский криминологический журнал*, 15(6), 744–755. EDN: <https://elibrary.ru/ipqdm>. DOI: [https://doi.org/10.17150/2500-4255.2021.15\(6\).744-755](https://doi.org/10.17150/2500-4255.2021.15(6).744-755)
- Тимшин, Ю. П. (2022). Формирование правовой модели использования объектов авторских прав в виртуальном пространстве метавселенных. *Юридическая наука*, 6, 172–177. <https://elibrary.ru/riwbjy>
- Федорченко, С. Н. (2020). Феномен искусственного интеллекта: гражданин между цифровым аватаром и политическим интерфейсом. *Журнал политических исследований*, 4(2), 34–57. EDN: <https://elibrary.ru/ebngsh>. DOI: <https://doi.org/10.12737/2587-6295-2020-34-57>
- Федосеева, Р. Р., Егармин, А. Е. (2022). Цифровые аватары и коммуникация в цифровой среде. *Научно-технические инновации и веб-технологии*, 1, 84–88. <https://elibrary.ru/QGBMOX>
- Филипова, И. А. (2022). Нейротехнологии в праве и правоприменении: прошлое, настоящее и будущее. *Правоприменение*, 6(2), 32–49. EDN: <https://elibrary.ru/ktqbm>. DOI: <https://doi.org/10.52468/2542-1514.2022>
- Шкарупета, Е. В. (2022). Концепция метавселенных Web 3.0 в стратегическом управлении цифровым потенциалом: теория, инструментарий и практические приложения. В книге: *Цифровая экономика и Индустрия 5.0: развитие в новой реальности* (с. 10–31). Санкт-Петербург: Политех-пресс. <https://elibrary.ru/gxcahg>
- Adrian, A. (2010). Beyond grieving: Virtual Crime. *Computer Law & Security Review*, 26(6), 640–648. <https://doi.org/10.1016/j.clsr.2010.09.003>
- Akyeşilmen, N. (2021). Editorial preface: towards a cyber dictatorship. *Cyberpolitik Journal*, 6(11), VI–VIII.
- Brenner, S. W. (2008). Fantasy Crime: The Role of Criminal Law in Virtual Worlds. *Vanderbilt Journal of Entertainment and Technology Law*, 11(1), 1–97.
- Bylieva, D., Bekirogullari, Z., Lobatyuk, V., & Nam, T. (2021). How Virtual Personal Assistants Influence Children's Communication. In *Knowledge in the Information Society*. PCSF 2020 (pp. 112–124). Cham, Springer. https://doi.org/10.1007/978-3-030-65857-1_12

- Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, 3(2). <https://doi.org/10.1365/s43439-022-00056-9>
- D'Cunha, C. (2021). A State in the disguise of a Merchant: Tech Leviathans and the rule of law. *European Law Journal*, 27, 1–53. <https://doi.org/10.1111/eulj.12399>
- Duranske, B. T. (2008). *Virtual Law. Navigating Legal Landscapes of Virtual Worlds*. Chicago: American Bar Association.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M. et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>
- Fick, N., Miscik, J., Segal, A. et al. (2022). Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. *Independent Task Force Report No. 80*. Washington: Council on Foreign Relations.
- Gurov, O. (2022). Panel discussion “The processes of reality creation: metaverses of visionaries and projects of its embodiment” (March 30). *Artificial Societies*, 17(2). EDN: <https://elibrary.ru/kcizif>. DOI: <https://doi.org/10.18254/S207751800020299-7>
- Ienca, M., & Andorno, R. (2017). Towards new human rights in the age of neuro-science and neurotechnology. *Life Sciences, Society and Policy*, 13(5), 1–27. <https://doi.org/10.1186/s40504-017-0050>
- Koos, S. (2022). Digital Globalization and Law. *Lex Scientia Law Review*, 6(1), 33–68. <https://doi.org/10.15294/lesrev.v6i1.55092>
- La Raudière, L. de. (2018). La fabrique de la loi à l'ère du numérique. *Enjeux numériques*, 3, 73–76.
- Ly, Zh., Qiao, L., Li, Y. et al. (2022). BlockNet: Beyond reliable spatial Digital Twins to Parallel Metaverse. *Patterns*, 3(5), 100468. <https://doi.org/10.1016/j.patter.2022.100468>
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2007). *Digital Citizenship: The Internet, Society, and Participation*. Cambridge, MA: MIT Press. <https://doi.org/10.7551/mitpress/7428.001.0001>
- Mostert, F., & Yeoh, W. T. (2022). Meta-Worse, a lawyer's mega paradise. *Journal of Intellectual Property Law & Practice*, 17(3), 211–212. <https://doi.org/10.1093/jiplp/jpac008>
- Nanobashvili, L. (2022). If the Metaverse is Built, Will Copyright Challenges Come? *UIC Review of Intellectual Property Law*, 21(3), 215–251.
- Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A. Mathematical Physical and Engineering Sciences*, 376(2133). <https://doi.org/10.1098/rsta.2018.0089>
- Rosenberg, L. (2022). Regulation of the Metaverse: A Roadmap. *6th International Conference on Virtual and Augmented Reality Simulations (ICVARS 2022)* (pp. 1–10). Brisbane. <https://doi.org/10.1145/3546607.3546611>
- Tang, Yi-Y., Tang, R., Posner, M. I. et al. (2022). Effortless training of attention and self-control: mechanisms and applications. *Trends in Cognitive Sciences*, 26(7), 567–577. <https://doi.org/10.1016/j.tics.2022.04.006>
- Weyl, E. G., Ohlhaver, P., & Buterin, V. (2022). Decentralized Society: Finding Web3's Soul. *ResearchHub*, 1–36. <https://doi.org/10.2139/ssrn.4105763>
- Williams, R. W. (2006). Democracy, Cyberspace, and the Body. *Cultural Logic: A Journal of Marxist Theory & Practice*, 13, 1–33. <https://doi.org/10.14288/cllogic.v13i0.191780>
- Zozulia, O., Zozulia, I., Brusakova, O. et al. (2021). Information Sovereignty as the Basis of Modern State Information Security. *International Journal of Computer Science and Network Security*, 21(12), 264–268. <https://doi.org/10.22937/IJCSNS.2021.21.12.38>

Сведения об авторе



Филипова Ирина Анатольевна – кандидат юридических наук, доцент, доцент кафедры трудового и экологического права, Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского
Адрес: 603922, Российская Федерация, г. Нижний Новгород, проспект Гагарина, 23

E-mail: irinafilipova@yandex.ru

ORCID ID: <https://orcid.org/0000-0003-1773-5268>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/R-1375-2016>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57327205000>

Google Scholar ID: <https://scholar.google.com/citations?user=opJc7fcAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=461586

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 31 августа 2022 г.

Дата одобрения после рецензирования – 14 сентября 2022 г.

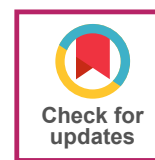
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.1>



Creating the Metaverse: Consequences for Economy, Society, and Law

Irina A. Filipova 

National Research Lobachevsky State University of Nizhni Novgorod
Nizhniy Novgorod, Russian Federation

Keywords

Artificial intelligence,
augmented reality,
cyberspace,
digital avatar
digital platform,
human rights,
law,
meta-universe,
neural rights,
virtual reality

Abstract

Objective: to define the degree of influence of such developing technological field as metaverse on various spheres of society and to identify the need for reaction on the part of law.

Methods: the key method used for the research is the systemic-structural method, which allows establishing connections between various elements of the society as a complex system, analyzing the regularities generated by the spreading influence of metaverse prototypes in one sphere on other ones. Additional methods used are formal-logical, comparative-legal methods, as well as the methods of legal modeling and forecasting.

Results: the practical implementation of the metaverse concept will open new opportunities for people, but will be accompanied by drastic changes in the economic subsystem of the society, in particular, the multifold growth of the share of virtual economy and structural changes in employment. The changes will also occur in the social subsystem: the social links and the education models will transform, new personal demands will occur. Changes in the economic and social spheres will entail the need to adapt law to them, in order to preserve the effective legal regulation of social relations. Also, it should be noted that the metaverse will increase the capabilities of not only people but also the artificial intelligence, for which virtual environment is actually the "natural" one. Legal norms must provide protection of a human under the increased virtual component in people's lives, accompanied by intellectualization of the environment.

Scientific novelty: the author has systematically analyzed the changes taking place in various spheres of the modern society in connection with the development of the technological field of metaverses; highlighted the key issues arising due to the said development and requiring legal solution both at the constitutional level and at the level of sector legislation; and proposed the necessary changes in legal regulation.

© Filipova I. 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.

Practical significance: the research materials can be used when preparing proposals on changes and amendments in the current legislation, as well as in pedagogical activity, in particular, for implementation of educational courses or modules related to law under digital transformation of the society.

For citation

Filipova, I. A. (2023). Creating the Metaverse: Consequences for Economy, Society, and Law. *Journal of Digital Technologies and Law*, 1(1), 7–32. <https://doi.org/10.21202/jdtl.2023.1>

References

- Adrian, A. (2010). Beyond grieving: Virtual Crime. *Computer Law & Security Review*, 26(6), 640–648. <https://doi.org/10.1016/j.clsr.2010.09.003>
- Akyeşilmen, N. (2021). Editorial preface: towards a cyber dictatorship. *Cyberpolitik Journal*, 6(11), VI–VIII.
- Alabina, T. A., Dzangieva, K. S., & Yushkovskaya, A. A. (2022). The metaverse as a global economic trend. *Economics Profession Business*, 1, 5–12. (In Russ.). <https://doi.org/10.14258/epb202201>
- Arkhipov, P. E. (2022). Identification of a person with his game avatar in game metaverse. Everyday practices in video games. *Sign: problematic field in media education*, 1(43), 53–61. (In Russ.). <https://doi.org/10.47475/2070-0695-2022-10106>
- Arkhipov, V. V. (2013). Virtual law: main problems of the new direction of legal studies. *Proceedings of Higher Educational Institutions. Pravovedenie*, 2, 93–114. (In Russ.).
- Arkhipov, V. V. (2019). The effect of legal norms in the digital media space and the semantic limits of law. *Pravovedenie*, 63(1), 8–27. (In Russ.). <https://doi.org/10.21638/spbu25.2019.101>
- Arkhipov, V. V. (2022). Personages (avatars) in multiuser computer games: issues of legal qualification in the light of interdisciplinary research. *Zakon*, 3, 58–74. (In Russ.). <https://doi.org/10.37239/0869-4400-2022-18-3-58-74>
- Brenner, S. W. (2008). Fantasy Crime: The Role of Criminal Law in Virtual Worlds. *Vanderbilt Journal of Entertainment and Technology Law*, 11(1), 1–97.
- Bylieva, D., Bekirogullari, Z., Lobatyuk, V., & Nam, T. (2021). How Virtual Personal Assistants Influence Children's Communication. In *Knowledge in the Information Society. PCSF 2020* (pp. 112–124). Cham, Springer. https://doi.org/10.1007/978-3-030-65857-1_12
- Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, 3(2). <https://doi.org/10.1365/s43439-022-00056-9>
- D'Cunha, C. (2021). A State in the disguise of a Merchant: Tech Leviathans and the rule of law. *European Law Journal*, 27, 1–53. <https://doi.org/10.1111/eulj.12399>
- Denisov, E. I. (2019). Robots, artificial intelligence, augmented and virtual reality: ethical, legal and hygienic issues. *Hygiene and Sanitation*, 98(1), 5–10. (In Russ.). <https://doi.org/10.18821/0016-9900-2019-98-1-5-10>
- Dobryakova, G., & Bliznets, I. (2022). Digital universes (metaverses) – rights for images of avatar and NPC. *Intellectual'naya sobstvennost'. Avtorskoe pravo i smezhnye prava*, 2, 54–58. (In Russ.).
- Duranske, B. T. (2008). *Virtual Law. Navigating Legal Landscapes of Virtual Worlds*. Chicago: American Bar Association.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M. et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>
- Fedorchenko, S. (2020). Artificial intelligence phenomenon: citizen between digital avatar and political interface. *Journal of Political Research Volume*, 4(2), 34–57. (In Russ.). <https://doi.org/10.12737/2587-6295-2020-34-57>
- Fedoseeva, R. R., & Egarmin, P. A. (2022). Digital avatars and communication in the digital environment. *Nauchno-tekhnicheskie Innovatsii i Veb-tehnologii*, 1, 84–88. (In Russ.).

- Fick, N., Miscik, J., Segal, A. et al. (2022). Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. *Independent Task Force Report No. 80*. Washington: Council on Foreign Relations.
- Filipova, I. A. (2022). Neurotechnologies in law and law enforcement: past, present and future. *Law Enforcement Review*, 6(2), 32–49. (In Russ.). [https://doi.org/10.52468/2542-1514.2022.6\(2\).32-49](https://doi.org/10.52468/2542-1514.2022.6(2).32-49)
- Glushchenko, G. I. (2021). Development of Virtual Migration in the Context of the Ongoing Digitalization. *DEMIS. Demographic Research*, 1(2), 57–64. (In Russ.). <https://doi.org/10.19181/demis.2021.1.2.4>
- Gurov, O. (2022). Panel discussion “The processes of reality creation: metaverses of visionaries and projects of its embodiment” (2022, March 30). *Artificial Societies*, 17(2). <https://doi.org/10.18254/S207751800020299-7>
- Gurov, O., & Konkova, T. (2022). Metaverses for Human or Human for Metaverses. *Artificial Societies*, 17(1). (in Russ.). <https://doi.org/10.18254/S207751800019011-1>
- Ienca, M., & Andorno, R. (2017). Towards new human rights in the age of neuro-science and neurotechnology. *Life Sciences, Society and Policy*, 13(5), 1–27. DOI: <https://doi.org/10.1186/s40504-017-0050>
- Koos, S. (2022). Digital Globalization and Law. *Lex Scientia Law Review*, 6(1), 33–68. <https://doi.org/10.15294/lesrev.v6i1.55092>
- La Raudière, L. de. (2018). La fabrique de la loi à l'ère du numérique. *Enjeux numériques*, 3, 73–76.
- Lv, Zh., Qiao, L., Li, Y. et al. (2022). BlockNet: Beyond reliable spatial Digital Twins to Parallel Metaverse. *Patterns*, 3(5), 100468. <https://doi.org/10.1016/j.patter.2022.100468>
- Malashenko, G. T., & Shestakov, D. Yu. (2022). National economic security in the age of the metaverse. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 3, 339–343. (In Russ.). <https://doi.org/10.24412/2073-0454-2022-3-339-343>
- Minbaleev, A. V. (2022). Problems of the civil law protection of personal non-property rights in the process of the digital profiling of citizens. *Grazhdanskoe Pravo*, 2, 9–11. (in Russ.).
- Mochalov, A. N. (2021). Digital Profile: Main Risks for Constitutional Human Rights in the face of Legal Uncertainty. *Lex Russica*, 74(9), 88–101. (In Russ.). <https://doi.org/10.17803/1729-5920.2021.178.9.088-101>
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2007). *Digital Citizenship: The Internet, Society, and Participation*. Cambridge, MA: MIT Press. <https://doi.org/10.7551/mitpress/7428.001.0001>
- Mostert, F., & Yeoh, W. T. (2022). Meta-Worse, a lawyer's mega paradise. *Journal of Intellectual Property Law & Practice*, 17(3), 211–212. <https://doi.org/10.1093/jiplp/jpac008>
- Nanobashvili, L. (2022). If the Metaverse is Built, Will Copyright Challenges Come? *UIC Review of Intellectual Property Law*, 21(3), 215–251.
- Naumov, V. B. (Ed.). (2020). *Legal and ethical aspects related to development and implementation of artificial intelligence systems and robotics: history, modern state and prospects of development*: monograph. Saint Petersburg: NP-Print. (In Russ.)
- Nedzvetskaya, N. P., & Prostakov, I. I. (2022). Virtual reality of a digital society. *Philosophy of Economy*, 3(141), 208–217. (In Russ.).
- Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A. Mathematical Physical and Engineering Sciences*, 376(2133). <https://doi.org/10.1098/rsta.2018.0089>
- Rezaev, A. V., Starikov, V. S., & Tregubova, N. D. (2020). Sociology in the Age of ‘Artificial Sociality’: Search of New Bases. *Sotsiologicheskie Issledovaniya*, 2, 3–12. (In Russ.). <https://doi.org/10.31857/S013216250008489-0>
- Rosenberg, L. (2022). Regulation of the Metaverse: A Roadmap. *6th International Conference on Virtual and Augmented Reality Simulations (ICVARS 2022)* (pp. 1–10). Brisbane. <https://doi.org/10.1145/3546607.3546611>
- Rozhkova, M. A. (2020). Digital rights: public-legal concept and notion in the Russian civil law. *Khozyaistvo i pravo*, 10, 3–12. (In Russ.).
- Shkarupeta, E. V. (2022). The Web 3.0 metaverse concept in strategic management of digital potential: theory, tools and practical applications. In *Digital economy and Industry 5.0: development in the new reality* (pp. 10–31). (In Russ.). Saint Petersburg: Politekh-press.
- Stepanov, P. P., & Filatova, M. A. (2021). Problems of Protecting Virtual Game Property by Means of Criminal Law. *Russian Journal of Criminology*, 15(6), 744–755. (In Russ.). [https://doi.org/10.17150/2500-4255.2021.15\(6\).744-755](https://doi.org/10.17150/2500-4255.2021.15(6).744-755)
- Tang, Yi-Y., Tang, R., Posner, M. I. et al. (2022). Effortless training of attention and self-control: mechanisms and applications. *Trends in Cognitive Sciences*, 26(7), 567–577. <https://doi.org/10.1016/j.tics.2022.04.006>
- Timshin, Yu. P. (2022). Formation of a legal model for the use of copyright objects in the virtual space of the metaverses. *Legal Science*, 6, 172–177. (In Russ.).
- Vatoropin, A. S., Vatoropin, S. A., Teplyakov, I. I., & Chevtayeva, N. G. (2022). Metaverse: creation perspectives and social consequences. *Theory and Practice of Social Development*, 4, 19–25. (In Russ.). <https://doi.org/10.24158/tipor.2022.4.2>

- Weyl, E. G., Ohlhaver, P., & Buterin, V. (2022). Decentralized Society: Finding Web3's Soul. *ResearchHub*, 1–36. <https://doi.org/10.2139/ssrn.4105763>
- Williams, R. W. (2006). Democracy, Cyberspace, and the Body. *Cultural Logic: A Journal of Marxist Theory & Practice*, 13, 1–33. <https://doi.org/10.14288/cllogic.v13i0.191780>
- Zaslavskii, D. A. (2021). Avatar as a means of self-presentation of a personality in the virtual environment. *Innovatsii. Nauka. Obrazovanie*, 48, 1909–1914. (In Russ.).
- Zhukov, V. A. (2022). Law and ethics of the metaverse. *Zakon*, 7, 148–164. (In Russ.). <https://doi.org/10.37239/0869-4400-2022-19-7-148-164>
- Zozulia, O., Zozulia, I., Brusakova, O. et al. (2021). Information Sovereignty as the Basis of Modern State Information Security. *International Journal of Computer Science and Network Security*, 21(12), 264–268. <https://doi.org/10.22937/IJCSNS.2021.21.12.38>

Author information



Irina A. Filipova – PhD (Law), Associate Professor, Department of Labor and Environmental Law, National Research Lobachevsky State University of Nizhni Novgorod

Address: 23 prospekt Gagarina, Nizhniy Novgorod 603922, Russian Federation

E-mail: irinafilipova@yandex.ru

ORCID ID: <https://orcid.org/0000-0003-1773-5268>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/R-1375-2016>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57327205000>

Google Scholar ID: <https://scholar.google.com/citations?user=opJc7fcAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=461586

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – August 31, 2022

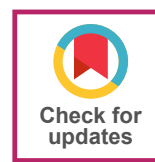
Date of approval – September 14, 2022

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 34:004.8:007.524:62-529.4
EDN: <https://elibrary.ru/unsonv>
DOI: <https://doi.org/10.21202/jdtl.2023.2>



Регулирование умных роботов и искусственного интеллекта в Европейском союзе

Кьяра Галлезе-Нобиле 

Эйнховенский технологический университет
г. Эйнховен, Королевство Нидерландов;
Университет Триеста
г. Триест, Итальянская Республика

Ключевые слова

Европейский союз,
законодательство,
искусственный интеллект,
кибербезопасность,
машинное обучение,
право,
регулирование,
робот,
робототехника,
цифровые технологии

Аннотация

Цель: в последние годы в Европе стала очевидной необходимость создания нормативных актов в области робототехники и искусственного интеллекта. Европейский союз нуждается в стандартизации регулирования, которое обеспечило бы высокий уровень безопасности робототехнических систем и предотвратило потенциальные нарушения. Поэтому новое законодательство должно гарантировать, что именно производители несут ответственность за выявление «слепых зон» в этих системах, содержащих недоработки, а в случае обнаружения уязвимостей на поздних этапах – обновлять систему, даже если модель уже не находится на рынке. Цель данной статьи – предложить ряд возможных поправок к существующим положениям нормативных актов Евросоюза.

Методы: используя методологию Кестемонта для юридических исследований, автор анализирует и сравнивает тексты нормативных актов и увязывает их с техническими положениями об умных роботах, в результате выделяя критические элементы, требующие доработки.

Результаты: в статье предлагаются поправки к существующим проектам законов: по мнению автора, хотя закон об искусственном интеллекте и закон о киберустойчивости представляют собой первый шаг в этом направлении, их основные принципы недостаточно детализированы, а значит, не позволяют регулировать их практическое применение. Поэтому законодатели должны тщательно определить, в каких случаях модели, использующие обучение в течение всего жизненного цикла, могут быть допущены на рынок. Автор предлагает

© Галлезе-Нобиле К., 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.

увеличить сроки обязательного обновления систем, предусмотренные в существующих проектах законов, поскольку пятилетний срок не соответствует уровню риска, связанного с продуктами длительного пользования, такими как транспортные средства.

Научная новизна: автор рассматривает действующую нормативную базу в области систем искусственного интеллекта и устройств с цифровыми элементами, выделяет риски действующей правовой базы и вносит предложения по возможному усовершенствованию существующих проектов законов.

Практическая значимость: материалы статьи могут быть использованы для доработки существующих проектов закона об искусственном интеллекте и закона о киберустойчивости.

Для цитирования

Галлезе-Нобиле, К. (2023). Регулирование умных роботов и искусственного интеллекта в Европейском союзе. *Journal of Digital Technologies and Law*, 1(1), 33–61. <https://doi.org/10.21202/jdtl.2023.2>

Содержание

Введение

1. Искусственный интеллект и роботы: определения
2. Регулирование искусственного интеллекта и умных роботов в ЕС: технические регламенты
3. Законодательные решения для предотвращения кибератак
 - 3.1. Машинное обучение и черные ящики
 - 3.1.1. Нормативные акты и стандарты безопасности для моделей на основе машинного обучения
 - 3.2. Правила и стандарты защиты для производителей и программистов
 - 3.3. Правила защиты и стандарты для пользователей
 - 3.4. Сбалансированная система защищенности и стандартов
4. Принципы закона о киберустойчивости

Выводы

Список литературы

Введение

Несмотря на заметные достижения Директивы о сетевой и информационной безопасности (Network and Information Security, NIS Directive) и предпринимаемые усилия по их углублению с помощью Директивы NIS II, проектов закона о киберустойчивости и закона об искусственном интеллекте, тема кибербезопасности в цифровую эпоху остается важнейшей для европейского рынка. Инструменты регулирования помогли нескольким государствам – членам Евросоюза адаптировать свои институциональные, правовые и ценностные подходы к кибербезопасности, однако распространение

таких современных технологий, как системы искусственного интеллекта, а также такие беспрецедентные обстоятельства, как пандемия COVID-19, ускорили переход к цифровому сообществу через увеличение картины угроз и создание новых проблем, требующих решения на национальном и международном уровнях. Участились и стали более серьезными кибератаки, исходящие как изнутри, так и снаружи Евросоюза и часто создающие значительные риски для прав и свобод граждан¹. Поскольку целями кибератак становятся все новые объекты оборудования и программного обеспечения, прогнозируется, что к 2021 г. ежегодный ущерб от киберпреступности в мире достигнет 5,5 трлн евро.

В Пояснительной записке к проекту закона о киберустойчивости показано, как недостаточный уровень понимания и низкая информированность пользователей мешают им выбирать продукты с адекватными возможностями киберзащиты и приводят к небезопасному потреблению². Такие продукты подвержены двум серьезным рискам, которые могут привести к ущербу для пользователей и сообщества в целом: (1) недостаточной информационной безопасности, которая проявляется в постоянных нарушениях защиты, а также в неадекватном и нерегулярном появлении обновлений, необходимых для борьбы с ними, и (2) низкому уровню знаний и доступности информации для пользователей³. Кибератака на один продукт может затронуть целую организацию или цепь поставки, зачастую быстро распространяясь за пределы границ внутреннего рынка⁴.

Реформирование правовых механизмов кибербезопасности находит поддержку среди предпринимателей и компетентных представителей власти. В ходе многочисленных консультаций они указывали, что Директиву NIS необходимо распространить на другие отрасли, интегрировать или оптимизировать дополнительные меры безопасности, а также упростить требования к отчетности⁵. Это говорит о том, что вопрос кибербезопасности воспринимается как важнейшая проблема, требующая решения на институциональном уровне.

В настоящей статье представлены некоторые результаты анализа проблем, связанных с сетевыми умными роботами в европейской системе права, и ряд предложений в этой сфере. В первой части представлен анализ определения искусственного интеллекта (далее – ИИ) и умных роботов, описаны инструменты регулирования в этой области. Затем приводятся некоторые соображения по поводу машинного обучения и принципа «черного ящика», выделены вопросы, требующие решения на уровне ЕС. Наконец, дается краткий анализ недостатков проекта закона о киберустойчивости.

¹ Commission Staff Working document Delivering on the UN's Sustainable Development Goals – A comprehensive approach. https://sdgtoolkit.org/wp-content/uploads/2021/02/EU-staff_working_document-delivering_on_uns_sustainable_development_goals_en.pdf

² European Commission. (2022). https://ireland.representation.ec.europa.eu/news-and-events/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products-2022-09-15_en

³ Там же.

⁴ Там же.

⁵ Commission Staff Working document Delivering on the UN's Sustainable Development Goals – A comprehensive approach. https://sdgtoolkit.org/wp-content/uploads/2021/02/EU-staff_working_document-delivering_on_uns_sustainable_development_goals_en.pdf

1. Искусственный интеллект и роботы: определения

В последнее десятилетие использование систем на основе искусственного интеллекта, включая роботов, особенно использующих машинное обучение, достигло значительных масштабов и будет только расти в будущем (Wang & Siau, 2019). Среди примеров их современного применения – дроны (De Swarte et al., 2019), самоуправляемые автомобили (Rao & Frtunikj, 2018), медицинское оборудование (O'Sullivan et al., 2019) и средства диагностики (Nobile et al., 2019), бытовая техника (Yuniarthe, 2017), роботы для ухода за пожилыми (Simoens et al., 2016) и для совместной работы с людьми (Demir et al., 2019), переводчики (Bi, 2020), распознавание образов (Rundo et al., 2019), страхование (Lamberton et al., 2017), прогнозирование (например, юридических решений (Sourdin, 2018) или финансовых вопросов), аварийная связь (Raza et al., 2020), HR (Yano, 2017), управление дорожным движением (Aladin et al., 2019), управление электронной почтой (включая фильтры от спама (Das et al., 2015)), строительство (Chakkravarthy, 2019), логистика (Pandian, 2019), образование (Roll & Wylie, 2016) и множество других областей. Это быстрое развитие привело к тому, что уже несколько лет на повестке дня в Европейском союзе стоит вопрос правовой определенности в отношении новых технологий.

Уровень, достигнутый к настоящему времени в области ИИ, очень далек от того, что предсказывал Тьюринг («сильный ИИ»). Нынешний искусственный интеллект называют «узким ИИ» (Artificial Narrow Intelligence, ANI) (Kaplan & Haenlein, 2019), или «слабым ИИ» (Lu et al., 2017). Он состоит из систем, способных решать конкретные задачи на основе моделей и алгоритмов, созданных и отлаженных человеком, используя данные и параметры, произвольно выбранные создателем модели. Это означает, что он способен выполнять определенные задачи, иногда даже лучше, чем человек, но не может перенести эти навыки в другую область знаний. Следовательно, термин «интеллект» ошибочен.

Прежде всего, необходимо определить соответствующую юридическую терминологию, поскольку правовые определения часто не совпадают с терминологией ученых в области компьютерных наук (Smith, 2016), среди которых при этом также нет единогласия (Bekey, 2012).

Проект общеевропейского нормативного акта по ИИ (так называемый закон об ИИ, AI Act)⁶ перечисляет технологии, которые на уровне ЕС считаются искусственным интеллектом; предлагаемое определение системы искусственного интеллекта является очень широким и включает технологии, которые известны уже не одно десятилетие: «<...> программное обеспечение, разработанное с использованием одной или более технологий и подходов, перечисленных в Приложении I, и способное для заданного набора определенных человеком целей породить такие результаты, как содержание, предсказания, рекомендации или решения, влияющие на окружение, с которым оно взаимодействует». Фактически список в Приложении I содержит широкий спектр различных технологий: «а) подходы с точки зрения машинного обучения, включая контролируемое, неконтролируемое обучение и обучение с подкреплением, с использованием разнообразных методов, включая глубокое обучение; б) подходы на основе логики и знаний, включая представление знаний, индуктивное (логическое) программирование, базы

⁶ С проектом можно ознакомиться по ссылке: <https://ec.europa.eu/newsroom/dae/items/709090>

знаний, механизмы логического вывода и дедукции, (символические) умозаключения и экспертные системы; в) статистические подходы, байесовское оценивание, методы поиска и оптимизации». Цель данного определения – включить множество различных моделей, способных оказывать влияние на человека, даже если они пока не относятся к ИИ. Это затруднит вывод приложения из-под регулирования путем простой замены определения модели так, чтобы она не относилась к ИИ. Однако данное определение все же подвергалось критике как слишком широкое⁷.

Для термина «робот» сложно подобрать подходящее определение. По мнению экспертной группы High-Expert Group, «робототехнику можно определить как “ИИ, действующий в физическом мире”» (говорят также «воплощенный ИИ»). Робот – это физический механизм, которому приходится справляться с динамичностью, неопределенностью и сложностью физического мира. Такие функции, как восприятие, рассуждение, действие, обучение, а также способность взаимодействовать с другими системами, обычно интегрированы в архитектуру управления робототехнического комплекса. Кроме ИИ, строение и функционирование робота определяется также другими дисциплинами, такими как инженерная механика и теория управления. Примерами роботов являются роботизированные манипуляторы, беспилотные транспортные средства (например, машины, дроны, воздушные такси), гуманоидные роботы, роботы-пылесосы и др.

В исследовании «Европейские нормы гражданского права в сфере робототехники» (Nevejans, 2016), напротив, утверждается, что, поскольку научное сообщество еще не выработало единого определения роботов, нерешенными остаются и проблемы с терминами «умный робот» и «автономный робот» (Haselager, 2005). Некоторые авторы ссылаются на определение Richards и Smart (Richards & Smart, 2016), согласно которому робот – это «сконструированная система, выполняющая как физические, так и интеллектуальные действия, но не живая в биологическом смысле», однако при этом ведется настолько широкое обсуждение понятия «действия», что мы не можем рассматривать эту проблему здесь; ей будет посвящена отдельная статья.

Согласно решению Европейского парламента от 16 февраля 2017 г. с рекомендациями для Комиссии по нормам гражданского права в сфере робототехники (European Parliament, 2017), для признания в качестве умного робота с юридической точки зрения объект должен отвечать следующим условиям:

- получение автономии путем использования сенсоров и/или обмена данными с окружающей средой (совместимость), сравнения и анализа этих данных;
- самообучение на основе опыта и путем взаимодействия (необязательный критерий);
- по крайней мере, минимальное физическое воплощение;
- адаптация своего поведения и действий к окружающей среде;
- отсутствие жизни в биологическом смысле.

⁷ См., например, проект заявления Комитета по проблемам промышленности, науки и энергетики для Комитета по проблемам внутреннего рынка и защиты прав потребителей и Комитета гражданских свобод, правосудия и внутренних дел, доступный по ссылке: https://www.europarl.europa.eu/doceo/document/ITRE-PA-719801_EN.pdf, а также проект заявления Комитета по правовым проблемам для Комитета по проблемам внутреннего рынка и защиты прав потребителей и Комитета гражданских свобод, правосудия и внутренних дел.

Определения очень важны для совершенствования существующих и выработки новых нормативных актов, поскольку многие ситуации могут выпасть из сферы регулирования, если они не подпадают под юридическое определение. При этом отмечается, что любые попытки дать всеобъемлющее определение обречены на провал, так как роботизированные приложения чрезвычайно разнообразны (Bertolini, 2013). В нашей работе мы используем термин «устройство» в отношении инструментов и роботов на основе ИИ, независимо от их типа, и термины «программное обеспечение» или «модель» в отношении систем ИИ, включая установленные на указанных устройствах.

Мы считаем, что с юридической точки зрения нет существенной разницы между механизмом, который можно назвать роботом, и управляемым искусственным интеллектом – устройством, которое нельзя в строгом смысле назвать роботом, но которое тем не менее является умным и может оказывать влияние на окружающую среду. Иногда граница между ними довольно подвижна. Например, являются ли роботами умная стиральная машина или робот-пылесос? Беспилотный автомобиль? Домашний помощник или мобильный телефон, управляющий дверями, светом, вентиляцией в доме, воротами гаража и т. д.? А что насчет 4D-принтера? Если это не роботы, то где должна проходить юридическая граница?

Если следовать определению, данному в вышеуказанной резолюции, то даже игрушечный утенок (отсутствие жизни и физическое воплощение),двигающийся по комнате и меняющий направление при блокировке колес о препятствие (адаптация к окружающей среде), имеющий таймер запуска в действие и исполняющий различные мелодии при перемене освещенности (получение автономии путем использования сенсоров), будет считаться умным роботом, даже если он состоит лишь из электрических цепей и механических деталей без какого-либо программного обеспечения или модели искусственного интеллекта.

Таким образом, данное определение довольно расплывчато и недостаточно для полного описания умного робота; оно включает механизмы, не обладающие никаким ИИ.

Предлагалось также считать ключевым аспектом робота его способность использовать программное обеспечение при выполнении конкретных задач (Leenes et al., 2017), однако, по нашему мнению, это неверно (так можно определить и компьютер!); фактически ни автономное выполнение задач (Santosuosso et al., 2012), ни наличие программного обеспечения не позволяют отграничить роботов от других механизмов. Например, достаточно вспомнить, что роботы могут создаваться с использованием таких физических компонентов, как мемристоры, которые выполняют ту же функцию, что и биологические синапсы в нейроморфных устройствах, не требуя при этом никакого программного обеспечения (Ames et al., 2012).

Программное обеспечение может быть загружено в робота, но может и существовать вне его, как в случае виртуальных роботов, которые подлежат регулированию как программное обеспечение. Более того, физические компоненты робота могут быть не связаны с конкретным программным обеспечением, которое при этом может продаваться отдельно. Код, управляющий роботом, может существовать как единое целое, но зачастую он составляется из множества взаимодействующих между собой модулей, где каждый компонент выполняет отдельную задачу.

В сфере ИИ важно различать концепции программного обеспечения, нейроморфных устройств и схем, а также программируемую пользователем вентильную

матрицу (ППВМ, FPGA). Различные технологии могут комбинироваться между собой, как в чипе Spikey⁸. При создании умного робота могут быть использованы любые решения, но правовые последствия для производителей и программистов будут различными.

Напротив, нейроморфные устройства (Ielmini & Ambrogio, 2019) и схемы (Pan et al., 2020) – это физические объекты, функционирующие только в конкретном роботе, в который они встроены; они разрабатываются для выполнения нейровычислений, но также используются для симуляции динамики биологических нейросетей (Papetti et al., 2020). Технология ППВМ (Botros & Abdul-Aziz, 1994) является промежуточной по отношению к двум вышеописанным решениям: это интегрированная физическая схема, которая может быть конфигурирована конечным пользователем или программистом.

Все эти решения могут использоваться при создании роботов, а в будущем, возможно, и функционирующего физического искусственного мозга.

Программируемость также не является существенным признаком робота: например, в принципе, возможно создать робота на магнитных модулях, который будет двигаться, самостоятельно выполнять действия и общаться с другими роботами световыми сигналами, при этом его создатель не будет знать, как он себя поведет, как в концепции М-куба (Romanishin et al., 2013).

Мы считаем, что программное обеспечение с использованием ИИ, которое может устанавливаться на любые устройства, должно регулироваться единым законодательством, независимо от того, установлено оно на устройство, имеющее в настоящий момент статус робота или нет; и наоборот, роботы, не относящиеся к категории умных роботов, особенно если они не связаны с Интернетом (как, например, промышленные роботы на заводском конвейере), должны относиться к сфере обычного законодательства о дефектной продукции и других норм, применимых к машинам. Различие следует проводить, руководствуясь влиянием на человека и общество, а не наличием физического объекта.

Основная причина, по которой необходимо объединить роботов и программное обеспечение на основе искусственного интеллекта в рамках одной дисциплины, состоит в том, что при их разделении будет возможно продавать программное обеспечение (далее – ПО) и устройство отдельно, не подпадая при этом под регулирование об умных роботах. Тогда любой пользователь сможет установить другое ПО и создать умного робота, запрограммировав его на выполнение любой деятельности. Следует отметить, что, по доминирующему мнению, не может считаться роботом устройство, дистанционно управляемое человеком, если человек должен присутствовать для выполнения определенных действий или контроля над устройством (Ebers & Navas, 2020; Funkhouser, 2013). Следовательно, физическое устройство без установленного на нем программного обеспечения (или доступного ему, как в случае выполнения ПО на облаке) также не может считаться роботом.

Следует также упомянуть, что робот, используемый в промышленном производстве, считается устройством, а значит, подпадает под Директиву 2006/42/ЕС Европейского парламента и Совета от 17 мая 2006 г. и под Директиву 95/16/ЕС³².

⁸ Дополнительную информацию см.: <https://www.kip.uni-heidelberg.de/vision/previous-projects/facets/neuromorphic-hardware/single-chip-system/spikey>

Европейский проект закона об ИИ фактически ссылается на Директиву об устройствах в аспекте включения умных роботов в общее регулирование ИИ, тем самым объединяя физических и виртуальных роботов.

2. Регулирование искусственного интеллекта и умных роботов в ЕС: технические регламенты

Когда тема искусственного интеллекта начала все более активно обсуждаться среди ученых в области компьютерных наук всего мира, европейские правоведы и законодотворцы задумались о правовых аспектах ИИ и умных роботов, сосредоточившись в основном на проблемах ответственности производителя, защиты прав потребителей и технического регулирования. В юридической доктрине была признана насущная необходимость принять сбалансированные отраслевые технические регламенты, которые отвечали бы потребностям самых разнообразных технологий роботостроения (Amidei, 2017).

При этом во многих случаях проблемы, вызванные роботами или устройствами с ИИ, рассматривались постфактум. Однако важно также понимать, как предотвращать аварии, особенно в области кибербезопасности. Даже если невозможно избежать проблемы в целом, важно анализировать ее с точки зрения предотвращения риска (такой подход используется в Директиве об устройствах), и новый проект закона об ИИ движется в этом направлении.

Самая важная инновация проекта закона об искусственном интеллекте – это положение о четырех категориях риска, связанного с системами ИИ, направленное на защиту основных прав граждан⁹.

⁹ Фактически в пояснительной записке к проекту отмечается: «Использование ИИ с его отличительными признаками (такими как непрозрачность, сложность, зависимость от данных, автономность действий) может отрицательно повлиять на количество фундаментальных прав, закрепленных в Европейской хартии по правам человека ("Хартия"). Данный проект нацелен на обеспечение высокого уровня защиты данных фундаментальных прав и работу с различными источниками рисков путем четко определенного подхода. Устанавливая ряд требований к надежному ИИ и пропорциональные обязательствам всех участников цепочки создания ценности, данный проект повысит и усилит защиту прав, закрепленных в Хартии: право на человеческое достоинство (ст. 1), уважение к частной жизни и защиту персональных данных (ст. 7 и 8), отсутствие дискриминации (ст. 21) и равенство между мужчиной и женщиной (ст. 23). Он нацелен на предотвращение нарушения прав в области свободы слова (ст. 11) и свободы собраний (ст. 12), на обеспечение защиты права на эффективное восстановление в правах и справедливое правосудие, прав на юридическую защиту и презумпцию невиновности (ст. 47 и 48), а также общего принципа компетентного руководства. Кроме того, при применении в определенных областях данный проект положительно повлияет на права ряда особых групп, например, права рабочих и справедливые условия работы (ст. 31), высокий уровень защиты прав потребителей (ст. 28), права ребенка (ст. 24) и интеграцию лиц с ограниченными возможностями (ст. 26). Сюда относятся также права на высокий уровень защиты и улучшение качества окружающей среды (ст. 37), в том числе в отношении здоровья и безопасности людей. Обязанности по априорному тестированию, управлению рисками и пользовательскому надзору будут также способствовать уважению других фундаментальных прав путем минимизации риска принятия ошибочных или предвзятых решений с помощью ИИ в таких критических областях, как образование и воспитание, занятость, важные услуги, правоохранительная и судебная деятельность. Если ущемление фундаментальных прав все же произойдет, пострадавшие лица смогут получить эффективное восстановление путем обеспечения прозрачности и отслеживаемости систем ИИ в сочетании со строгим последующим контролем».

Категории риска относятся к степени (интенсивности и масштабу) риска для безопасности или основных прав граждан и классифицируются по трем группам (четвертая группа – отсутствие риска):

- (i) неприемлемый риск,
- (ii) высокий риск,
- (iii) низкий или минимальный риск.

Данная классификация берет начало в законодательстве о безопасности товара и основана на предусмотренном назначении и условиях использования системы ИИ, а не только ее конкретной функции¹⁰. В проекте также приводится список запрещенных систем искусственного интеллекта, попадающих в первую категорию риска.

В рамках такого подхода умные роботы относятся к категории высокого риска (фактически, как уже говорилось, это ссылка на Директиву об устройствах). Такая классификация приводит к выработке новых требований, и программисты/производители должны применять следующее:

- систему управления риском;
- систему распоряжения данными;
- меры по обеспечению прозрачности;
- меры пользовательского надзора;
- меры по обеспечению точности, последовательности кибербезопасности;
- систему управления качеством.

После появления проекта закона об ИИ Еврокомиссия опубликовала новый проект относительно кибербезопасности: так называемый закон о киберустойчивости¹¹, нацеленный на обеспечение: 1) повышенной безопасности изделий с цифровыми элементами в течение всего их жизненного цикла; 2) гармонизации структуры кибербезопасности в Европе; 3) повышенной прозрачности свойств безопасности таких изделий; 4) повышенной безопасности таких изделий для организаций и потребителей.

В дополнение к новому подходу были опубликованы еще два проекта: Директива об ответственности в сфере ИИ и новая редакция Директивы об ответственности производителя.

В следующих разделах мы покажем, как эти требования могут быть реализованы и расширены за счет новых положений на этапе рассмотрения нового законодательства.

3. Законодательные решения для предотвращения кибератак

Следует отметить, что с развитием технологий обнаруживается все больше ошибок и дефектов в старом программном обеспечении (Buchanan, 2016), которые приводят к уязвимости перед киберугрозами (Ozkan & Bulkan, 2019) и требуют усовершенствования средств защиты. Среди примеров недавних атак можно упомянуть первый зарегистрированный случай смерти от кибератаки в сентябре 2020 г., когда из-за

¹⁰ В зависимости от правовой системы конкретного государства, квалификация высокого риска может повлечь иные последствия, помимо ответственности, см., например, ст. 2050 Гражданского кодекса Италии.

¹¹ Cyber-resilience Act. https://ireland.representation.ec.europa.eu/news-and-events/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products-2022-09-15_en

взлома 30 компьютеров через программу-вымогатель в больнице Дюссельдорфа (Германия) медицинская помощь не была оказана вовремя¹²; взлом умных камер наблюдения в 2019 г., результатом которого стал коллективный судебный иск в США¹³; обнаружение уязвимостей кардиоимплантов в больнице св. Иуды, с помощью которых хакеры могли разрядить батарею, вызвать неправильный ритм или сердечный приступ¹⁴; бот-сеть Мираи (Zhang et al., 2020), с 2016 г. атаковавшая ряд устройств интернета вещей. Угрозы системам ИИ могут быть физическими: в литературе описаны примеры, показывающие, как цветовые поля¹⁵ могут мешать работе нейронной сети, используемой беспилотными машинами (Ranjan et al., 2019), что приводит к неверному распознаванию или классификации сигналов и может вызвать аварии.

Очевидно, что борьба с кибератаками приобретает чрезвычайную важность, когда речь идет о фундаментальных правах, например, в сфере здравоохранения, которая особенно часто становится целью (Luna et al., 2016), или беспилотных машин, военной техники, спутников и других объектов, используемых для государственной обороны.

Производители и программисты постоянно обновляют программное обеспечение и устройства, пока не перейдут на новый продукт или новую версию существующего продукта. Через некоторое время они перестают разрабатывать защитные патчи и обновления для устаревших устройств, поскольку становится слишком дорого поддерживать тысячи продуктов на рынке, которые будут куплены лишь очень небольшим числом покупателей, или разрабатывать обновления для тех продуктов, которые уже ушли с рынка.

Чтобы программное обеспечение или операционные системы работали на определенных устройствах, производители последних вынуждены писать драйверы специально для этих устройств; поскольку такое ПО зачастую не является открытым, обновить эти устройства может только их производитель. Это означает, что устаревшие устройства, операционные системы и программное обеспечение в определенный момент остаются защищенными (например, Windows XP используется почти на 4 % компьютеров в мире, хотя уже не поддерживается компанией Microsoft), тем самым становясь легкой мишенью для атак. В некоторых случаях производители хотели бы обновить свои устройства, но не могут сделать этого, потому что осталось уже очень мало людей, которые понимают и могут правильно использовать древний или экзотический язык программирования (например, COBOL, который используется в банках; ADA – в военных приложениях, системах контроля авиатранспорта, коммерческих ракетах, спутниках, железнодорожном и скоростном транспорте; FORTRAN – в научных вычислениях), либо потому, что исходный код слишком длинный и сложный, чтобы его можно было изменить.

¹² Подробнее см. www.bbc.com/news/technology-54204356. Программа-вымогатель – это вредоносная программа, блокирующая доступ к данным пользователя и иногда угрожающая раскрыть их третьим лицам, если жертва не заплатит определенную сумму.

¹³ С полным текстом можно ознакомиться на: <https://www.courtlistener.com/docket/16630199/1/orange-v-ring-llc>

¹⁴ Об этом сообщало агентство CNN: <https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack>

¹⁵ Цветовое поле – это особый вид вредоносных патчей, технология машинного обучения, которая с помощью ложной информации пытается обмануть нейросети и вызвать их неправильное функционирование.

Если существующая система останется такой же, вполне вероятно, что производители не будут обновлять умных роботов в течение всего их жизненного цикла, поскольку по действующему законодательству производители не несут ответственности по истечении трех лет после обнаружения дефекта потребителем в рамках 10-летнего периода, тогда как проект закона о киберустойчивости предлагает защиту лишь в течение пяти лет. Однако некоторые роботы могут прослужить более 10 лет (например, автомобили только приобретают ценность через 30 лет; см., например, итальянское понятие «auto d'epoca» – «автомобиль эпохи»), а значит, останутся без защиты через несколько лет эксплуатации.

Техническое регулирование в этих областях может быть достигнуто тремя путями: запретом устаревших технологий, которые представляют риск для фундаментальных прав человека; принуждением производителей к обновлению устаревших устройств и программного обеспечения; комбинацией двух этих решений. Каждый вариант имеет свои плюсы и минусы.

Наконец, при создании нового законодательства по умным роботам необходимо учитывать свойства различных типов роботов, чтобы сформулировать конкретные положения для каждого из них. Некоторые роботы создаются самостоятельно путем взаимодействия между объектами (например, модульные роботы создают новый объект или в будущем роботы будут создавать роботов), поэтому человеку сложно предвидеть, как они будут собраны. Роботов такого типа следует отнести к категории высокого риска из-за непредсказуемости их поведения. Некоторые роботы могут передвигаться или влиять на окружающую среду, потенциально представляя риск нанесения вреда людям, тогда как другие не могут этого делать (например, светофоры). Некоторые действуют без надзора человека (например, автоматическая торговля на бирже), представляя значительный риск, а другие напрямую управляются человеком или иными внешними силами (такими как свет, звуки, химикаты, магниты, электричество и даже животные); некоторые выполняют действия и принимают «решения», оказывающие значительное влияние на определенные права, а другие имеют лишь ограниченное влияние. Наконец, некоторые связаны с Интернетом или другой сетью (интернет вещей) и потенциально подвержены кибератакам, а другие нет. Все эти аспекты необходимо тщательно рассматривать при применении технического регулирования.

Новый проект закона об искусственном интеллекте не касается вопроса регулирования умных роботов. Фактически положение о кибербезопасности звучит расплывчато: «Статья 15. Достоверность, устойчивость и кибербезопасность. 1. Системы ИИ, относящиеся к категории высокого риска, должны разрабатываться и создаваться таким образом, чтобы достичь, с учетом их предполагаемого назначения, надлежащего уровня достоверности, устойчивости и кибербезопасности, и последовательно действовать соответствующим образом в течение всего их жизненного цикла. 2. Уровни достоверности и соответствующей достоверности измерений в системах ИИ категории высокого риска должны быть указаны в прилагаемых пользовательских инструкциях. 3. Системы ИИ категории высокого риска должны обладать устойчивостью к отказам в отношении ошибок, неточностей и непоследовательностей, которые могут возникнуть внутри системы или в среде, где работает система, в особенности при ее взаимодействии с физическими лицами или другими системами. Устойчивость систем ИИ категории высокого риска может быть достигнута через технически избыточные решения, в том числе системы дублирования или

защиты от отказа. Системы ИИ категории высокого риска, которые продолжают обучаться после выхода на рынок или ввода в эксплуатацию, должны разрабатываться так, чтобы были приняты соответствующие меры защиты против возможных искажений в результате использования искаженных выходных данных на входе будущих операций («петля обратной связи»). 4. Системы ИИ категории высокого риска должны обладать устойчивостью к отказам в отношении попыток неуполномоченных третьих лиц изменить их использование или функционирование через уязвимости системы. Технические решения, направленные на обеспечение кибербезопасности систем ИИ категории высокого риска, должны быть адекватны соответствующим обстоятельствам и рискам. Технические решения для борьбы с конкретными уязвимостями ИИ должны включать, где это необходимо, меры для предотвращения и контролирования атак, направленных на манипулирование обучающими базами данных («заражение данных»), на ввод данных с целью заставить модель ошибаться («вредные примеры») и на недостатки модели».

В следующем разделе мы сфокусируем внимание на машинном обучении (контролируемом и неконтролируемом) и черных ящиках, так как они имеют особые свойства.

3.1. Машинное обучение и черные ящики

Благодаря научно-фантастической литературе мы привыкли к образу умного самообучающегося робота, однако в действительности лишь небольшая часть роботов запрограммирована для обучения на своем опыте. Некоторые роботы выглядят как умные роботы, так как выполняют сложные задачи и взаимодействуют с окружающей средой, но на самом деле они лишь запрограммированы с помощью простых алгоритмов.

С юридической точки зрения модели на основе машинного обучения (особенно глубокого обучения и непрерывного обучения) заслуживают пристального внимания благодаря своим характеристикам, поэтому мы обсудим их в отдельном подразделе.

3.1.1. Нормативные акты и стандарты безопасности для моделей на основе машинного обучения

Как известно, невозможно априори исключить наличие отклонений или дефектов (Naur & Randell, 1968), которые могут повлиять на поведение или решения, принимаемые устройством на основе искусственного интеллекта. Фактически модель создается человеком, который, разумеется, может ошибаться. Это означает, что программист никогда не сможет гарантировать, что модель поведет себя в точности так, как было запрограммировано¹⁶, но также это означает, что, меняя гиперпараметры и выбирая данные так, как удобно (или политически выгодно), можно при помощи того же инструмента получить иные результаты.

Используемые данные могут сами по себе представлять ту же проблему: они могут быть неверными, ошибочными, неполными или просто слишком скудными, чтобы иметь какой-то смысл¹⁷, поэтому результат будет ненадежным; более того, даже

¹⁶ Даже проведя множество тестов, нельзя исключить наличие багов. По словам Е. В. Дейкстра, известного специалиста в области компьютерных наук, обладателя премии Тьюринга, «тестирование показывает присутствие, а не отсутствие багов» (Dijkstra, 1982).

¹⁷ Фактически машинное обучение модели часто требует использования тысяч примеров.

если данные корректны, искусственный интеллект может сделать выводы, предвзятые по отношению к определенным группам¹⁸, на основе процессов, происходящих из-за неравенства, существующего в обществе, что в конечном итоге может нарушить соотношение между причиной и следствием, как показали некоторые широко известные эпизоды (Falletti, 2020).

Учитывая все вышесказанное, необходимо определить некоторые существенные риски и стандарты, которым должна отвечать модель искусственного интеллекта перед выпуском ее на рынок. По нашему мнению, ИИ следует моделировать по следующим общим критериям, часть из которых уже входит в Перечень для оценки надежности искусственного интеллекта (Assessment List for Trustworthy Artificial Intelligence, ALTAI):

- он должен быть понятным (в литературе чаще всего используются термины «прозрачность», «интерпретируемость», «объяснимость», «определимость» (Chakraborti et al., 2021; Gilpin et al., 2018; Holzinger et al., 2019), но мы считаем, что корректным термином является «интерпретируемость»), т. е. должны представляться прозрачными способы, которыми модель приходит к тем или иным решениям, так что всегда можно понять причины, по которым она делает выбор, а результат и обоснование решения модели всегда должны быть понятны людям;

- он должен соблюдать тайну частной жизни по умолчанию (Hildebrandt, 2019), т. е. модель должна отвечать требованиям европейского Общего регламента по защите данных в отношении данных пользователя и третьих лиц, а согласие на их использование должно быть информированным¹⁹;

- он должен быть этичным (Greene et al., 2019), т. е. должно быть установлено правило избегания любого дискриминирующего поведения, которое может возникнуть, когда робот будет выпущен в общество, даже если такое поведение еще не предусмотрено действующим законом²⁰;

- он должен быть непредвзятым (Dietterich & Kong, 1995), т. е. обучение ИИ должно проходить под контролем экспертов, чтобы устранить любую возможную предвзятость, одновременно добиваясь надежности и точности и соблюдения применимых законов и норм²¹;

- он должен быть современным и безопасным (Barreno et al., 2010), т. е. на регулярной основе должны применяться обновления и патчи, проводиться проверки,

¹⁸ Правовые аспекты машинного обучения в отношении возможной предвзятости и ее влияния на уязвимые группы будут рассмотрены в отдельной статье, так как эта тема слишком обширна для разбора здесь.

¹⁹ Хотя этот элемент уже присутствует в европейском законодательстве, граждане ЕС могут пострадать, если их данные будут собраны системами искусственного интеллекта за пределами Евросоюза.

²⁰ Следует отметить, что в настоящей работе мы не исследуем исключительно права, защищаемые законом в каждой правовой системе, так как тот факт, что какое-либо право еще не признано государством, не означает, что оно не существует или что оно не будет в дальнейшем введено в эту систему. Некоторые проблемы, возникающие при использовании ИИ, проистекают не от багов и других видов ошибок программирования, а от политических решений или ненамеренной предвзятости человека.

²¹ Важно заметить, что мы используем слово «предвзятость» в понимании юридической науки, которое отличается от понимания компьютерных наук; фактически с точки зрения программиста можно показать, что действительно непредвзятой модели не может существовать. В настоящей работе мы рассматриваем только такую предвзятость, которая с правовой и этической точек зрения может повлечь дискриминацию или нарушение прав личности.

а механическая часть должна также проходить регулярный осмотр и ремонт в течение всего жизненного цикла робота;

– он должен соответствовать четким стандартам (O'Sullivan et al., 2019), т. е. в ЕС должен применяться ряд норм в отношении минимальных стандартов, которым должен соответствовать каждый робот в своей области функционирования, не только с точки зрения качества, но и с позиций безопасности. Это требование также содержится в проекте закона о киберустойчивости.

Проект закона об ИИ содержит некоторые из этих пунктов, но не рассматривает вопросы объяснимости и интерпретируемости в важнейших областях. Фактически требования в тексте проекта, в частности в Статье 10, относятся не к объяснимости и интерпретируемости, а скорее к информации, которая должна быть представлена в технической документации о функционировании системы ИИ.

Мы считаем, что недальновидно использовать модель черного ящика, по крайней мере, в случаях, когда затрагиваются здоровье и другие фундаментальные права, но также и во всех случаях, когда экономический ущерб может быть разрушительным для благосостояния пользователей (например, настолько крупный ущерб, что пользователи лишаются дома из-за рискованных инвестиций, сделанных роботом). Более того, мы считаем, что, когда речь идет о персональных данных, модели черного ящика не отвечают принципам Общего регламента по защите данных²².

Хотя Европейский союз может ввести строгие регламенты и стандарты безопасности в дополнение к существующим регламентам (например, в медицинской области – нормы для медицинского оборудования), согласно их внутренней природе, однако модели с непрерывным обучением в течение всего жизненного цикла должны строго контролироваться во всех областях, где может возникнуть потенциальный вред для человека, даже если это создает негативные последствия для рынка. Защита пользователей (особенно пациентов, несовершеннолетних и представителей уязвимых групп населения) должна быть важнее, чем обеспечение разработки новых технологий в промышленном секторе, поскольку последнее все равно достигается научными исследованиями и государственными инвестициями. Таким образом, пресловутый сдерживающий эффект регламентов безопасности (как и правил ответственности производителя) на технологический прогресс не может считаться достаточным аргументом влияния на законодателей.

Что касается военных и других потенциально опасных устройств с ИИ, государство должно обеспечить специфичный и строгий контроль над ними, как это делается сейчас по отношению к опасным продуктам и некоторым суперкомпьютерам, для использования которых необходима лицензия, а перед утилизацией проводятся проверки данных. Такие ИИ-устройства никогда не должны выпускаться для широкой публики, не говоря уже об открытом исходном коде. Например, если бы умные роботы могли пользоваться оружием или иным образом убивать людей, а кто-то построил бы такого робота благодаря открытому исходному коду и доступу к 3D- и 4D-принтерам, то его можно было бы легко использовать для гражданской

²² Проблема соответствия моделей машинного обучения принципам Общего регламента по защите данных выходит за рамки данной статьи и будет исследована в отдельной работе в ближайшие месяцы. Вопрос интерпретируемости и объяснимости более подробно разбирается в главе нашей выходящей книги «Правовые аспекты ИИ в области биомедицины. Роль интерпретируемых моделей».

войны или совершения террористических атак, особенно учитывая, что напечатанное пластиковое оружие не опознается металлодетекторами²³ (Falletti, 2022). Такой риск должен всерьез рассматриваться государственными органами тех стран, где законодательство по контролю над оружием менее строгое.

Что касается обязательных проверок, обновления и применения патчей безопасности для минимизации риска кибератак, именно государство должно вводить строгие проверки и аудит. Для потенциально опасных устройств, таких как хирургические роботы, должна вводиться обязательная регистрация на уровне ЕС.

Учитывая все вышесказанное, в том, что касается машинного обучения, мы считаем необходимым введение специфического регулирования на общеевропейском уровне. Существующие нормы не являются адекватными для регулирования всего комплекса вопросов, которые могут возникнуть после выхода таких технологий на рынок. В частности, учитывая неоднородный характер технологий на основе машинного обучения, а также отраслевой характер их конкретного применения, представляется невозможным создание всеобъемлющего законодательства, однако целесообразно регулировать каждую отрасль по отдельности. При этом можно подчеркнуть специфику каждой отрасли (например, диагностические, хирургические, автомобильные, образовательные устройства и т. д.) и соответственно адаптировать под нее регламенты.

Как было отмечено еще в работе Amidei, затягивание принятия новых регламентов при наличии запроса рынка может привести к огромным убыткам и рискам, когда под влиянием различных факторов придется принимать несправедливые нормы и следовать им, а также к риску неравноценных норм в государствах – членах ЕС, если они будут приняты в разное время (Amidei, 2017).

К сожалению, проекты европейских законов об искусственном интеллекте и о киберустойчивости не дают удовлетворительного решения по регулированию умных роботов, поскольку не учитывают множество разнообразных аспектов в этой области.

3.2. Правила и стандарты защиты для производителей и программистов

Если производители будут вынуждены обновлять свое программное обеспечение при выявлении новых угроз, то нагрузка ляжет на компанию, а не на миллионы граждан; однако это не всегда возможно. Например, такой подход заставит компанию держать сотрудника, потому что он один знает устаревший язык программирования, или инвестировать в создание патча безопасности, используемого только в одном типе устройств. Одна из возможных исправительных мер – обязательное профессиональное обучение сотрудников (подобное тому, что требуется в Италии для регулируемых профессий согласно Декрету Президента республики № 137/2012) в области устаревших или экзотических языков программирования и обновления устаревших технологий. Однако в некоторых случаях такое решение невозможно, так как код слишком сложный (например, в области авиационной бортовой радиоэлектронной

²³ Фактически даже в тех странах, где контроль над оружием менее строг, законодатели пытаются установить запрет на самостоятельную печать оружия; этот вопрос поясняется в прессе и в нашей выходящей статье «Этические и юридические ограничения на распространение самостоятельно произведенного оружия»: <https://www.markey.senate.gov/news/press-releases/senator-markey-rep-meng-lead-colleagues-in-urging-biden-to-roll-back-trumps-deregulation-of-3d-printed-ghost-guns>

аппаратуры: полный спектр функционирования самолета-истребителя F-35 требует исходного кода длиной 24 млн строк²⁴). В других случаях закон мог бы заставить производителя заменить там, где это возможно, устаревший код на новый, тем самым устранив часть проблемы устаревания; фактически решения отказаться от конкретной технологии и прекратить выпуск обновлений часто оставляются на усмотрение производителя, даже если негативный эффект от нарушения безопасности ляжет на потребителей. То же верно и для тех решений по безопасности, которые могли бы предотвратить большое количество кибератак, но не являются обязательными для устройств из интернета вещей; например, это обязанность обновлять программное обеспечение устройства, пароли, физические части устройства, менять заложенное по умолчанию имя пользователя и пароль, требование использовать уникальный пароль для каждого устройства из интернета вещей.

Реализация подобного подхода могла бы изменить нашу экономику, возможно, замедлив технологический прогресс, но оказав положительный эффект на устойчивость развития за счет замедления устаревания умных продуктов.

Недавний пример, ярко показывающий необходимость нормативно-правового решения, которое заставило бы программистов обновлять программное обеспечение, – это уязвимость CVE-2018-13379 программного обеспечения компании Fortinet, о которой компании стало известно в 2018 г.²⁵, но обновление появилось только в мае прошлого года. Было обнаружено, что если задействован протокол безопасных соединений (SSL) сервиса виртуальной частной сети (VPN), то хакеры могут получить полномочия пользователей через обход каталога и удаленно скачать файлы системы FortiOS без авторизации. В Сеть был немедленно выложен список из более 49 тысяч VPN-адресов Fortinet FortiGate, которые могли быть атакованы хакерами.

Что касается кибербезопасности устройств, первый шаг в верном направлении был сделан установлением общей системы сертификации в Регламенте (Евросоюза) 2019/881 Европейского парламента и Совета от 17 апреля 2019 г. относительно Европейского агентства по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA), хотя в ст. 56 этого Регламента и говорится, что «сертификация кибербезопасности является добровольной». Установление обязательной сертификации на общеевропейском уровне и системы наказаний за ее неисполнение явилось бы мощным инструментом в борьбе с киберугрозами.

Другим возможным решением стало бы принуждение производителей к использованию открытого программного обеспечения, созданного и применяемого в ЕС, с перспективой правдивого предоставления информации. Этот подход благоприятен по многим причинам. Во-первых, он позволяет легко и быстро выявить дефекты и создать патчи безопасности, так как множество программистов в разных странах Евросоюза (обладающие различными знаниями) будут работать одновременно. Кроме того, если программное обеспечение создается не производителями оборудования, то они не несут ответственности за дефекты в нем, даже в рамках законодательства об ответственности производителя, однако такую ответственность могут нести страны – члены Евросоюза.

²⁴ Объяснение этой проблемы см.: <https://spectrum.ieee.org/f35-program-continues-to-struggle-with-software>

²⁵ Эта уязвимость более подробно описывается в блоге компании, которая ее обнаружила: <https://blog.orange.tw/2019/08/attacking-ssl-vpn-part-2-breaking-the-fortigate-ssl-vpn.html>

3.3. Правила защиты и стандарты для пользователей

Если по причине недостаточных знаний о степени риска или по принципу предосторожности государство запрещает устаревшую технологию (своего рода «плановое устаревание»), чтобы предотвратить использование старого оборудования, которое можно взломать (Zech, 2021), то оно перекладывает нагрузку на своих граждан, вынуждая их заменять устройства, чтобы избежать штрафов и ответственности. Таким образом, например, компания, сдающая в аренду парк беспилотных автомобилей, может обанкротиться, если не сможет вложить деньги в закупку новых машин. Это может произойти как с крупной транспортной компанией, владеющей беспилотными грузовиками, так и с отдельной семьей, пользующейся одним автомобилем.

Если, напротив, никаких запретов не существует, но бремя исполнения законов также лежит на пользователях, то большинство из них не будет иметь достаточной защиты. Фактически, даже в случае системы обязательного страхования, весьма вероятно, что большое количество людей не получит адекватной компенсации, так как одно лишь страховое покрытие не достаточно эффективно (Samu, 2014).

С точки зрения кибербезопасности, было бы опасно возлагать на пользователей ответственность за использование необновленного устройства в основном потому, что во многих ситуациях принцип ответственности неэффективен. Известно, что степень законопослушности меняется в зависимости от множества обстоятельств, среди которых личные, культурные, социальные факторы и даже возраст (Ma, 1985).

В эпоху, когда, вероятно, многие люди будут пользоваться роботами (например, беспилотными автомобилями), слишком высокими становятся риски от использования устаревших и необновленных устройств, которые могут продаваться на черном рынке тем, кто не может себе позволить новый продукт; это особенно касается ситуаций, когда эти устройства могут приводить к повреждениям и смерти. Беспилотные грузовики могут угонять и использовать для террористических атак (Gallese, 2018), угрожая множеству людей. Нежелательно позволять пользователям решать, утилизировать старый грузовик или нет. Более того, даже если ЕС введет такую систему, в любой другой стране останутся риски кибератак.

Кроме того, даже если рядовой пользователь готов подчиняться закону, он не способен диагностировать поломку или дефект и исправить его. В самом обычном случае люди, незнакомые с технологиями, будут наиболее уязвимы для атак, даже не осознавая этого. С другой стороны, продвинутые пользователи могут собрать робота в домашних условиях, используя различное программное обеспечение, даже с открытым исходным кодом, которое было опубликовано с другой целью. В этом случае программист не несет ответственности за результат постройки робота, который функционирует через некую комбинацию различного программного обеспечения; ответственным будет пользователь. Разумеется, тот же принцип должен применяться при использовании роботов, которые запрещены законом, сняты с производства или не имеют лицензии.

3.4. Сбалансированная система защищенности и стандартов

Нагрузка, налагаемая нормами безопасности и защищенности, должна распределяться на законодательном уровне между производителями, пользователями и государством, поскольку некоторые меры являются очень дорогостоящими или трудновыполнимыми для пользователей или производителей, тогда как другие для них доступны.

Как только постоянные проверки безопасности на основе анализа степени риска выявили угрозу, министерство может выпустить различные регламенты и принудить потребителей, производителей и даже государственные органы исполнять их, как этого требует ситуация. Например, если на придорожный рекламный щит помещен вредоносный цветовой патч, представляющий непосредственную угрозу для безопасности на дороге, то у производителя не будет достаточно времени, чтобы создать обновление программного обеспечения (если это вообще возможно), поэтому мэр будет обязан перекрыть движение на дороге и в течение нескольких часов удалить объект.

С другой стороны, если разработка обновлений станет обязательной для производителя, можно предусмотреть также обязательную, где это возможно, замену устаревшего программного обеспечения пользователями или регулярное прохождение технического осмотра роботов. Обязанности производителя могут устанавливаться по остаточному принципу, т. е. в тех случаях, которые не могут контролироваться ни государством, ни пользователем.

Это решение не сильно отличается от функционирования других регламентов безопасности: когда новый закон или постановление о чрезвычайной ситуации вводится, чтобы избежать угрозы здоровью, обязанность по его исполнению иногда ложится на пользователя (например, в Италии обязательное устройство, контролирующее посадку ребенка в автомобильном кресле), иногда на производителя (ст. 19 Регламента (Еврокомиссии) № 178/2002 об удалении продуктов питания с рынка). Бремя расходов на исполнение регламента может быть также смягчено через государственное финансирование и другие льготы для производителей и пользователей.

Особое внимание следует уделить в случае возможной угрозы демократии, например, обеспечения национальной безопасности (Allen & Chan, 2017) или выборов. Используемые для этих целей устройства должны регулироваться отдельной и более строгой отраслью права, а контроль над ними должен быть обязанностью государства. Мы считаем, что ни один инструмент, каким-либо образом используемый в демократическом процессе, не должен оставаться в руках частных компаний²⁶, особенно в эпоху, когда демократия и так находится под угрозой из-за злоупотреблений в области персональных (больших) данных, социальных сетей и фейковых новостей (Manheim & Kaplan, 2019; Persily, 2017; Heawood, 2018; Helbing et al., 2018).

Правила безопасности и защищенности должны применяться также для того, чтобы не позволить производителям выпустить на рынок продукты, обучающиеся в течение всего жизненного цикла, которые могут быть опасными, либо установить особые условия выпуска (обязательное страхование или лицензирование, регистрация и т. д.).

Абсолютно приемлемым является мнение о постоянном присутствии надзора со стороны человека, однако следует учитывать, что с усилением интегрированности технологий в повседневную жизнь люди все больше полагаются на них, не задумываясь о таком надзоре и фактически не осуществляя его; это явление называется ошибкой автоматизации.

²⁶ Это включает возможность распространять политические материалы и рекламу через социальные сети, приложения для смартфонов и домашние устройства, работающие на алгоритмах искусственного интеллекта, и использовать профили пользователей для влияния на их поведение. Скандал с компанией Cambridge Analytica показал насущную необходимость выработать нормативное решение для моделей ИИ, способных повлиять на демократические институты.

4. Принципы закона о киберустойчивости

Новый подход, сформулированный в проекте закона о киберустойчивости, отличается ограниченностью, поскольку он не специфичен для систем ИИ или роботов, что исключает из сферы его действия медицинские устройства, беспилотные автомобили и дроны. Однако он представляет собой важный шаг в направлении развития безопасного и защищенного рынка устройств с цифровыми элементами.

Основные требования, перечисленные в приложениях, постулируют, что такие устройства должны соответствовать ряду правил, а именно:

- включать безопасную по умолчанию конфигурацию и возможность промышленной перезагрузки;
- включать меры защиты устройства от несанкционированного доступа;
- распространять меры обеспечения конфиденциальности и целостности данных на неперсональные данные;
- распространять принципы адекватности, ограничения назначения и минимизации данных на неперсональные данные;
- применять меры киберустойчивости для сохранения существенных функций устройств;
- минимизировать влияние на доступность услуг, предоставляемых другими устройствами или сетями;
- ограничивать поверхность атаки;
- применять соответствующие сдерживающие механизмы и технологии эксплуатации для снижения влияния аварий;
- вести журналы работы;
- обеспечивать обновление систем безопасности на пять лет.

Как и закон об искусственном интеллекте, новый проект также представляет подробный список требований, таких как ведение технической документации, информирование пользователей и оценка рисков.

Предусмотрено особое ограничение для бета-продуктов: «Государства-члены не препятствуют доступу к незавершенному программному обеспечению, которое не соответствует данному Регламенту, если доступ к указанному программному обеспечению предоставляется на ограниченный период времени с целью тестирования и данное программное обеспечение несет на себе четкое указание о несоответствии данному Регламенту и предоставлении исключительно с целью тестирования». Это положение может быть распространено на устройства, разрабатываемые в исследовательских целях, хотя это не указано явным образом в основном тексте проекта.

В пункте 10 поясняется: «Для защиты инноваций или исследований данный Регламент не распространяется на бесплатное программное обеспечение и программное обеспечение с открытым исходным кодом, разрабатываемое или поставляемое вне рамок коммерческой деятельности. Это относится, в частности, к программному обеспечению, включая исходный код и модифицированные версии, которое открыто распространяется, используется, модифицируется и перераспределяется. В контексте программного обеспечения коммерческая деятельность характеризуется не только установлением цены на продукт, но также установлением цены на техническое обслуживание, предоставление программной платформы, через которую производитель монетизирует иные услуги, или использованием персональных

данных по причинам, отличным от повышения безопасности, совместимости или взаимозаменяемости программного обеспечения».

При этом термин «делать доступным на рынке» относится также к устройствам, предоставляемым бесплатно: «[делать доступным на рынке] означает любые поставки продукта с цифровыми элементами для распространения или использования на рынок Евросоюза в процессе коммерческой деятельности, будь то за плату или бесплатно», поэтому ученые, работающие в коллаборации с промышленностью, должны проявлять осторожность.

Выводы

Выработка полного и согласованного законодательства по робототехнике в Европе еще далека от завершения, учитывая быстрое развитие ИИ и многообразие типов устройств, которые могут использоваться в самых разных сферах нашей жизни. Каждая такая сфера имеет свои особенности, поэтому желательно наряду с общими законами – об искусственном интеллекте и о киберустойчивости – задействовать множество других правовых инструментов, мер, инструкций, стандартов, относящихся к различным отраслям.

Первый шаг в разработке всеобъемлющей сбалансированной отрасли права, регулирующей ИИ через закон о киберустойчивости и его нормы безопасности и защищенности, – это установление минимальных технических стандартов, которым должно соответствовать устройство с искусственным интеллектом, прежде чем попадет на рынок Евросоюза. Предотвращение кибератак в важнейших областях и защита фундаментальных прав граждан должны быть главной заботой законодателей. Закон об ИИ и закон о киберустойчивости являются первым шагом в этом направлении, однако их общие принципы не достаточно детализированы, чтобы служить руководством для программистов в их практическом применении.

После того как законодатели разрешат применять все подходящие стандарты и технические регламенты, чтобы гарантировать, что на рынок попадают только безопасные и защищенные продукты, они должны тщательно оценить, в каких случаях на рынок могут быть допущены модели, обучающиеся в течение всего жизненного цикла, и, где это возможно, оставить технологический прогресс прерогативой научных исследований и государственных институтов под центральным наблюдением стран – членов ЕС; особенно это касается опасных продуктов.

В сфере роботов на основе машинного обучения на общеевропейском уровне необходимо специальное техническое регулирование, поскольку существующие нормы неадекватны потребности в регулировании всех вопросов, которые могут возникнуть после выпуска таких устройств на рынок. В частности, учитывая разнообразие подобных технологий, в каждой отрасли должны применяться отдельные нормы. Необходимо также учитывать убытки и риски, возникающие вследствие задержки с принятием новых регламентов в ответ на потребности рынка.

Список литературы

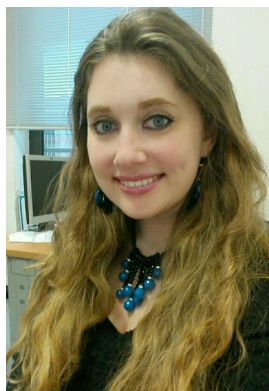
Aladin, D., Varlamov, O., Chuvikov, D., Chernenkiy, V., Smelkova, E., & Baldin, A. (2019). Logic-based artificial intelligence in systems for monitoring the enforcing traffic regulations. In *IOP Conference Series: Materials Science and Engineering* (Vol. 534, p. 012025). IOP Publishing. <https://doi.org/10.1088/1757-899x/534/1/012025>

- Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs Cambridge, MA.
- Ames, H., Mingolla, E., Sohail, A., Chandler, B., Gorchetchnikov, A., L'èveillé, J., Livitz, G., & Versace, M. (2012). The animat: New frontiers in whole brain modeling. *IEEE pulse*, 3(1), 47–50. <https://doi.org/10.1109/mpul.2011.2175638>
- Amidei, A. (2017). Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo. In U. Ruffolo (ed.), *Intelligenza Artificiale e responsabilità, Responsabilità Comunicazione Impresa* (Vol. 20, Giuffrè Editore, pp. 63–106).
- Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning*, 81(2), 121–148. <https://doi.org/10.1007/s10994-010-5188-5>
- Bekey, G. A. (2012). Current trends in robotics: Technology and ethics. In *Robot ethics: the ethical and social implications of robotics* (pp. 17–34). The MIT Press, Cambridge.
- Bertolini, A. (2013). Robots as products: the case for a realistic analysis of robotic applications and liability rules. *Law, Innovation and Technology*, 5(2), 214–247. <https://doi.org/10.5235/17579961.5.2.214>
- Bi, S. (2020). Intelligent system for English translation using automated knowledge base. *Journal of Intelligent & Fuzzy Systems*, 39(4), 5057–5066. <https://doi.org/10.3233/jifs-179991>
- Botros, N. M., & Abdul-Aziz, M. (1994). Hardware implementation of an artificial neural network using field programmable gate arrays (FPGA's). *IEEE Transactions on Industrial Electronics*, 41(6), 665–667. <https://doi.org/10.1109/41.334585>
- Buchanan, B. (2016). The life cycles of cyber threats. *Survival*, 58(1), 39–58. <https://doi.org/10.1080/00396338.2016.1142093>
- Chakkravarthy, R. (2019). Artificial intelligence for construction safety. *Professional Safety*, 64(1), 46.
- Chakraborti, T., Kulkarni, A., Sreedharan, S., Smith, D. E., & Kambhampati, S. (2021). Explicability? Legibility? Predictability? Transparency? Privacy? Security? The Emerging Landscape of Interpretable Agent Behavior. *Proceedings of the International Conference on Automated Planning and Scheduling*, 29, 86–96. <https://doi.org/10.1609/icaps.v29i1.3463>
- Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer Applications*, 115(9), 31–41. <https://doi.org/10.5120/20182-2402>
- De Swarte, T., Boufous, O., & Escalle, P. (2019). Artificial intelligence, ethics and human values: the cases of military drones and companion robots. *Artificial Life and Robotics*, 24(3), 291–296. <https://doi.org/10.1007/s10015-019-00525-1>
- Demir, K. A., Döven, G., & Sezen, B. (2019). Industry 5.0 and Human-Robot Co-working. *Procedia Computer Science*, 158, 688–695. <https://doi.org/10.1016/j.procs.2019.09.104>
- Dietterich, T. G., & Kong, E. B. (1995). *Machine learning bias, statistical bias, and statistical variance of decision tree algorithms*. Technical report, Department of Computer Science, Oregon State University.
- Dijkstra, E. W. (1982). *Selected writings on computing: a personal perspective*. Springer Science & Business Media.
- Ebers, M., & Navas, S. (2020). *Algorithms and Law*. Cambridge University Press.
- European Parliament. (2017). *European Parliament resolution of 16 February 2017 with recommendations to the commission on civil law rules on robotics (2015/2103(INL))*.
- Falletti, E. (2020). Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche. *Il diritto dell'informazione e dell'informatica*, 3, 169–206.
- Funkhouser, K. (2013). Paving the road ahead: autonomous vehicles, products liability, and the need for a new approach. *Utah Law Review*, 437.
- Gallese, C. (2018). Prospettive di riforma del diritto internazionale privato giapponese. In M. Cestari, G. Coci, D. Moro, A. Specchio (Eds.), *Orizzonti giapponesi: ricerche, idee, prospettive* (pp. 185–186). Aracne editrice, Roma.
- Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 80–89). <https://doi.org/10.1109/dsaa.2018.00018>
- Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. *Proceedings of the Annual Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/hicss.2019.258>
- Haselager, W. F. (2005). Robotics, philosophy and the problems of autonomy. *Cognitive Technologies and the Pragmatics of Cognition*, 13(3), 515–532. <https://doi.org/10.1075/pc.13.3.07has>
- Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, 23(4), 429–434. <https://doi.org/10.3233/ip-180009>
- Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R. V., & Zwitter, A. (2018). Will Democracy Survive Big Data and Artificial Intelligence? *Towards Digital Enlightenment*, 73–98. https://doi.org/10.1007/978-3-319-90869-4_7

- Hildebrandt, M. (2019). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. *Theoretical Inquiries in Law*, 20(1), 83–121. <https://doi.org/10.1515/til-2019-0004>
- Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *WIREs Data Mining and Knowledge Discovery*, 9(4). <https://doi.org/10.1002/widm.1312>
- Ielmini, D., & Ambrogio, S. (2019). Emerging neuromorphic devices. *Nanotechnology*, 31(9), 092001. <https://doi.org/10.1088/1361-6528/ab554b>
- Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15–25. <https://doi.org/10.1016/j.bushor.2018.08.004>
- Lamberton, C., Brigo, D., & Hoy, D. (2017). Impact of robotics, RPA and AI on the insurance industry: challenges and opportunities. *Journal of Financial Perspectives*, 4(1).
- Leenes, R., Palmerini, E., Koops, B. J., Bertolini, A., Salvini, P., & Lucivero, F. (2017). Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. *Law, Innovation and Technology*, 9(1), 1–44. <https://doi.org/10.1080/17579961.2017.1304921>
- Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2017). Brain Intelligence: Go beyond Artificial Intelligence. *Mobile Networks and Applications*, 23(2), 368–375. <https://doi.org/10.1007/s11036-017-0932-8>
- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), 1–9. <https://doi.org/10.3233/thc-151102>
- Ma, H. K. (1985). Cross-Cultural Study of the Development of Law-Abiding Orientation. *Psychological Reports*, 57(3), 967–974. <https://doi.org/10.2466/pr0.1985.57.3.967>
- Manheim, K. M., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law and Technology*, 21, 106–188.
- Naur, P., & Randell, B. (Eds.) (1968). *Software Engineering: Report of a conference sponsored by the NATO Science Committee*. Newcastle University.
- Nevejans, N. (2016). *European civil law rules in robotics*. Policy Department for Citizens' Rights and Constitutional Affairs.
- Nobile, M. S., Vlachou, T., Spolaor, S., Cazzaniga, P., Mauri, G., Pelicci, P. G., & Besozzi, D. (2019). ProCell: Investigating cell proliferation with Swarm Intelligence. *2019 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)* (pp. 1–8). <https://doi.org/10.1109/cibcb.2019.8791468>
- O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *The International Journal of Medical Robotics and Computer Assisted Surgery*, 15(1), e1968. <https://doi.org/10.1002/rcs.1968>
- Ozkan, B. E., & Bulkan, S. (2019). Hidden Risks to Cyberspace Security from Obsolete COTS Software. *2019 11th International Conference on Cyber Conflict (CyCon)* (pp. 1–19). <https://doi.org/10.23919/cycon.2019.8756990>
- Pan, C., Wang, C. Y., Liang, S. J., Wang, Y., Cao, T., Wang, P., Wang, C., Wang, S., Cheng, B., Gao, A., Liu, E., Watanabe, K., Taniguchi, T., & Miao, F. (2020). Reconfigurable logic and neuromorphic circuits based on electrically tunable two-dimensional homojunctions. *Nature Electronics*, 3(7), 383–390. <https://doi.org/10.1038/s41928-020-0433-9>
- Pandian, D. A. P. (2019). Artificial intelligence application in smart warehousing environment for automated logistics. *Journal of Artificial Intelligence and Capsule Networks*, 1(2), 63–72. <https://doi.org/10.36548/jaicn.2019.2.002>
- Papetti, D. M., Spolaor, S., Besozzi, D., Cazzaniga, P., Antoniotti, M., & Nobile, M. S. (2020). On the automatic calibration of fully analogical spiking neuromorphic chips. *2020 International Joint Conference on Neural Networks (IJCNN)*. <https://doi.org/10.1109/ijcnn48605.2020.9206654>
- Persily, N. (2017). Can Democracy Survive the Internet? *Journal of Democracy*, 28(2), 63–76. <https://doi.org/10.1353/jod.2017.0025>
- Ranjan, A., Janai, J., Geiger, A., & Black, M. (2019). Attacking Optical Flow. *2019 IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 2404–2413). <https://doi.org/10.1109/iccv.2019.00249>
- Rao, Q., & Frtunikj, J. (2018). Deep learning for self-driving cars. *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems* (pp. 35–38). <https://doi.org/10.1145/3194085.3194087>
- Raza, M., Awais, M., Ali, K., Aslam, N., Paranthaman, V. V., Imran, M., & Ali, F. (2020). Establishing effective communications in disaster affected areas and artificial intelligence based detection using social media platform. *Future Generation Computer Systems*, 112, 1057–1069. <https://doi.org/10.1016/j.future.2020.06.040>
- Richards, N. M., & Smart, W. D. (2016). How should the law think about robots? In R. Calo, M. A. Froomkin, I. Kerr (Eds.). *Robot law*. Edward Elgar.

- Roll, I., & Wylie, R. (2016). Evolution and Revolution in Artificial Intelligence in Education. *International Journal of Artificial Intelligence in Education*, 26(2), 582–599. <https://doi.org/10.1007/s40593-016-0110-3>
- Romanishin, J. W., Gilpin, K., & Rus, D. (2013). M-blocks: Momentum-driven, magnetic modular robots. *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems* (pp. 4288–4295). <https://doi.org/10.1109/iros.2013.6696971>
- Rundo, L., Tangherloni, A., Nobile, M. S., Militello, C., Besozzi, D., Mauri, G., & Cazzaniga, P. (2019). MedGA: A novel evolutionary method for image enhancement in medical imaging systems. *Expert Systems With Applications*, 119, 387–399. <https://doi.org/10.1016/j.eswa.2018.11.013>
- Samu, S. (2014). The effectiveness of compulsory motor insurance in Zimbabwe. *Journal of Strategic Studies: A Journal of the Southern Bureau of Strategic Studies Trust*, 5(1), 45–60.
- Santosuosso, A., Boscarato, C., & Caroleo, F. (2012). Robot e diritto: una prima ricognizione. *La Nuova Giurisprudenza Commentata*, 494.
- Simoens, P., Mahieu, C., Ongenae, F., De Backere, F., De Pestel, S., Nelis, J., De Turck, F., Elprama, S. A., Kilpi, K., Jewell, C., & Jacobs, A. (2016). Internet of Robotic Things: Context-Aware and Personalized Interventions of Assistive Social Robots (Short Paper). *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)* (pp. 204–207). <https://doi.org/10.1109/cloudnet.2016.27>
- Smith, B. Walker (2016). Lawyers and engineers should speak the same robot language. In R. Calo, M. A. Froomkin, I. Kerr (Eds.), *Robot law* (pp. 78–101). Edward Elgar Publishing.
- Sourdin, T. (2018). Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *University of New South Wales Law Journal*, 41(4), 25167–25177. <https://doi.org/10.53637/zgux2213>
- Wang, W., & Siau, K. (2019). Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity. *Journal of Database Management*, 30(1), 61–79. <https://doi.org/10.4018/jdm.2019010104>
- Yano, K. (2017). How artificial intelligence will change HR. *People & Strategy*, 40(3), 42–47.
- Yuniarthe, Y. (2017). Application of Artificial Intelligence (AI) in Search Engine Optimization (SEO). In *2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIIT)* (pp. 96–101). <https://doi.org/10.1109/icsiit.2017.15>
- Zech, H. (2021). Liability for AI: public policy considerations. *ERA Forum*, 22(1), 147–158. <https://doi.org/10.1007/s12027-020-00648-0>
- Zhang, X., Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, 32, 300926. <https://doi.org/10.1016/j.fsidi.2020.300926>

Сведения об авторе



Галлезе-Нобиле Кьяра – доктор наук, научный сотрудник (постдок) по управлению исследовательскими данными, Эйндховенский технологический университет (Эйндховен, Королевство Нидерландов); научный сотрудник (постдок) департамента математики и наук о земле, Университет Триеста (Триест, Итальянская Республика)

Адрес: а/я 513 5600 МБ Эйндховен, Королевство Нидерландов

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57222726276>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/AGE-9594-2022>

ORCID ID: <https://orcid.org/0000-0001-8194-0261>

Google Scholar ID: <https://scholar.google.com/citations?user=Vmoen8UAAAAJ>

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование выполнено при поддержке проекта UNI 4 JUSTICE.

История статьи

Дата поступления – 13 октября 2022 г.

Дата одобрения после рецензирования – 4 ноября 2022 г.

Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.2>



Regulating Smart Robots and Artificial Intelligence in the European Union

Chiara Gallese Nobile 

Eindhoven University of Technology
Eindhoven, Kingdom of the Netherlands;
University of Trieste
Trieste, Italian Republic

Keywords

Artificial intelligence,
cybersecurity,
digital technologies,
European Union,
law,
legislation,
machine learning,
regulation,
robot,
robotics

Abstract

Objective: In recent years, the need for regulation of robots and Artificial Intelligence has become apparent in Europe. European Union needs a standardized regulation that will ensure a high level of security in robotics systems to prevent potential breaches. Therefore a new regulation should make clear that it is the responsibility of producers to identify the blind spots in these systems, exposing their flaws, or, when a vulnerability is discovered in a later stage, to update the system even if that model is not on the market anymore. This article aims at suggesting some possible revisions of the existing legal provisions in the EU.

Methods: The author employed the Kestemont legal methodology, analyzing legal text, comparing them, and connecting them with technical elements regarding smart robots, resulting in the highlighting of the critical provisions to be updated

Results: This article suggests some revisions to the existing regulatory proposals: according to the author, although the AI Act and the Cyber-resilience Act represent a first step towards this direction, their general principles are not sufficiently detailed to guide programmers on how to implement them in practice, and policymakers should carefully assess in what cases lifelong learning models should be allowed to the market. The author suggests that the current proposal regarding mandatory updates should be expanded, as five years are a short time frame that would not cover the risks associated with long-lasting products, such as vehicles.

© Gallese Nobile C., 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 author has examined the existing regulatory framework regarding AI systems and devices with digital elements, highlighted the risks of the current legal framework, and suggested possible amendments to the existing regulatory proposals

Practical significance: The article can be employed to update the existing proposals for the AI Act and the Cyber-resilience Act

For citation

Gallese Nobile, C. (2023). Regulating Smart Robots and Artificial Intelligence in the European Union. *Journal of Digital Technologies and Law*, 1(1), 33–61. <https://doi.org/10.21202/jdtl.2023.2>

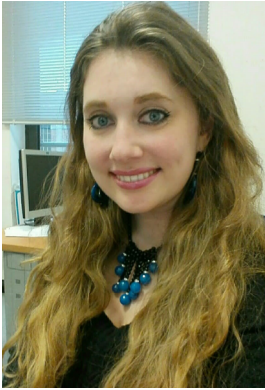
References

- Aladin, D., Varlamov, O., Chuvikov, D., Chernenkiy, V., Smelkova, E., & Baldin, A. (2019). Logic-based artificial intelligence in systems for monitoring the enforcing traffic regulations. In *IOP Conference Series: Materials Science and Engineering* (Vol. 534, p. 012025). IOP Publishing. <https://doi.org/10.1088/1757-899x/534/1/012025>
- Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs Cambridge, MA.
- Ames, H., Mingolla, E., Sohail, A., Chandler, B., Gorchetchnikov, A., L'èveillé, J., Livitz, G., & Versace, M. (2012). The animat: New frontiers in whole brain modeling. *IEEE pulse*, 3(1), 47–50. <https://doi.org/10.1109/mpul.2011.2175638>
- Amidei, A. (2017). Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo. In U. Ruffolo (ed.), *Intelligenza Artificiale e responsabilità, Responsabilità Comunicazione Impresa* (Vol. 20, Giuffrè Editore, pp. 63–106).
- Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning*, 81(2), 121–148. <https://doi.org/10.1007/s10994-010-5188-5>
- Bekey, G. A. (2012). Current trends in robotics: Technology and ethics. In *Robot ethics: the ethical and social implications of robotics* (pp. 17–34). The MIT Press, Cambridge.
- Bertolini, A. (2013). Robots as products: the case for a realistic analysis of robotic applications and liability rules. *Law, Innovation and Technology*, 5(2), 214–247. <https://doi.org/10.5235/17579961.5.2.214>
- Bi, S. (2020). Intelligent system for English translation using automated knowledge base. *Journal of Intelligent & Fuzzy Systems*, 39(4), 5057–5066. <https://doi.org/10.3233/jifs-179991>
- Botros, N. M., & Abdul-Aziz, M. (1994). Hardware implementation of an artificial neural network using field programmable gate arrays (FPGA's). *IEEE Transactions on Industrial Electronics*, 41(6), 665–667. <https://doi.org/10.1109/41.334585>
- Buchanan, B. (2016). The life cycles of cyber threats. *Survival*, 58(1), 39–58. <https://doi.org/10.1080/00396338.2016.1142093>
- Chakkravarthy, R. (2019). Artificial intelligence for construction safety. *Professional Safety*, 64(1), 46.
- Chakraborti, T., Kulkarni, A., Sreedharan, S., Smith, D. E., & Kambhampati, S. (2021). Explicability? Legibility? Predictability? Transparency? Privacy? Security? The Emerging Landscape of Interpretable Agent Behavior. *Proceedings of the International Conference on Automated Planning and Scheduling*, 29, 86–96. <https://doi.org/10.1609/icaps.v29i1.3463>
- Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer Applications*, 115(9), 31–41. <https://doi.org/10.5120/20182-2402>
- De Swarte, T., Boufous, O., & Escalle, P. (2019). Artificial intelligence, ethics and human values: the cases of military drones and companion robots. *Artificial Life and Robotics*, 24(3), 291–296. <https://doi.org/10.1007/s10015-019-00525-1>
- Demir, K. A., Döven, G., & Sezen, B. (2019). Industry 5.0 and Human-Robot Co-working. *Procedia Computer Science*, 158, 688–695. <https://doi.org/10.1016/j.procs.2019.09.104>
- Dietterich, T. G., & Kong, E. B. (1995). *Machine learning bias, statistical bias, and statistical variance of decision tree algorithms*. Technical report, Department of Computer Science, Oregon State University.

- Dijkstra, E. W. (1982). *Selected writings on computing: a personal perspective*. Springer Science & Business Media.
- Ebers, M., & Navas, S. (2020). *Algorithms and Law*. Cambridge University Press.
- European Parliament. (2017). *European Parliament resolution of 16 February 2017 with recommendations to the commission on civil law rules on robotics (2015/2103(INL))*.
- Falletti, E. (2020). Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche. *Il diritto dell'informazione e dell'informatica*, 3, 169–206.
- Funkhouser, K. (2013). Paving the road ahead: autonomous vehicles, products liability, and the need for a new approach. *Utah Law Review*, 437.
- Gallese, C. (2018). Prospettive di riforma del diritto internazionale privato giapponese. In M. Cestari, G. Coci, D. Moro, A. Specchio (Eds.), *Orizzonti giapponesi: ricerche, idee, prospettive* (pp. 185–186). Aracne editrice, Roma.
- Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 80–89). <https://doi.org/10.1109/dsaa.2018.00018>
- Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. *Proceedings of the Annual Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/hicss.2019.258>
- Haselager, W. F. (2005). Robotics, philosophy and the problems of autonomy. *Cognitive Technologies and the Pragmatics of Cognition*, 13(3), 515–532. <https://doi.org/10.1075/pc.13.3.07has>
- Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, 23(4), 429–434. <https://doi.org/10.3233/ip-180009>
- Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R. V., & Zwitter, A. (2018). Will Democracy Survive Big Data and Artificial Intelligence? *Towards Digital Enlightenment*, 73–98. https://doi.org/10.1007/978-3-319-90869-4_7
- Hildebrandt, M. (2019). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. *Theoretical Inquiries in Law*, 20(1), 83–121. <https://doi.org/10.1515/til-2019-0004>
- Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *WIREs Data Mining and Knowledge Discovery*, 9(4). <https://doi.org/10.1002/widm.1312>
- Ielmini, D., & Ambrogio, S. (2019). Emerging neuromorphic devices. *Nanotechnology*, 31(9), 092001. <https://doi.org/10.1088/1361-6528/ab554b>
- Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15–25. <https://doi.org/10.1016/j.bushor.2018.08.004>
- Lamberton, C., Brigo, D., & Hoy, D. (2017). Impact of robotics, RPA and AI on the insurance industry: challenges and opportunities. *Journal of Financial Perspectives*, 4(1).
- Leenes, R., Palmerini, E., Koops, B. J., Bertolini, A., Salvini, P., & Lucivero, F. (2017). Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. *Law, Innovation and Technology*, 9(1), 1–44. <https://doi.org/10.1080/17579961.2017.1304921>
- Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2017). Brain Intelligence: Go beyond Artificial Intelligence. *Mobile Networks and Applications*, 23(2), 368–375. <https://doi.org/10.1007/s11036-017-0932-8>
- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), 1–9. <https://doi.org/10.3233/thc-151102>
- Ma, H. K. (1985). Cross-Cultural Study of the Development of Law-Abiding Orientation. *Psychological Reports*, 57(3), 967–974. <https://doi.org/10.2466/pr0.1985.57.3.967>
- Manheim, K. M., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law and Technology*, 21, 106–188.
- Naur, P., & Randell, B. (Eds.) (1968). *Software Engineering: Report of a conference sponsored by the NATO Science Committee*. Newcastle University.
- Nevejans, N. (2016). *European civil law rules in robotics*. Policy Department for Citizens' Rights and Constitutional Affairs.
- Nobile, M. S., Vlachou, T., Spolaor, S., Cazzaniga, P., Mauri, G., Pelicci, P. G., & Besozzi, D. (2019). ProCell: Investigating cell proliferation with Swarm Intelligence. *2019 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)* (pp. 1–8). <https://doi.org/10.1109/cibcb.2019.8791468>
- O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *The International Journal of Medical Robotics and Computer Assisted Surgery*, 15(1), e1968. <https://doi.org/10.1002/rcs.1968>

- Ozkan, B. E., & Bulkan, S. (2019). Hidden Risks to Cyberspace Security from Obsolete COTS Software. *2019 11th International Conference on Cyber Conflict (CyCon)* (pp. 1–19). <https://doi.org/10.23919/cycon.2019.8756990>
- Pan, C., Wang, C. Y., Liang, S. J., Wang, Y., Cao, T., Wang, P., Wang, C., Wang, S., Cheng, B., Gao, A., Liu, E., Watanabe, K., Taniguchi, T., & Miao, F. (2020). Reconfigurable logic and neuromorphic circuits based on electrically tunable two-dimensional homojunctions. *Nature Electronics*, 3(7), 383–390. <https://doi.org/10.1038/s41928-020-0433-9>
- Pandian, D. A. P. (2019). Artificial intelligence application in smart warehousing environment for automated logistics. *Journal of Artificial Intelligence and Capsule Networks*, 1(2), 63–72. <https://doi.org/10.36548/jaicn.2019.2.002>
- Papetti, D. M., Spolaor, S., Besozzi, D., Cazzaniga, P., Antoniotti, M., & Nobile, M. S. (2020). On the automatic calibration of fully analogical spiking neuromorphic chips. *2020 International Joint Conference on Neural Networks (IJCNN)*. <https://doi.org/10.1109/ijcnn48605.2020.9206654>
- Persily, N. (2017). Can Democracy Survive the Internet? *Journal of Democracy*, 28(2), 63–76. <https://doi.org/10.1353/jod.2017.0025>
- Ranjan, A., Janai, J., Geiger, A., & Black, M. (2019). Attacking Optical Flow. *2019 IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 2404–2413). <https://doi.org/10.1109/iccv.2019.00249>
- Rao, Q., & Frtunikj, J. (2018). Deep learning for self-driving cars. *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems* (pp. 35–38). <https://doi.org/10.1145/3194085.3194087>
- Raza, M., Awais, M., Ali, K., Aslam, N., Paranthaman, V. V., Imran, M., & Ali, F. (2020). Establishing effective communications in disaster affected areas and artificial intelligence based detection using social media platform. *Future Generation Computer Systems*, 112, 1057–1069. <https://doi.org/10.1016/j.future.2020.06.040>
- Richards, N. M., & Smart, W. D. (2016). How should the law think about robots? In R. Calo, M. A. Froomkin, I. Kerr (Eds.). *Robot law*. Edward Elgar.
- Roll, I., & Wylie, R. (2016). Evolution and Revolution in Artificial Intelligence in Education. *International Journal of Artificial Intelligence in Education*, 26(2), 582–599. <https://doi.org/10.1007/s40593-016-0110-3>
- Romanishin, J. W., Gilpin, K., & Rus, D. (2013). M-blocks: Momentum-driven, magnetic modular robots. *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems* (pp. 4288–4295). <https://doi.org/10.1109/iro.2013.6696971>
- Rundo, L., Tangherloni, A., Nobile, M. S., Militello, C., Besozzi, D., Mauri, G., & Cazzaniga, P. (2019). MedGA: A novel evolutionary method for image enhancement in medical imaging systems. *Expert Systems With Applications*, 119, 387–399. <https://doi.org/10.1016/j.eswa.2018.11.013>
- Samu, S. (2014). The effectiveness of compulsory motor insurance in Zimbabwe. *Journal of Strategic Studies: A Journal of the Southern Bureau of Strategic Studies Trust*, 5(1), 45–60.
- Santosuosso, A., Boscarato, C., & Caroleo, F. (2012). Robot e diritto: una prima ricognizione. *La Nuova Giurisprudenza Commentata*, 494.
- Simoens, P., Mahieu, C., Ongenae, F., De Backere, F., De Pestel, S., Nelis, J., De Turck, F., Elprama, S. A., Kilpi, K., Jewell, C., & Jacobs, A. (2016). Internet of Robotic Things: Context-Aware and Personalized Interventions of Assistive Social Robots (Short Paper). *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)* (pp. 204–207). <https://doi.org/10.1109/cloudnet.2016.27>
- Smith, B. Walker (2016). Lawyers and engineers should speak the same robot language. In R. Calo, M. A. Froomkin, I. Kerr (Eds.), *Robot law* (pp. 78–101). Edward Elgar Publishing.
- Sourdin, T. (2018). Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *University of New South Wales Law Journal*, 41(4), 25167–25177. <https://doi.org/10.53637/zgux2213>
- Wang, W., & Siau, K. (2019). Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity. *Journal of Database Management*, 30(1), 61–79. <https://doi.org/10.4018/jdm.2019010104>
- Yano, K. (2017). How artificial intelligence will change HR. *People & Strategy*, 40(3), 42–47.
- Yuniarthe, Y. (2017). Application of Artificial Intelligence (AI) in Search Engine Optimization (SEO). In *2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIT)* (pp. 96–101). <https://doi.org/10.1109/icsit.2017.15>
- Zech, H. (2021). Liability for AI: public policy considerations. *ERA Forum*, 22(1), 147–158. <https://doi.org/10.1007/s12027-020-00648-0>
- Zhang, X., Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, 32, 300926. <https://doi.org/10.1016/j.fsidi.2020.300926>

Author information



Chiara Gallese Nobile – PhD, Researcher (postdoc) of research data management, Eindhoven University of Technology (Eindhoven, the Netherlands), Researcher (postdoc) of the Department of Mathematics and Geosciences at the University of Trieste (Trieste, Italy).

Address: P/O 513 5600 MB Eindhoven, the Netherlands

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57222726276>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/AGE-9594-2022>

ORCID ID: <https://orcid.org/0000-0001-8194-0261>

Google Scholar ID: <https://scholar.google.com/citations?user=Vmoen8UAAAAJ>

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research has been funded by the UNI 4 JUSTICE project.

Article history

Date of receipt – October 13, 2022

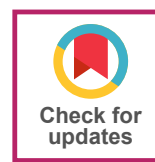
Date of approval – November 4, 2022

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 34:530.145:004
EDN: <https://elibrary.ru/fkawrt>
DOI: <https://doi.org/10.21202/jdtl.2023.3>



Квантовое право: начало

Елизавета Александровна Громова  

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Сергей Анатольевич Петренко 

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
имени В. И. Ульянова (Ленина)
г. Санкт-Петербург, Российская Федерация;
Университет Иннополис
г. Иннополис, Российская Федерация

Ключевые слова

Квант,
квантовое право,
квантовые вычисления,
квантовые технологии,
право,
регулирование,
риск,
цифровые технологии,
экспериментальные
правовые режимы,
этика

Аннотация

Цель: на основании изучения свойств квантовых явлений и особенностей квантовых технологий, обусловивших риски и вызовы, связанные с появлением данных технологий, а также анализа правового регулирования квантовых технологий в Российской Федерации и зарубежных странах формирование основ квантового права как права будущего.

Методы: для проведения данного исследования применялся комплекс общенаучных методов системного анализа, а также предметных методов технических и юридических наук. Применение сравнительно-правового метода дало возможность выявить основные направления развития регулирования квантовых технологий в российских и зарубежных правовых порядках. Метод правового моделирования позволил сформировать концепт квантового права, выявить основные векторы его развития и комплекс его этико-правовых принципов.

Результаты: выявлены особенности и свойства квантовых технологий, которые способны изменить развитие права с приходом таких технологий; определены основные риски и вызовы, связанные с развитием квантовых технологий; выявлены особенности регулирования квантовых технологий в отдельных зарубежных странах; определены тенденции развития регулирования квантовых технологий в Российской Федерации; сформированы концептуальные основы квантового права, а также векторы его развития.

 Контактное лицо

© Громова Е. А., Петренко 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.

Научная новизна: впервые в юридической науке проводится комплексный анализ существующего национального (как российского, так и зарубежного) регулирования квантовых технологий, на основании которого предпринимается попытка обоснования необходимости формирования квантового права и очерчиваются основные векторы его развития.

Практическая значимость: результаты проведенного исследования закладывают основу для формирования концепта квантового права, в связи с чем выводы, к которым пришли авторы, и выдвинутые ими предложения по совершенствованию существующего регулирования квантовых технологий могут быть использованы для правотворчества и правоприменения в данной сфере, а также способны заложить основы дальнейших исследований в области квантовых технологий.

Для цитирования

Громова, Е. А., Петренко, С. А. (2023). Квантовое право: начало. *Journal of Digital Technologies and Law*, 1(1), 62–88. <https://doi.org/10.21202/jdtl.2023.3>

Содержание

Введение

1. Текущий уровень развития квантовых технологий

- 1.1. Особенности квантовых явлений и их основные свойства
- 1.2. Основные направления развития квантовых технологий
- 1.3. Вызовы и риски, связанные с появлением квантовых технологий

2. Регулирование квантовых технологий

- 2.1. Регулирование квантовых технологий за рубежом
- 2.2. Регулирование квантовых технологий в Российской Федерации

3. На пути к квантовому праву

- 3.1. Общие векторы формирования квантового права
 - 3.1.1. От детерминизма к вероятностям в праве – смена правовой парадигмы
 - 3.1.2. Проецирование свойств квантовых явлений на регулирование общественных отношений
 - 3.1.3. Поиск «квантового» уровня права и его следствия
- 3.2. Регуляторные песочницы и иные специальные режимы как составляющие квантового права

4. Этика квантов

- 4.1. Базовые этические принципы, применимые к квантовым технологиям
- 4.2. Специальные этические принципы развития и применения квантовых технологий

Выводы

Список литературы

Всё чудесатее и чудесатее!

Льюис Кэрролл.

Приключения Алисы в Стране чудес

Введение

Плоды научно-технического прогресса уже не раз вызывали наше изумление. Однако даже среди цифровых технологических новшеств квантовые технологии стоят особняком. Потенциал данных технологий еще полностью не раскрыт, а свойства не изучены до конца. Кроме того, их внедрение и распространение смогут оказать существенное влияние на будущее человечества, наверное, гораздо более существенное, чем развитие искусственного интеллекта. Однако наиболее важная особенность, даже уникальность квантовых технологий заключается в их физической (природной) сущности, основанной на законах и явлениях квантовой механики (квантовых эффектах) (Arndt et al., 2011; Холодная, 2022).

Ключевые свойства квантовых технологий уже изменили наш привычный мир. Так, открытие квантовой механики и ее основные достижения, ставшие одной из причин смены технологического уклада и первой квантовой революции, существенно повлияли на уровень нашей жизни. Возможность управления коллективными квантовыми явлениями позволила создать ускорители частиц, ядерное оружие, лазеры, транзисторы и др.

Сегодня мы находимся на пороге второй квантовой революции, в основе которой находятся три обладающие значительным потенциалом квантовые субтехнологии: квантовые вычисления, квантовая криптография и квантовая сенсорика и метрология. Так, например, возможность осуществления квантовых вычислений является одним из ожидаемых и прогнозируемых событий в научном мире. Данный способ вычислений позволит выполнять вероятностные расчеты такой сложности, которая недоступна современным суперкомпьютерам.

Развитие квантовых технологий будет способствовать прорывам во многих сферах: от военно-промышленного комплекса и автомобилестроения до медицины и исследований космоса. Отмеченный потенциал квантовых технологий обусловил начало квантовой гонки многих государств на пути к квантовому превосходству.

Именно поэтому одной из важнейших задач каждого государства является адекватное и максимально эффективное урегулирование создания, внедрения и коммерциализации таких технологий. Очевидно, что поиск решения указанной задачи не будет легким. Инновационная природа большинства цифровых технологий уже обусловила понимание того факта, что право устаревает и регулирование общественных отношений требует его трансформации и адаптации. А если мы говорим о квантовых технологиях, то их свойства способны существенно повлиять на развитие общественных отношений, и от этого стоящая перед правом задача еще больше усложняется, и в будущем возможно формирование нового «квантового» права.

На сегодняшний день квантовые технологии находятся в фокусе внимания мирового научного сообщества. Значительное число исследований опубликовано представителями технических наук как за рубежом (Belenchia et al., 2022; Ball, 2021; Browne et al., 2017; Chen et al., 2021; Kearney & Perez-Delgado, 2020; Kumar et al., 2022; Mosca, 2018; Taylor, 2020), так и в Российской Федерации (Sigov et al., 2020; Petrenko, 2022).

Представители юридической науки также не обходят стороной квантовые технологии. Обращает на себя внимание тот факт, что зарубежные исследователи активно разрабатывают концепт квантового вычислительного права (Atik, 2022; Ritter, 2015), или же этики квантовых технологий (Atik & Jeutner, 2021; Jeutner, 2021), или исследуют правовые аспекты применения квантовых технологий в отдельных областях юриспруденции (Yanamadala & Seema, 2022). В то время как российские ученые сосредоточились на выработке понятийно-категориального аппарата в сфере квантовых технологий, а также создания основ правового регулирования данных технологий и особенностей их регулирования в России на современном этапе (Холодная, 2022; Добробаба и др., 2022; Наумов и Станковский, 2019).

Отметим, что за рамками исследований остался комплексный анализ существующего международного, национального (как российского, так и зарубежного) регулирования квантовых технологий, а также определение таких особенностей квантовых технологий, которые являются причиной необходимости формирования квантового права.

В этой связи целью данного исследования стала попытка формирования концепта квантового права как права будущего.

Задачами исследования стали:

- 1) изучение свойств и особенностей квантовых технологий;
- 2) определение угроз, рисков и вызовов, связанных с развитием квантовых технологий;
- 3) выявление особенностей регулирования данных технологий в зарубежных странах;
- 4) анализ регулирования квантовых технологий в России;
- 5) формирование основных векторов развития квантового права.

Для проведения исследования применялся комплекс общенаучных методов, а также методов научного познания, применяемых в технических и юридических науках.

Методами, положенными в основу технической (инженерной) составляющей исследования, стали: методы системного анализа, методы квантовой механики, а также модели и методы дискретной математики и программотехники.

Методами, положенными в основу юридической составляющей исследования, стали сравнительно-правовой и метод правового моделирования. Применение сравнительно-правового метода дало возможность выявить основные направления развития правового регулирования квантовых технологий в российских и зарубежных правовых системах на основе анализа международного и национального регулирования квантовых технологий. Метод правового моделирования позволил сформировать концепт квантового права как права будущего, выявить основные векторы его развития и комплекс его эτικο-правовых принципов.

1. Текущий уровень развития квантовых технологий

1.1. Особенности квантовых явлений и их основные свойства

Центральным термином в сфере квантовых технологий является квантовый бит, или кубит. Кубитом может стать практически любая квантовая система (обладающая как минимум двумя состояниями). При этом квантовые состояния записываются как $|0\rangle$ и $|1\rangle$ (Дирак, 1979) (рис. 1).

Заметим, что общее состояние такой системы с двумя состояниями может быть представлено суперпозицией базисных состояний (рис. 1) (С. А. Петренко и др., 2021).

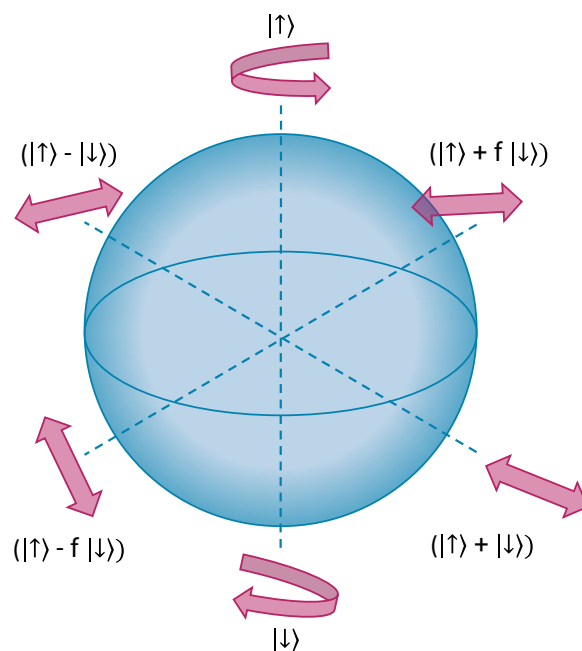


Рисунок 1. Состояния кубита

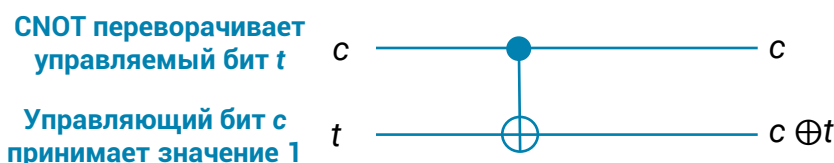
Источник: (С. А. Петренко и др., 2021).

Регистр, составленный из L двухуровневых кубитов, может хранить одновременно до 2^L чисел в квантовой суперпозиции. Соответственно, если пополнить регистр дополнительными кубитами, это повлечет экспоненциальное увеличение объема хранимой информации в регистре.

Так, в качестве примера можно привести 250-кубитный регистр, обладающий атомарными размерами, который способен хранить больше чисел, чем существует атомов во Вселенной.

Указанное позволяет сформулировать еще одну исключительную особенность квантового вычисления: используя только операцию суперпозиции, можно выполнить серию математических операций, каждая из которых оперирует всеми хранимыми данными одновременно (С. А. Петренко и др., 2021).

Под квантовым алгоритмом вычислений обычно понимается ряд последовательных унитарных операций. При этом операции будут всегда выполняться согласно ранее определенному порядку. Это подразумевает отсутствие известного логического условия «IF...THEN», применение которого позволяет нам изменить порядок вычисления. Вместо этого существуют условные операции, реализуемые гейтом CNOT (рис. 2) (Duplij & Shapoval, 2007).



Действие элемента CNOT

$|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |10\rangle$

Рисунок 2. Применение гейта (оператора) CNOT

Источник: (С. А. Петренко и др., 2021).

Указанное предопределило возможность сформулировать ряд базовых принципов создания «святого Грааля» квантовой теории – квантового компьютера: а) кубит может быть инициализирован в известном состоянии (например, состоянии $|0\rangle$); б) он также может быть измерен в базисе $\{|0\rangle, |1\rangle\}$; в) универсальный квантовый гейт может воздействовать на любое ограниченное подмножество кубитов; г) состояние кубитов может быть изменено исключительно посредством указанных выше преобразований. По мнению ряда ученых, квантовые компьютеры смогут решать ряд вычислительных задач значительно эффективнее по сравнению с классическими (Duplij & Shapoval, 2007).

Однако пока что весьма сложно удерживать кубиты в относительно стабильном (когерентном) состоянии, поскольку любое взаимодействие системы с внешним миром ведет к потере когерентности (декогеренции), а следовательно, к аварийному завершению работы компьютера. Этот эффект приводит к нарушению квантовых шагов вычисления, что в свою очередь делает невыполнимым требование о неизменяемости состояния квантовой системы (Deutsch & Jozsa, 1992), так как не существует идеального квантового гейта, а также полностью изолированной системы. Сконструировать квантовую систему, в которой потеря когерентности имела бы место реже одного раза на миллион применений гейта XOR, оказалось достаточно сложной инженерной задачей. По мнению ученых, еще только предстоит узнать, позволяют ли законы физики найти нижний предел скорости потери когерентности (Deutsch & Jozsa, 1992; Shor, 1994; Shor, 1999; А. С. Петренко и др., 2021).

1.2. Основные направления развития квантовых технологий

В настоящее время к основным направлениям развития квантовых технологий относятся технологии, показанные на рис. 3.

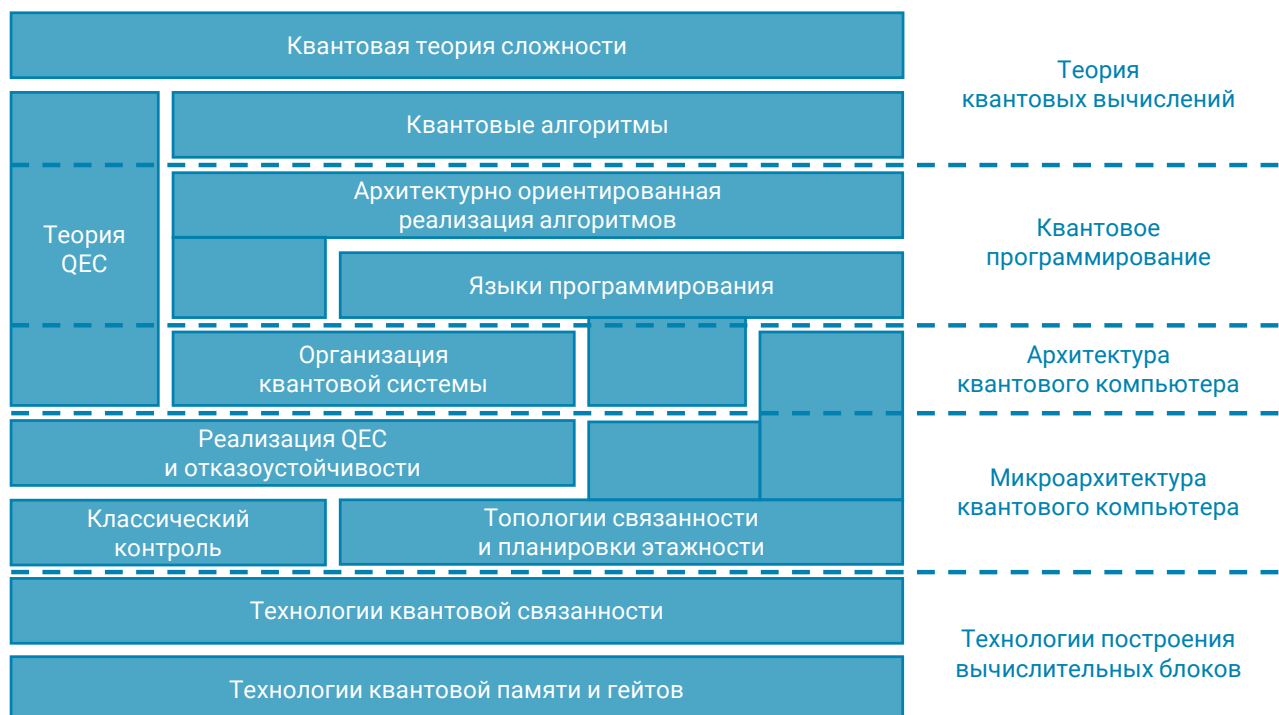


Рисунок 3. Основные направления развития квантовых технологий

Источник: (С. А. Петренко и др., 2021).

Наибольшую популярность имеют такие направления развития квантовых технологий, как квантовые компьютеры, квантовая сенсорика и метрология, а также квантовая (постквантовая) криптография. Поскольку о квантовых компьютерах было сказано выше, следует остановиться на двух других важных направлениях развития квантовых технологий.

Так, развитие такого направления, как квантовая сенсорика и метрология, обусловлено способностью квантовых сенсоров осуществлять высокоточные, а в перспективе и высокочувствительные измерения. Появление таких сенсоров позволит совершить прорывы в области медицины, обороны и безопасности, нефтедобычи и строительства, а также создания совершенных навигационных систем.

Постквантовая криптография является одним из наиболее востребованных направлений в сфере развития квантовых технологий. Идея создания шифра, который невозможно будет взломать, владеет умами ученых довольно давно. Именно поэтому квантовая криптография как направление исследований находится под пристальным вниманием большинства современных государств. При этом заметим, что ученые условно разделяют квантовую криптографию на квантово-безопасную и квантово-небезопасную (А. С. Петренко и др., 2021). Следует отметить, что в отдельных странах, в частности Соединенных Штатах Америки (далее – США) и странах Европейского союза (далее – ЕС), планируется переход к устойчивой постквантовой криптографии уже в 2025 г. (А. С. Петренко и др., 2021).

1.3. Вызовы и риски, связанные с появлением квантовых технологий

Основными вызовами, которые поставили перед правом квантовые технологии, являются следующие.

Во-первых, это вызовы современной экономике, связанные с проблемой наличия финансовых ресурсов. Так, гонка в борьбе за квантовое превосходство потребует от государств аккумулирования средств для развития таких технологий внутри страны, что может быть проблематичным в современных экономических условиях.

Во-вторых, это вызов системе национальной безопасности государства. Дело в том, что появление таких технологий у одной страны станет угрозой национальной безопасности для других. И это, в свою очередь, потребует адекватных и «симметричных» ответов, которые можно будет дать лишь в том случае, если государство будет обладать квантовыми технологиями аналогичного или более высокого уровня развития.

В-третьих, появление квантовых технологий повлечет за собой увеличение цифровых разрывов между теми, кто владеет квантовыми технологиями, и теми, кто таковыми не обладает, что в итоге может привести к усилению неравенства. Это также станет глобальным вызовом и потребует от государств совместного поиска решений указанной проблемы.

Следует также выделить риски, которые могут повлечь за собой создание и распространение квантовых технологий. Таковыми являются риски:

- 1) дестабилизации мировой финансовой системы;
- 2) нарушения конфиденциальности и безопасности данных;
- 3) утраты доверия к новым технологиям;
- 4) распространения фальшивых новостей, дезинформации и их влияния на демократические процессы;
- 5) повышения правовой неопределенности;
- 6) негативных изменений геополитических отношений.

2. Регулирование квантовых технологий

Как отмечалось выше, квантовые технологии находятся в фокусе особого внимания современных государств. Большинство из них активно включились в квантовую гонку и стремятся создать благоприятные условия, необходимые для эффективного развития таких технологий.

2.1. Регулирование квантовых технологий за рубежом

Китайская Народная Республика. В Национальном плане «Сделано в Китае 2025» (далее – Национальный план)¹, а также в текущем 14-м пятилетнем плане социально-экономического развития Китая (2021–2025 гг.)² объявлено о «крупных прорывах», в том числе в сфере квантовых технологий. Согласно Национальному плану, это будет возможно за счет систематического «наращивания мозгов», развития многочисленных национальных инновационных проектов, создания лабораторий³. Государственное финансирование позволит достигнуть значительных успехов в развитии квантовых технологий, что сделает китайскую технологическую промышленность лидером мирового рынка. Финансирование направлено преимущественно на коммерциализацию технологий квантовой связи, а также квантового распределения ключей и интерферометрии холодных атомов (табл. 1).

Европейский союз. В мае 2016 г. ЕС анонсировал запуск масштабной программы – Инициативы квантового лидерства (Quantum Flagship Initiative)⁴. Указанный документ предполагает как проведение исследований в сфере квантовых технологий, так и организацию и проведение масштабного комплекса действий, направленных на тестирование и апробацию квантовых технологий. При этом сумма финансирования, установленная Европейской комиссией, составила 1 млрд евро⁵.

Следует отметить, что основные направления деятельности в области развития квантовых технологий в ЕС детально описаны в Квантовом манифесте 2016 г.⁶ Отмечается, что в 2016–2017 гг. более 3400 частных компаний из различных стран ЕС присоединились к Манифесту⁷. Для таких компаний предусмотрена возможность участия в процессе создания и развития квантовых технологий в форме государственно-частного партнерства, а также грантов и др.

¹ *Made In China 2025: The Plan to Dominate Manufacturing and High-Tech Industries*. <https://www.fdicchina.com/blog/made-in-china-2025-plan-to-dominate-manufacturing/>

² *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*. (2021, March 12). t0284_14th_Five_Year_Plan_EN (georgetown.edu)

³ *Made In China 2025: The Plan to Dominate Manufacturing and High-Tech Industries*. <https://www.fdicchina.com/blog/made-in-china-2025-plan-to-dominate-manufacturing/>

⁴ *Quantum Technologies Flagship*. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>

⁵ Там же.

⁶ *Quantum Manifesto for Quantum Technologies*. <https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html>

⁷ Там же.

Акты стратегического планирования в области создания квантовых технологий приняты в отдельных странах ЕС (табл. 1).

Королевство Нидерландов. Национальная повестка в области квантовых технологий⁸ была принята в Нидерландах в 2019 г. Данным актом предусматривается создание Консорциума регуляторов, стейкхолдеров и университетов, которые объединяют усилия по разработке квантовых технологий⁹ (табл. 1).

Федеративная Республика Германия. Рамочная программа федерального правительства Германии «Квантовые технологии – от фундаментальных исследований до рынка»¹⁰ определила следующие цели федерального правительства: укрепление сильных позиций Германии в области исследований квантовой физики и прокладывание пути к приложениям с использованием квантовых технологий; создание рамочных условий для подготовки к новым экономическим возможностям и рынкам; создание прочной основы для ведущей роли Германии в промышленном использовании квантовых технологий; развитие международного сотрудничества в сфере создания квантовых технологий; информирование населения Германии и его вовлечение в процесс продвижения новой ключевой технологии¹¹ (табл. 1).

Соединенные Штаты Америки. Законом о Национальной квантовой инициативе¹² от 13 декабря 2018 г. поставлена задача удержания технологического лидерства США в области квантовых технологий в среднесрочной и долгосрочной перспективе. Данный акт содержит план на 10-летний период развития и продвижения квантовых технологий в стране. Среди необходимых действий – учреждение специальных органов и комитетов, которые будут осуществлять организацию исследований в сфере квантовых технологий, а также выработку стандартов в данной сфере¹³.

Другой важный документ в этой сфере – Меморандум о национальной безопасности по продвижению лидерства Соединенных Штатов в квантовых вычислениях при снижении рисков для уязвимых криптографических систем¹⁴. В нем определены ключевые шаги, необходимые для поддержания конкурентного преимущества страны в области квантовой информатики при одновременном снижении рисков, связанных с появлением квантовых компьютеров для кибер-, экономической и национальной безопасности страны¹⁵.

⁸ *National Agenda for Quantum Technology*. <https://qutech.nl/wp-content/uploads/2019/09/NAQT-2019-EN.pdf>

⁹ Там же.

¹⁰ *Quantum technologies – from basics to markets*. https://www.bmbf.de/pub/BMBF_Fo__rderprogramm_Quantentechnologie_2018.pdf

¹¹ Там же.

¹² Public Law No. 115-368. (2018, December 21). National Quantum Initiative Act. <https://www.congress.gov/bill/115th-congress/house-bill/6227>

¹³ Там же.

¹⁴ *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>

¹⁵ Там же.

Меморандум также перечисляет конкретные действия в целях устранения уязвимостей компьютерных систем на квантово-устойчивую криптографию. В секретном приложении к этому меморандуму рассматриваются наиболее «чувствительные» вопросы национальной безопасности¹⁶ (табл. 1).

Соединенное Королевство Великобритании и Северной Ирландии. В 2014 г. в Великобритании была создана Национальная программа квантовых технологий¹⁷ (далее – NQTP), целью которой является превращение Великобритании в мирового лидера в области разработки и коммерциализации квантовых технологий. В 2020 г. NQTP опубликовала «Стратегический замысел», в котором излагается видение следующего десятилетия для экономики Великобритании с квантовыми технологиями¹⁸ (табл. 1).

Канада. На развитие Национальной квантовой стратегии Канады¹⁹ было выделено \$360 млн. Стратегия поддерживает динамично развивающуюся канадскую квантовую индустрию и поможет создать рабочую силу, необходимую для укрепления глобального лидерства Канады в сфере квантовых технологий²⁰ (табл. 1).

Австралийский Союз. Национальная квантовая стратегия²¹ содержит план, целью которого является способствование австралийскому кванту реализовать свой экономический потенциал. Для этого Австралия открыла Квантовый центр коммерциализации, который будет сопровождать и поддерживать коммерциализацию квантовых исследований и развитие квантового бизнеса в Австралии²². Другой интересной инициативой стала Дорожная карта по применению квантовых технологий для австралийской армии (Army Quantum Technology Roadmap)²³ (табл. 1).

Республика Сингапур. Новая Национальная сеть квантовой безопасности²⁴ (NQSN) будет развертывать коммерческие технологии для испытаний с участием государственных учреждений и частных компаний, проводить углубленную оценку систем безопасности и разрабатывать руководящие принципы для поддержки

¹⁶ Memorandum on Preparing for Post-Quantum Cryptography. <https://www.dhs.gov/publication/memorandum-preparing-post-quantum-cryptography>

¹⁷ UK National Quantum Technologies Programme (NQTP). <https://uknqt.ukri.org/>

¹⁸ UK National Quantum Technologies Programme (NQTP). A quantum-enabled future: legal and regulatory aspects of quantum technology. <https://techinsights.linklaters.com/post/102hryr/a-quantum-enabled-future-legal-and-regulatory-aspects-of-quantum-technology>

¹⁹ Government of Canada launches public consultations on National Quantum Strategy. <https://www.canada.ca/en/innovation-science-economic-development/news/2021/07/government-of-canada-launches-public-consultations-on-national-quantum-strategy.html>

²⁰ National Quantum Strategy. <https://digitalnovascotia.com/news/government-of-canada-launches-public-consultations-on-national-quantum-strategy/>

²¹ National Quantum Strategy: proposed framework. <https://consult.industry.gov.au/national-quantum-strategy>

²² Australian National Quantum Strategy. <https://www.insidequantumtechnology.com/news-archive/australias-vision-for-quantum/>

²³ Army Quantum Technology Roadmap. <https://researchcentre.army.gov.au/rico/army-quantum-technology-roadmap>

²⁴ CQT researchers join new project to build National Quantum-Safe Network in Singapore. <https://www.science.nus.edu.sg/blog/2022/03/15/cqt-researchers-join-new-project-to-build-national-quantum-safe-network-in-singapore/>

компаний, внедряющих такие технологии. Сумма государственного финансирования составит 8,5 млн сингапурских долларов в течение трех лет²⁵ (табл. 1).

Республика Корея. В 2019 г. был одобрен План по развитию квантовых вычислений²⁶. В течение пяти лет планируется осуществить разработку основных технологий, таких как аппаратное обеспечение квантовых компьютеров, а также перспективных направлений, включая новую архитектуру квантовых вычислений, квантовые алгоритмы и базовое программное обеспечение. Целью данного плана стала разработка 5-кубитного компьютера со степенью устойчивости 90 % к 2023 г.²⁷ Для дальнейшей реализации политики в сфере развития квантовых технологий в 2022 г. Южная Корея приняла Пятилетнюю программу развития квантовых технологий²⁸ (табл. 1).

Таблица 1. Регулирование квантовых технологий в зарубежных странах

Страна	Программа	Актеры	Действия	Стадия	Бюджет
Китайская Народная Республика	14-й пятилетний план «Социально-экономическое развитие Китая»; Национальный план «Сделано в Китае – 2025»	Преимущественно государство	Развитие национальных инновационных проектов, создание лабораторий; подготовка кадров	Коммерциализация	15,3 млрд долл.
Соединенные Штаты Америки	Закон о Национальной квантовой инициативе; Меморандум о национальной безопасности	Государство/частный сектор	Организация и поддержка исследований, создание стандартов	Коммерциализация	2,5 млрд долл.
Европейский союз и отдельные страны-участницы	Инициатива квантового лидерства; Квантовый манифест	Государство/частный сектор	Государственно-частное партнерство, гранты, консорциумы	Коммерциализация	1 млрд долл.
Королевство Нидерландов	Национальная стратегия в области квантовых технологий	Государство и частный сектор	Создание консорциума регуляторов, стейкхолдеров и университетов	Создание	850 млн долл.
Федеративная Республика Германия	Рамочная программа федерального правительства «Квантовые технологии – от фундаментальных исследований до рынка»	Государство	Поддержка исследований, развитие сотрудничества	Создание/коммерциализация	2,4 млрд долл.

²⁵ National Quantum Security Network. <https://www.eurekalert.org/news-releases/943794>

²⁶ Korea Starts Five-year Development Program for Quantum Computing Technology. <https://k-erc.eu/korea-starts-five-year-development-program-for-quantum-computing-technology/>

²⁷ Quantum Computing Development Plan. <http://www.businesskorea.co.kr/news/articleView.html?idxno=28881>

²⁸ 5-Years Plan for Quantum Technologies. <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=610&searchOpt=ALL&searchTxt=>

Страна	Программа	Актеры	Действия	Стадия	Бюджет
Соединенное Королевство Великобритании и Северной Ирландии	Национальная программа квантовых технологий	Государство/частный сектор	Поддержка исследований, развитие сотрудничества, государственно-частное партнерство, гранты, консорциумы	Создание	1,23 млрд долл.
Республика Сингапур	Национальная сеть квантовой безопасности	Государство/частный сектор	Создание руководящих принципов государственной поддержки компаний-разработчиков	Коммерциализация	90,9 млн долл.
Канада	Национальная квантовая стратегия	Государство/частный сектор	Поддержка канадской квантовой индустрии; подготовка кадров	Создание/коммерциализация	650 млн долл.
Австралийский Союз	1. Национальная квантовая стратегия. 2. Дорожная карта по использованию квантовых технологий для нужд армии	Государство/частный сектор	Поддержка коммерциализации квантовых технологий и развитие «квантового» бизнеса	Коммерциализация	94 млн долл.
Республика Корея	План по развитию квантовых вычислений; Пятилетняя программа развития квантовых технологий	Государство/частный сектор	Поддержка исследований, развитие сотрудничества, подготовка кадров	Создание	40,9 млн долл.

2.2. Регулирование квантовых технологий в Российской Федерации

Развитие высоких квантовых технологий является одной из задач, направленных на достижение цели научно-технологического развития России в соответствии со Стратегией национальной безопасности Российской Федерации²⁹. При этом заметим, что квантовые технологии находятся в фокусе внимания не только как средство обеспечения национальной безопасности. Они также выступают одним из направлений развития научно-технологического прогресса³⁰. Более того, на необходимость создания и развития таких технологий указывается также в федеральной целевой программе «Цифровая экономика»³¹.

²⁹ Указ Президента РФ № 4005 от 02.07.2021. (2021). *Собрание законодательства РФ*, 27 (ч. II), ст. 5351.

³⁰ Постановление Правительства РФ № 377 от 29.03.2019. (2019). *Собрание законодательства РФ*, 15 (ч. III), ст. 1750.

³¹ Паспорт Федерального проекта «Цифровые технологии», утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9 // СПС «КонсультантПлюс»; Постановление Правительства РФ № 377 от 29.03.2019. (2019). *Собрание законодательства РФ*, 15 (ч. III), ст. 1750.

В рамках данной программы была утверждена Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» (далее – дорожная карта)³². В ней проанализированы существующие виды квантовых технологий (субтехнологий) – квантовые вычисления, квантовая сенсорика и метрология, квантовая криптография, а также определены необходимые меры для развития квантовых технологий в России. Общий бюджет на реализацию дорожной карты (на период 2019–2024 гг.) составил 51,1 млрд руб., включая внебюджетное финансирование в размере 8,7 млрд руб.³³

Существенно, что поддержка всех трех основных субтехнологий квантовых технологий является критически важной для национальной безопасности и обеспечения цифрового суверенитета Российской Федерации. Отмечается, что необходимым условием для прорыва в области квантовых технологий является поддержка исследований и запуск инфраструктурных проектов национального масштаба, а также реализация организационных мероприятий по преодолению барьеров.

Среди таковых – создание необходимой инновационной инфраструктуры для их развития. Так, например, был создан инновационный научно-технологический центр «Квантовая долина»³⁴ в целях стимулирования предпринимательской деятельности в сфере создания цифровых технологий.

Кроме того, в Российской Федерации уделяется внимание и разработке национальных стандартов продуктов и решений, созданных на основе квантовых технологий. Так, уже сейчас разработан ГОСТ Р 58568-2019. «Национальный стандарт Российской Федерации. Оптика и фотоника. Фотоника. Термины и определения»³⁵. Кроме того, в ближайшее время планируется завершить разработку еще целого ряда иных стандартов в сфере квантовых технологий³⁶.

³² Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». <https://digital.gov.ru/>

³³ Там же.

³⁴ Постановление Правительства РФ № 2133 от 30.11.2021. (2021). *Собрание законодательства РФ*, 49 (ч. II), ст. 8318.

³⁵ Национальный стандарт Российской Федерации ГОСТ Р 57257-2016/ISO/TS 80004-12:2016 «Нанотехнологии. Часть 12. Квантовые явления. Термины и определения» (утв. и введен в действие приказом Росстандарта от 10.11.2016 № 1673-ст). Москва: Стандартинформ, 2016.

³⁶ Так, в настоящий момент разрабатываются стандарты: «Квантовые коммуникации. Термины и определения»; «Квантовые коммуникации. Общие положения»; «Квантовый интернет вещей. Термины и определения»; «Квантовый интернет вещей. Общие положения»; «Квантовый интернет вещей. Типовой программно-аппаратный комплекс, реализующий функции системы квантового распределения ключей. Архитектура»; «Квантовый интернет вещей. Типовой программно-аппаратный комплекс, реализующий функции системы квантового распределения ключей. Интерфейсы подключения». (В России начали создавать стандарты квантовых технологий. <https://habr.com/ru/news/t/684540/>)

3. На пути к квантовому праву

Не грусти, – сказала Алиса. –
Рано или поздно все станет понятно,
все станет на свои места и выстроится
в единую красивую схему, как кружева.

**Художественный фильм
«Алиса в Стране чудес»,
режиссер Тим Бертон, 2010 г.**

3.1. Общие векторы формирования квантового права

Учеными уже не раз высказывались предположения о том, как сильно квантовые технологии способны изменить нашу жизнь (Arndt et al., 2011; Browne et al., 2017; Sigov et al., 2020). Трансформации подвергнутся многие сферы нашей жизни. Право не будет являться исключением. При этом полагаем, что трансформации подвергнется не только правовое регулирование, но и право в целом.

Уникальные свойства квантовых технологий не только откроют перед нами новые возможности, но и, конечно же, принесут новые риски и угрозы. Думается, что они обладают потенциалом изменения некоторых фундаментальных основ, в том числе и правовых. Это означает возможность формирования квантового права.

Ранее отмечалось, что зарубежные ученые активно работают над развитием идеи квантового права. Так, в статье «Рождение квантового права: концептуальные замечания» Дж. Риттер выдвигает концепт квантового права – некоего набора универсальных правил, применять которые будет возможно независимо от местонахождения или происхождения информации или технологии. При этом, по мнению ученого, квантовое право позволит пересмотреть наши представления о том, как поддерживать верховенство закона (Ritter, 2015).

Ему вторит и проф. Дж. Атик, считающий, что квантовая логика, квантовые алгоритмы и квантовые вычисления совместно с квантовым пониманием Вселенной способны преобразить и право, открывая новые возможности для создания квантовых норм, квантовых судебных решений и квантового правопорядка (Atik, 2022).

Как квантовые технологии могут преобразить право? Анализ работ ученых в данной сфере позволил выделить следующие векторы развития права в условиях второй квантовой революции.

3.1.1. От детерминизма к вероятностям в праве – смена правовой парадигмы

Можно допустить, что новое право будет развиваться по законам, свойственным квантовой механике, а не классической физике. Уже сейчас можно провести некоторые аналогии существующего права с детерминистским подходом, принятым в классической физике, и квантового права как права будущего с вероятностным подходом, свойственным квантовой механике.

По мнению профессора Дж. Атика, с приходом данных технологий «придет и квантовый способ мышления с информацией, “закодированной” в вероятностях, а не в определенностях. А это повлияет на то, как мы думаем о сложных системах. Уже давно понятно, что к истинному равновесию можно приблизиться, но никогда его не достичь в физических системах, и, вероятно, того менее в социальных системах» (Atik, 2022).

Развивая мысль ученого, отметим, что аналогичным образом можно говорить и о достижении истины в праве. Вопрос о том, что является истиной, например в уголовном праве, и как ее определить, дискуссионный, и найти однозначный, определенный ответ на него крайне сложно. Таким образом, как и в квантовой механике, в отдельных вопросах права мы уже мыслим в вероятностях, а не в определенностях, отказываясь от детерминизма.

Более того, заметим, что цифровизация буквально заставляет нас отказаться от прежнего концепта и требует «обновления» права. В этой связи уже сейчас появляются неортодоксальные инструменты, позволяющие создать эффективное регулирование для цифровых технологий. Так, например, позволяя тестировать цифровые инновации в рамках экспериментальных правовых режимов (регуляторных песочниц), мы также отказываемся от детерминистского подхода и мыслим в вероятностях. Временно не применяя отдельные регуляторные требования, мы пытаемся определить, какова вероятность того, что отступление от правил «пойдет на пользу» технологическому прогрессу, и стоит ли в дальнейшем перевести это «временное и специальное» в «постоянное и общее».

3.1.2. Проецирование свойств квантовых явлений на регулирование общественных отношений

В чем это будет выражено и как может отразиться на праве будущего с практической точки зрения? Тот факт, что особенностью квантовых технологий является вероятностный характер вычислений, потребует от основных акторов внедрения риск-ориентированных подходов во многие сферы. На сегодняшний день риск-ориентированный подход уже внедряется и применяется для регулирования различного рода общественных отношений (Бегишев, 2021). Так, в Российской Федерации это прежде всего область государственного и муниципального контроля за деятельностью субъектов предпринимательства³⁷. Зарубежные страны используют данный подход к регулированию технологии искусственного интеллекта³⁸.

Вполне вероятно, что с распространением квантовых технологий, в частности квантовых вычислений, концепт мышления юристов тоже может измениться. В зарубежной науке уже ставится вопрос о трансформации вычислительного права (computational law) в квантовое вычислительное право (quantum computational law), которое позволит принимать более объективные судебные решения и находить решения, казалось бы, нерешаемых правовых проблем, опираясь на свойства квантовых явлений (Atik & Jeutner, 2021).

Переходя к следующему свойству квантовых явлений – квантовой запутанности, которая, по сути, представляет собой постоянное взаимодействие квантовых частиц и их взаимозависимость одной от другой, можно будет проецировать это на будущее квантовое право. Думается, что данное право уже не будет «чистым» правом в его классическом понимании. Оно все больше и больше будет взаимодействовать

³⁷ О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации. Федеральный закон от 31.07.2020 № 248-ФЗ. (2020). *Собрание законодательства РФ*. 2020. № 31 (ч. I). Ст. 5007.

³⁸ См., напр.: EU AI Act. <https://artificialintelligenceact.eu/>

с иными областями научного знания: этикой, экономикой, техническими науками. Данный процесс уже запущен. Так, например, зарубежные и российские ученые уже давно отстаивают необходимость применения методов экономических наук в праве (экономический анализ права) (Гаджиев, 2016; Познер, 2004).

Более того, на современном этапе, пытаясь урегулировать процессы создания и внедрения искусственного интеллекта, мы обращаемся не столько к правовым нормам, сколько к этическим принципам. Указанное объясняется тем, что для регулирования цифровых технологий недостаточно классического правового инструментария.

3.1.3. Поиск «квантового» уровня права и его следствия

Другой вопрос, который ставится в науке, звучит так: обладает ли право «квантовым» уровнем?³⁹ Профессор Дж. Риттер высказывает предположение, что квантовое право обладает квантовым уровнем, не указывая, однако, на то, что это за уровень. И хотя нам весьма сложно найти какой-то иной ответ на данный вопрос, помимо того, что таковым уровнем будет являться норма права, мы считаем важным сфокусироваться не на определении квантового уровня права, а на том, как, собственно, «кванты» могут повлиять на регулирование. Означают ли какие-либо идеи из квантовой теории, что мы должны пересмотреть наши предположения о законе или внутри закона?⁴⁰

Думается, что с приходом этих цифровых технологий само правовое регулирование может стать «квантовым». В данном случае это означает, что оно может стать более конкретным, практико-ориентированным, уйдя при этом от излишней абстрактности. Заметим, что это уже является своего рода трендом. Регулирование во всем сейчас формируется не только законодательными органами. В данный процесс активно включился частный сектор. В основном крупные транснациональные корпорации. Так, уже сейчас говорят о праве, формируемом цифровыми платформами, например, есть концепт права eBay (eBayLaw) (Guadamuz, 2003), а частные компании активно подключаются к процессам разработки международных и национальных стандартов. Новое регулирование будет, несомненно, более практико-ориентированным, поскольку, формируя такие правила, бизнес отталкивается от существующих проблем, с которыми повседневно сталкивается.

3.2. Регуляторные песочницы и иные специальные режимы как составляющие квантового права

Масштабная, глобальная и интенсивная цифровизация и появление новых технологий как ее следствие уже привели к возникновению правовой неопределенности и потребовали поиска более гибких подходов к правовому регулированию. Одним из таковых стали специальные режимы и экспериментальные режимы как их разновидность.

Как представляется, указанное в полной мере применимо и к квантовым технологиям, чья инновационная природа также требует от права трансформации

³⁹ Quantum law: an interdisciplinary exploration of quantum theory law and ethics. <https://www.westminster.ac.uk/events/quantum-law-an-interdisciplinary-exploration-of-quantum-theory-law-and-ethics>

⁴⁰ Там же.

и адаптации к реалиям, которые будут обусловлены распространением квантовых технологий.

Уже сейчас эксперты говорят о необходимости отдельных отступлений или изъятий из действующего законодательства. Так, например, идея о специальном правовом режиме в сфере патентования квантовых технологий предложена проф. В. Джойтнером. По его мнению, необходимость сокращения цифровых разрывов и неравенства в целом, вызванных появлением квантовых технологий, требует введения ограничения на их патентование (Jeutner, 2021). Это обусловлено тем, что уже сейчас ряд стран ведут весьма агрессивную политику в области патентования квантовых технологий⁴¹ и международное закрепление таких правил будет способствовать борьбе с усилением неравенства. Кроме того, ученый также предлагает сделать обязательным трансфер квантовых технологий в отдельных сферах (например, социально значимых).

Ученые также предлагают специальный режим для контроля экспорта квантовых технологий. Так, высказывается идея о включении таких технологий в Вассенарское соглашение (Jeutner, 2021).

О специальном регулировании говорят и применительно к тому моменту, когда мы станем массово переходить на квантовые облачные услуги. Квантовые облачные вычисления должны демократизировать рынок, позволяя частным лицам и компаниям получить доступ к исключительной вычислительной мощности без необходимости создавать и поддерживать собственную инфраструктуру квантовых вычислений. Квантовые облачные сервисы будут особенно важны в ближайшие три-пять лет, поскольку позволят проводить эксперименты до того, как квантовые компьютеры станут более доступными. Это, однако, потребует внесения изменений в законодательство о персональных данных. Именно поэтому технологическим лидерам важно прояснить, какие данные могут передаваться через различные организационные границы, какие данные передаются и как это происходит.

Российские ученые также активно участвуют в процессе создания основ регулирования квантовых технологий и отмечают необходимость разработки правового регулирования квантовых технологий. Помимо указанного, следует также сосредоточиться на выработке правового регулирования применения квантовых технологий в различных сферах деятельности (социальной, культурной, экономической и др.) (Холодная, 2022; Добробаба и др., 2022). Внимания заслуживают и конкретные предложения российских ученых в рамках совершенствования отдельных отраслей в целях развития квантовых технологий. Так, в частности, предлагается наделение лиц – разработчиков квантовых технологий рядом налоговых льгот и преференций (Добробаба и др., 2022). Экспертами также предлагается ввести ответственность за нарушение запрета на использование обычных методов шифрования информации (Наумов и Станковский, 2019).

В поисках оптимальных подходов к регулированию квантовых технологий и формированию права таких технологий следует применять экспериментальные правовые режимы в сфере создания цифровых инноваций (регуляторные песочницы).

⁴¹ Quantum USA vs. Quantum China: The World's Most Important Technology Race. <https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=311e182372de>

В условиях такого режима происходит временный отказ от применения отдельных регуляторных требований в целях проверки жизнеспособности цифровой инновации и попытки создания их оптимального правового регулирования. Это позволяет субъектам инновационной предпринимательской деятельности сократить финансовые и временные издержки, связанные с запуском инновации; государству – определить оптимальную модель правового их регулирования. Заметим, что отмеченная гибкость регуляторных песочниц позволит создать проактивное право, идущее в ногу с цифровизацией.

Полагаем, что для создания эффективного правового регулирования квантовых технологий применение экспериментальных правовых режимов будет одним из оптимальных решений.

Однако при этом следует помнить о том, что свойства квантовых технологий и их потенциал пока что до конца не изучены, и это требует больших мер предосторожности и эффективных мер защиты заинтересованных лиц. В этой связи предлагается особым образом учитывать риски, связанные с указанными особенностями квантовых технологий, и предпринимать попытки их минимизации на уровне программы экспериментального правового режима. Также предлагается предусмотреть дополнительные компенсации и страхование ответственности субъектов экспериментального правового режима (Gromova & Ivanc, 2020). Кроме того, следует помнить и о том, что создание квантовых технологий в условиях экспериментального правового режима потенциально может повлечь и нарушение антимонопольного законодательства. Дело в том, что временное отступление от применения к деятельности участника такого режима отдельных регуляторных требований дает ему конкурентные преимущества, связанные с быстрым входом на рынок, а иногда и сокращением затрат на совершение отдельных действий (сертификацию, лицензирование, аккредитацию и т. п.) (Громова, 2022).

4. Этика квантов

4.1. Базовые этические принципы, применимые к квантовым технологиям

В зарубежной литературе предлагается использовать подход этического регулирования, который используется в отношении искусственного интеллекта⁴². При этом представляется, что квантовые технологии будут регулироваться общими, базовыми этическими принципами, такими как безопасность, надежность, контролируемость и управляемость, прозрачность, интерпретируемость и предсказуемость.

Рассматривая принцип безопасности применительно к квантовым технологиям, важно отметить, что разработчики таких технологий, а также иные причастные к их созданию и внедрению лица должны обеспечить необходимую безопасность тех, кто будет применять такие технологии, а также не допустить причинения вреда потребителям, пользователям и иным субъектам.

Принцип надежности квантовых технологий подразумевает необходимость обеспечения возможности таких технологий сохранить в течение продолжительного

⁴² См., напр.: Ethics guidelines for trustworthy AI: Shaping Europe's digital future – European Commission. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>; OECD AI Policy Observatory. <https://oecd.ai/en/>; Кодекс этики в сфере искусственного интеллекта. <https://a-ai.ru/ethics/index.html>

времени способность выполнять требуемые функции в условиях применения, технического обслуживания, хранения и транспортирования.

Говоря о принципах контролируемости и управляемости квантовых технологий, следует отметить, что при их разработке и применении должны максимально возможно учитываться риски, связанные с их применением, а также быть апробированы способы их минимизации.

Принцип прозрачности квантовых технологий подразумевает возможность открытого, исчерпывающего, доступного, четкого и понятного представления информации как о самих квантовых технологиях, сферах их применения, так и последствиях их применения.

Интерпретируемость будет подразумевать необходимость разработки объяснимых квантовых технологий, применение которых может повысить доверие к ним, предоставляя обществу возможность понимания принципов их работы, распознавания случаев дискриминации или предвзятости при их применении, а также информирования о нарушениях прав.

Несомненно, квантовые технологии должны быть предсказуемыми. И хотя, учитывая вышеназванные особенности квантовых технологий и свойства квантовых явлений, обеспечить исполнение данного принципа будет крайне сложным, тем не менее разработчикам таких технологий следует сделать все возможное для того, чтобы способы их применения приводили к ожидаемым и приемлемым результатам.

4.2. Специальные этические принципы развития и применения квантовых технологий

Вместе с тем, учитывая специфику квантовых технологий, можно говорить о необходимости выработки специальных этических принципов. На это обращают внимание и российские (Yunakovsky et al., 2021; Kabanov et al., 2018; Kitaev et al., 1999; Korolkov, 2015) и зарубежные представители технических наук (Arute et al., 2019; Muheidat et al., 2022; Kabanov et al., 2018; Kitaev et al., 1999). Так, например, исследовательским коллективом Университета Лунд в рамках их проекта «Квантовое право» был разработан так называемый Квантовый императив. Данный императив предусматривает, что регулирующие органы и разработчики должны быть уверены, что квантовые компьютеры:

- не создавали и не усугубляли неравенства;
- не подрывали индивидуальную автономию личности;
- учитывали мнения тех, чьи интересы могут быть затронуты при применении квантовых технологий (Jeutner, 2021).

Кроме того, анализ зарубежных источников, в которых затрагиваются вопросы этики квантовых технологий, позволил дополнить данный Квантовый императив следующими этическими принципами:

– этико-первостепенное мышление в отношении квантовых разработок (ethic-first quantum mind). Данный принцип предполагает следующие составляющие: проактивность и соразмерность. Проактивность подразумевает так называемую работу на опережение – активные, ответственные действия регуляторов, бизнеса и технологических лидеров в целях создания этического будущего для квантовой экосистемы. В прошлом возможности для разработки этических рекомендаций по мере появления новых технологий были упущены. Это привело к возникновению серьезных проблем, например, расистских алгоритмов распознавания лиц. Именно поэтому акторы обязаны занять более проактивную позицию в отношении квантовых

технологий. Соразмерность предполагает такое поведение регуляторов и разработчиков, которое учитывает действительную необходимость применения квантовых технологий и соотносит это с реалиями. Как отмечают эксперты, часто создается впечатление, что компании и государственные органы используют революционные технологии ради самих технологий без полного учета сопутствующих экономических, операционных и репутационных рисков;

– межсекторное и междисциплинарное сотрудничество для установления четких границ этичного и неэтичного использования квантовых технологий.

Думается, что принятие Кодекса этики регуляторов и разработчиков квантовых технологий (Кодекс этики квантов) будет способствовать развитию этичного, добро-совестного создания и применения данных технологий.

Кроме того, следует рассмотреть возможность внедрения в деятельность компании – разработчика системы квантового этико-правового комплаенса (по аналогии с антимонопольным комплаенсом) – специальной внутренней корпоративной политики, направленной на выявление и пресечение возможных нарушений этических и правовых норм.

Выводы

Проведенное исследование позволило прийти к следующим выводам:

1. Включение многих стран в квантовую гонку и их стремление уже не просто создавать, но и коммерциализировать квантовые технологии означает, что рано или поздно такие технологии прочно войдут в нашу жизнь. А учитывая их революционные свойства и активную работу мирового научного сообщества по их «обузданию», становится очевидно, что такие технологии не просто войдут в нашу жизнь, но и существенно ее изменят.

2. Государства создают плацдарм для такой трансформации, в том числе за счет создания регулирования квантовых технологий. Пока что это, как правило, акты общего стратегического планирования, хотя уже сейчас начинают появляться специальные документы, регулирующие особенности создания и внедрения квантовых технологий в отдельных сферах.

3. На основании изучения регулирования квантовых технологий зарубежными странами можно сделать следующие выводы.

Во-первых, регулирование квантовых технологий большинством рассмотренных стран на данный момент осуществляется актами стратегического планирования общего характера. Однако уже сейчас начинает формироваться отраслевое регулирование квантовых технологий. Во-вторых, обращает на себя внимание тот факт, что в отдельных странах национальными программами развития квантовых технологий уделяется внимание не столько созданию таких технологий, сколько их коммерциализации – это означает, что этап разработки таких технологий может находиться на завершающей стадии и страны сосредоточились на том, чтобы создать условия для их применения. В-третьих, данные акты предусматривают преимущественно государственное финансирование создания и коммерциализации квантовых технологий, хотя и поощряют развитие государственно-частного партнерства и частного инвестирования в области таких цифровых технологий.

4. С учетом описанных свойств квантовых явлений, а также тех вызовов и рисков, которые несет применение квантовых технологий, становится очевидным, что трансформации подвергнется и само право. Одним из следствий может стать

формирование нового квантового права. Его концептуальные основы будут обусловлены свойствами квантовых технологий.

5. Векторами развития квантового права станет применение специальных, в том числе экспериментальных, правовых режимов. Регуляторные песочницы позволят протестировать сервисы, бизнес-модели и продукты, основанные на квантовых технологиях, и выработать наиболее оптимальное для них регулирование.

6. Важное значение в развитии квантового права будет придаваться этическим принципам регулирования и применения таких технологий. В этой связи, а также с учетом необходимости работы на опережение уже сейчас необходимо приступить к созданию кодекса квантовой этики и разработки системы этико-правового комплаенса.

Список литературы

- Бегишев, И. Р. (2021). Криминологическая классификация роботов: риск-ориентированный подход. *Правоприменение*, 5(1), 185–201. [https://doi.org/10.52468/2542-1514.2021.5\(1\).185-201](https://doi.org/10.52468/2542-1514.2021.5(1).185-201)
- Гаджиев, Г. А. (2016). *Право и экономика (методология)*. Москва: Норма: ИНФРА-М.
- Громова, Е. А. (2022). Экспериментальные режимы создания цифровых инноваций и проблемы обеспечения добросовестной конкуренции. *Журнал российского права*, 26(10), 41–51. EDN: <https://elibrary.ru/higrhr>. DOI: <https://doi.org/10.12737/jrl.2022.104>
- Дирак, П. А. М. (1979). *Принципы квантовой механики*. Москва: Мир.
- Добробаба, М. Б., Чаннов, С. Е., Минбалева, А. В. (2022). Квантовые коммуникации: перспективы правового регулирования. *Вестник Университета им. О. Е. Кутафина*, 4, 25–37. EDN: <https://elibrary.ru/maompt>. DOI: <https://doi.org/10.17803/2311-5998.2022.92.4.025-037>
- Корж, О. В., Андреев, Д. Ю., Корж, А. А., Коробков, С. В., Чернявский, А. Ю. (2013). Моделирование работы идеального квантового компьютера на суперкомпьютере «Ломоносов». *Вычислительные методы и программирование*, 2(14), 24–34. <https://elibrary.ru/rowasx>
- Наумов, В. Б., Станковский, Г. В. (2019). Правовые аспекты квантовых коммуникаций: новые горизонты. *Пробелы в российском законодательстве*, 4, 235–239.
- Петренко, С. А., Петренко, А. С., Ожиганова, М. И. (2021). Оценка возможностей квантовых алгоритмов криптоанализа. *Защита информации. Инсайд*, 6(102), 70–82.
- Петренко, А. С., Петренко, С. А., Ожиганова, М. И. (2021). Модель угроз безопасности по аналитике зарубежных национальных квантовых программ. *Защита информации. Инсайд*, 4(100), 50–59.
- Познер, Р. А. (2004). *Экономический анализ права*. В 2 т. Т. 1. Санкт-Петербург: Экономическая школа, 2004.
- Холодная, Е. В. (2022). Квантовые технологии как объект права. *Вестник Университета им. О. Е. Кутафина*, 4, 38–45. EDN: <https://elibrary.ru/aayhpk>. DOI: <https://doi.org/10.17803/2311-5998.2022.92.4.038-045>
- Arndt, M., Bassi, A., Giulini, D., Heidmann, A., & Raimond, J. M. (2011). Fundamental Frontiers of Quantum Science and Technology. *Procedia Computer Science*, 7, 77–80. <https://doi.org/10.1016/j.procs.2011.12.024>
- Arute, F., Arya, K., & Babbush, R. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574, 505–510. <https://doi.org/10.1038/s41586-019-1666-5>
- Atik, J., & Jeutner, V. (2021). Quantum Computing and Computational Law. *Law, Innovation and Technology*, 3, 1–23. <https://doi.org/10.1080/17579961.2021.1977216>
- Atik, J. (2022). Quantum computing and the legal imagination. *SciTech Lawyer*, 22, 1–5. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4087044
- Ball, Ph. (2021). Where does quantum weirdness end? *New Scientist*, 251(3349), 38–39. [https://doi.org/10.1016/S0262-4079\(21\)01518-9](https://doi.org/10.1016/S0262-4079(21)01518-9)
- Belenchia, A., Carlesso, M., Bayraktar, M., Dequal, D., Derkach, I., Gasbarri, G., Herr, W., Li, Y. L., Rademacher, M., Sidhu, J., Oi, D. K., Seidel, S. T., Kaltenbaek, R., Marquardt, C., Ulbricht, H., Usenko, V. C., Wörner, L., Xuereb, A., Paternostro, M., ... Bassi, A. (2022). Quantum physics in space. *Physics Reports*, 951, 1–70. <https://doi.org/10.1016/j.physrep.2021.11.004>
- Browne, D., Bose, S., Mintert, F., & Kim, M. (2017). From quantum optics to quantum technologies. *Progress in Quantum Electronics*, 54, 2–18. <https://doi.org/10.1016/j.pquantelec.2017.06.002>
- Chen, Y. A., Zhang, Q., Chen, T. Y. et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589, 214–219. <https://doi.org/10.1038/s41586-020-03093-8>

- Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Seria A: Mathematical, Physical and Engineering sciences*, 439(1907), 553–555. <https://doi.org/10.1098/rspa.1992.0167>
- Duplij, S., & Shapoval, I. (2007). Topological Methods In Quantum Computations. *Journal of Kharkov National University. Ser. Nuclei, Particles and Fields*, 3(35), 3–30.
- Gromova, E., & Ivanc, T. (2020). Regulatory sandboxes (experimental legal regimes) for digital innovations in BRICS. *BRICS Law Journal*, 7, 2, 10–36. EDN: <https://elibrary.ru/kzqaum>. DOI: <https://doi.org/10.21684/2412-2343-2020-7-2-10-36>
- Guadamuz, A. (2003). Ebay Law: The Legal Implications of the C2c Electronic Commerce Model. *Computer Law & Security Report*, 19, 6, 468–473.
- Jeutner, V. (2021). The Quantum Imperative: Legal Dimensions of Quantum Computing. *Morals & Machines*, 1(1), 52–59.
- Kabanov, I. S., Yunusov, R. R., Kurochkin, Y. V., & Fedorov, A. K. (2018). Practical cryptographic strategies in the post-quantum era. *AIP Conference Proceedings* 1936, 020021. <https://doi.org/10.1063/1.5025459>
- Kearney, J. J., & Perez-Delgado, C. A. (2020). Vulnerability of blockchain technologies to quantum attacks. *Array*, 10, 100065. <https://doi.org/10.1016/j.array.2021.100065>
- Kitaev, A., Shen, A., & Vyal, M. (1999). *Classical and quantum computing*. Moscow: ICNMO, Publishing House of Chero.
- Korolkov, A. V. (2015). On some applied aspects of quantum cryptography in the context of the development of quantum computing and the emergence of quantum computers. *Issues of cybersecurity*, 1(9), 6–13.
- Kumar Adarsh, Pacheco Diego Augusto de Jesus, Kaushik Keshav, & Rodrigues Joel J. P. C. (2022). Futuristic view of the Internet of Quantum Drones: Review, challenges and research agenda. *Vehicular Communications*, 36, 100487. <https://doi.org/10.1016/j.vehcom.2022.100487>
- Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, 16(5), 38–41. <https://doi.org/10.1109/MSP.2018.3761723>
- Muheidat, F., Dajani, K., & Tawalbeh, L. A. (2022). Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication. *Procedia Computer Science*, 203, 32–40. <https://doi.org/10.1016/j.procs.2022.07.007>
- Petrenko, A. (2022). *Applied Quantum Cryptanalysis*. River Publishers.
- Ritter, J. (2015). *The Birth of Quantum Law: A Concept Paper*. <https://doi.org/10.13140/RG.2.1.4263.7285>
- Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*, 27, 379–423.
- Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Foundations of Computer Science*, 10, 134–145. <https://doi.org/10.1109/SFCS.1994.365700>
- Shor, P. W. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26, 1484–1509. <https://doi.org/10.1137/S0097539795293172>
- Sigov, A., Ratkin, L., & Ivanov, L. A. (2020). Quantum Information Technology. *Journal of Industrial Information Integration*, 28, 100365. <https://doi.org/10.1016/j.jii.2022.100365>
- Taylor, R. D. (2020). Quantum Artificial Intelligence: A “precautionary” U.S. approach? *Telecommunications Policy*, 44(6), 101909. <https://doi.org/10.1016/j.telpol.2020.101909>
- Yanamadala, S., & Seema, S. (2022). Quantum dots: policy and ethics. In Yarub Al-Douri (Ed.). *Woodhead Publishing Series in Electronic and Optical Materials, Graphene, Nanotubes and Quantum Dots-Based Nanotechnology* (pp. 887–899). Woodhead Publishing. <https://doi.org/10.1016/B978-0-323-85457-3.00031-1>
- Yunakovsky, S. E., Kot, M., Pozhar, N. O., Nabokov, D., Kudinov, M. A., Guglya, A., Kiktenko, E. O., Kolycheva, E. V., Borisov, A., & Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology*, 8, 1–19. <https://doi.org/10.1140/epjqt/s40507-021-00104-z>

Сведения об авторах



Громова Елизавета Александровна – кандидат юридических наук, доцент, заместитель директора Юридического института по международной деятельности, доцент кафедры предпринимательского, конкурентного и экологического права, Южно-Уральский государственный университет (национальный исследовательский университет)

Адрес: 454080, Российская Федерация, г. Челябинск, проспект Ленина, 78

E-mail: gromovaea@susu.ru

ORCID ID: <https://orcid.org/0000-0001-6655-8953>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/AAO-8876-2020>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57208846603>

Google Scholar ID: <https://scholar.google.com/citations?user=fDz6FkUAAAAJ&hl>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=652593



Петренко Сергей Анатольевич – доктор технических наук, профессор, профессор кафедры информационной безопасности, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина); профессор, Университет Иннополис

Адрес: 420500, Российская Федерация, г. Иннополис, ул. Университетская, 1

E-mail: s.petrenko@innopolis.ru

ORCID ID: <https://orcid.org/0000-0003-0644-1731>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/O-5049-2017>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57195327289>

Google Scholar ID: https://scholar.google.com/citations?user=x_gez2gAAAAJ&hl=ru

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=805505

Вклад авторов

Е. А. Громова осуществляла общее руководство и постановку задач исследования, анализ отечественного и зарубежного регулирования квантовых технологий.

С. А. Петренко провел анализ текущего состояния науки «Квантовые вычисления» и определил перспективные направления инженерных исследований в этой области.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 1 декабря 2022 г.

Дата одобрения после рецензирования – 18 января 2023 г.

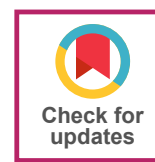
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.3>



Quantum Law: the Beginning

Elizaveta A. Gromova  

South Ural State University (National Research University)
Chelyabinsk, Russian Federation

Sergey A. Petrenko 

Saint Petersburg State Electrotechnical University "LETI" named after V. I. Ulyanov (Lenin)
Saint Petersburg, Russian Federation;
Innopolis University
Innopolis, Russian Federation

Keywords

Ethical issues
experimental legal regimes,
legal regulation,
quantum calculation,
quantum law,
quantum technology,
risks and challenges of using
quantum technologies

Abstract

Objective: to formulate the bases for quantum law as the law of the future, based on the study of quantum phenomena and features of quantum technologies determining the risks and challenges associated with the emergence of these technologies, as well as the analysis of legal regulation of quantum technologies in the Russian Federation and abroad.

Methods: to carry out this research, the authors applied a complex of general scientific methods of systemic analysis and specific methods of engineering and legal sciences. The use of comparative-legal method allowed revealing the main directions of developing legal regulation of quantum technologies in the Russian and foreign law orders based on the analysis of their international and national regulation. The method of legal modeling allowed forming a concept of quantum law, revealing the main vectors of its development and the complex of its ethical-legal principles.

Results: the features and properties of quantum technologies were revealed which can change the development of law with the advent of these technologies; the main risks and challenges were identified which are associated with the development of quantum technologies; the features of quantum technologies regulation in some foreign countries were specified; the trends of developing the quantum technologies regulation in the Russian Federation were identified; the conceptual bases of quantum law were formulated, as well as the vectors of its development.

 Corresponding author

© Gromova E. A., Petrenko 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.

Scientific novelty: for the first time in the legal science, a complex analysis of the current national (both Russian and foreign) regulation of quantum technologies was carried out, based on which an attempt was made to substantiate the need to form quantum law and to outline the main vectors of its development.

Practical significance: the research results lay the foundation for forming the concept of quantum law; in this regard, the authors' conclusions and proposals for improving the current regulation of quantum technologies can be used in law-making and law enforcement in this sphere, and may lay the bases for further research in the sphere of quantum technologies.

For citation

Gromova, E. A., & Petrenko, S. A. (2023). Quantum Law: The Beginning. *Journal of Digital Technologies and Law*, 1(1), 62–88. <https://doi.org/10.21202/jdtl.2023.3>

References

- Arndt, M., Bassi, A., Giulini, D., Heidmann, A., & Raimond, J. M. (2011). Fundamental Frontiers of Quantum Science and Technology. *Procedia Computer Science*, 7, 77–80. <https://doi.org/10.1016/j.procs.2011.12.024>
- Arute, F., Arya, K., & Babbush, R. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574, 505–510. <https://doi.org/10.1038/s41586-019-1666-5>
- Atik, J., & Jeutner, V. (2021). Quantum Computing and Computational Law. *Law, Innovation and Technology*, 3, 1–23. <https://doi.org/10.1080/17579961.2021.1977216>
- Atik, J. (2022). Quantum computing and the legal imagination. *SciTech Lawyer*, 22, 1–5. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4087044
- Ball, Ph. (2021). Where does quantum weirdness end? *New Scientist*, 251(3349), 38–39. [https://doi.org/10.1016/S0262-4079\(21\)01518-9](https://doi.org/10.1016/S0262-4079(21)01518-9)
- Begishev, I. R. (2021). Criminological classification of robots: risk-oriented approach. *Pravoprimereniye*, 5(1), 185–201. [https://doi.org/10.52468/2542-1514.2021.5\(1\).185-201](https://doi.org/10.52468/2542-1514.2021.5(1).185-201)
- Belenchia, A., Carlesso, M., Bayraktar, M., Dequal, D., Derkach, I., Gasbarri, G., Herr, W., Li, Y. L., Rademacher, M., Sidhu, J., Oi, D. K., Seidel, S. T., Kaltenbaek, R., Marquardt, C., Ulbricht, H., Usenko, V. C., Wörner, L., Xuereb, A., Paternostro, M., ... Bassi, A. (2022). Quantum physics in space. *Physics Reports*, 951, 1–70. <https://doi.org/10.1016/j.physrep.2021.11.004>
- Browne, D., Bose, S., Mintert, F., Kim, M. (2017). From quantum optics to quantum technologies. *Progress in Quantum Electronics*, 54, 2–18. <https://doi.org/10.1016/j.pquantelec.2017.06.002>
- Chen, Y. A., Zhang, Q., Chen, T. Y. et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589, 214–219. <https://doi.org/10.1038/s41586-020-03093-8>
- Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439(1907), 553–555. <https://doi.org/10.1098/rspa.1992.0167>
- Dirak, P. A. M. (1979). *Principles of quantum mechanics*. Moscow: Mir.
- Dobrobaba, M. B., Channov, S. E., & Minbaleev, A. V. (2022). Quantum communications: prospects of legal regulation. *Vestnik Universiteta im. O. E. Kutafina*, 4, 25–37. <https://doi.org/10.17803/2311-5998.2022.92.4.025-037>
- Duplij, S., & Shapoval, I. (2007). Topological Methods In Quantum Computations. *Journal of Kharkov National University, ser. Nuclei, particles and fields*, 3(35), 3–30.
- Gadzhiev, G. A. (2016). *Law and economics (methodology)*. Moscow: Norma: INFRA-M.
- Gromova, E. A. (2022). Experimental regimes of creating digital innovations and problems of ensuring good faith competition. *Zhurnal rossiyskogo prava*, 26(10), 41–51. <https://doi.org/10.12737/jrl.2022.104>
- 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>

- Guadamuz, A. (2003). Ebay Law: The Legal Implications of the C2c Electronic Commerce Model. *Computer Law & Security Report*, 19, 6, 468–473.
- Jeutner, V. (2021). The Quantum Imperative: Legal Dimensions of Quantum Computing. *Morals & Machines*, 1(1), 52–59.
- Kabanov, I. S., Yunusov, R. R., Kurochkin, Y. V., & Fedorov, A. K. (2018). Practical cryptographic strategies in the post-quantum era. *AIP Conference Proceedings* 1936, 020021. <https://doi.org/10.1063/1.5025459>
- Kearney, J. J., & Perez-Delgado, C. A. (2020). Vulnerability of blockchain technologies to quantum attacks. *Array*, 10, 100065. <https://doi.org/10.1016/j.array.2021.100065>
- Kholodnaya, E. V. (2022). Quantum technologies as an object of law. *Vestnik Universiteta im. O. E. Kutafina*, 4, 38–45. (In Russ.). <https://doi.org/10.17803/2311-5998.2022.92.4.038-045>
- Kitaev, A., Shen, A., & Vyalı, M. (1999). *Classical and quantum computing*. Moscow: ICNMO, Publishing House of Chero.
- Korolkov, A. V. (2015). On some applied aspects of quantum cryptography in the context of the development of quantum computing and the emergence of quantum computers. *Issues of Cybersecurity*, 1(9), 6–13.
- Korzh, O. V., Andreev, D. Yu., Korzh, A. A., Korobkov, S. V., & Chernyavskiy, A. Yu. (2013). Modeling of the work of an ideal quantum computer with the Lomonosov supercomputer. *Vychislitelnye metody i programmirovaniye*, 2(14), 24–34. (In Russ.).
- Kumar, Adarsh, Pacheco, Diego Augusto de Jesus, Kaushik, Keshav, & Rodrigues, Joel J. P. C. (2022). Futuristic view of the Internet of Quantum Drones: Review, challenges and research agenda. *Vehicular Communications*, 36, 100487. <https://doi.org/10.1016/j.vehcom.2022.100487>
- Naumov, V. B., & Stankovskiy, G. V. (2019). Legal aspects of quantum communications: new horizons. *Probely v rossiyskom zakonodatelstve*, 4, 235–239. (In Russ.).
- Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, 16(5), 38–41. <https://doi.org/10.1109/MSP.2018.3761723>
- Muheidat, F., Dajani, K., & Tawalbeh, L. A. (2022). Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication. *Procedia Computer Science*, 203, 32–40. <https://doi.org/10.1016/j.procs.2022.07.007>
- Petrenko, A. (2022). *Applied Quantum Cryptanalysis*. River Publishers.
- Petrenko, A. S., Petrenko, S. A., & Ozhiganova, M. I. (2021). Model of safety threats according to the analytics of foreign national quantum programs. *Zashchita informatsii. Insayd*, 4 (100), 50–59. (In Russ.).
- Petrenko, S. A., Petrenko, A. S., & Ozhiganova, M. I. (2021). Evaluating the capabilities of quantum algorithms of cryptanalysis. *Zashchita informatsii. Insayd*, 6(102), 70–82. (In Russ.).
- Pozner, R. A. (2004). *Economic analysis of law*. In 2 vol. Vol. 1. Sankt-Peterburg: Ekonomicheskaya shkola, 2004. (In Russ.).
- Ritter, J. (2015). *The Birth of Quantum Law: A Concept Paper*. <https://doi.org/10.13140/RG.2.1.4263.7285>
- Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*, 27, 379–423.
- Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Foundations of Computer Science*, 10, 134–145. <https://doi.org/10.1109/SFCS.1994.365700>
- Shor, P. W. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26, 1484–1509. <https://doi.org/10.1137/S0097539795293172>
- Sigov, A., Ratkin, L., & Ivanov, L. A. (2020). Quantum Information Technology. *Journal of Industrial Information Integration*, 28, 100365. <https://doi.org/10.1016/j.jii.2022.100365>
- Taylor, R. D. (2020). Quantum Artificial Intelligence: A “precautionary” U.S. approach? *Telecommunications Policy*, 44(6), 101909. <https://doi.org/10.1016/j.telpol.2020.101909>
- Yanamadala, S., & Seema, S. (2022). Quantum dots: policy and ethics. In Yarub Al-Douri (Ed.). *Woodhead Publishing Series in Electronic and Optical Materials, Graphene, Nanotubes and Quantum Dots-Based Nanotechnology* (pp. 887–899). Woodhead Publishing. <https://doi.org/10.1016/B978-0-323-85457-3.00031-1>
- Yunakovskiy, S. E., Kot, M., Pozhar, N. O., Nabokov, D., Kudinov, M. A., Guglya, A., Kiktenko, E. O., Kolycheva, E. V., Borisov, A., & Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology*, 8, 1–19. <https://doi.org/10.1140/epjqt/s40507-021-00104-z>

Authors information



Elizaveta A. Gromova – PhD (Law), Associate Professor, Associate Professor of the Department of Entrepreneurial, Competition and Environmental Law, South Ural State University (National Research University)

Address: 78 prospekt Lenina, 454080 Chelyabinsk, Russian Federation

E-mail: gromovaea@susu.ru

ORCID ID: <https://orcid.org/0000-0001-6655-8953>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/AAO-8876-2020>

ScopusAuthorID: <https://www.scopus.com/authid/detail.uri?authorId=57208846603>

Google Scholar ID: <https://scholar.google.com/citations?user=fDz6FkUAAAAJ&hl>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=652593



Sergey A. Petrenko – Doctor of Engineering, Professor, Professor of the Department of Informational Security, Saint Petersburg State Electrotechnical University "LETI" named after V. I. Ulyanov (Lenin); Professor, Innopolis University

Address: 1 Universitetskaya Str., 420500 Innopolis, Russian Federation

E-mail: s.petrenko@innopolis.ru

ORCID ID: <https://orcid.org/0000-0003-0644-1731>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/O-5049-2017>

ScopusAuthorID: <https://www.scopus.com/authid/detail.uri?authorId=57195327289>

Google Scholar ID: https://scholar.google.com/citations?user=x_gez2gAAAAJ&hl=ru

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=805505

Authors' contributions

Elizaveta A. Gromova performed general supervision and set the research tasks, analyzed the Russian and foreign regulation of quantum technologies.

Sergey A. Petrenko analyzed the current state of Quantum computations science and determined the prospective directions of engineering research in this sphere.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – December 1, 2022

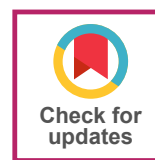
Date of approval – January 18, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 34:620.3:004
EDN: <https://elibrary.ru/wnraoe>
DOI: <https://doi.org/10.21202/jdtl.2023.4>



Медицинские нанороботы в фокусе права

Полина Сергеевна Гуляева 

Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации
г. Москва, Российская Федерация

Ключевые слова

Айзек Азимов,
здравоохранение,
медицина,
медицинский робот,
наноробот,
право,
регулирование,
робототехника,
цифровые технологии,
этика,
in vivo

Аннотация

Цели: формирование доктринальных основ и механики правового регулирования применения медицинских нанороботов, концептуализация идеи наноробототехнического права в границах его базовых дефиниций, норм безопасности, рисков, типологии устройств, юридических параметров технологических терминов.

Методы: познавательный инструментарий представлен в виде интеграции общенаучных и современных специальных юридических методов (в том числе методов сравнительного правоведения, правового моделирования и юридического прогнозирования, NBICS-конвергенции), в совокупности позволяющих выделить в объекте изучения не только собственно правовые, но и антропологические, биомедицинские, информационные, механистические исследовательские проекции.

Результаты: сформулировано авторское определение понятия медицинского наноробота; исследовано правовое содержание и квазиправовые аспекты дефиниции, имеющие значение для теоретического и прикладного развития терминологии; выявлены признаки смежных понятий (биомедицинский робот, наноробототехническая система, медицинская наноробототехническая система), и установлены логические связи между ними; проведена классификация основных видов рисков, связанных с практическим применением медицинских нанороботов; выявлен перечень теоретико-правовых противоречий, которые потенциально способны негативно повлиять на будущее развитие регуляторной практики; рассмотрен отечественный и зарубежный опыт правовой регламентации и доктринального осмысления проблем медицинской наноробототехники (на примере США, Японии, Европы, Китая).

Научная новизна: в условиях междисциплинарного научно-исследовательского вакуума предпринята попытка комплексного рассмотрения понятия медицинского наноробота в технологическом, юридическом и коммуникативном ключе («робот-человек» в наномасштабе) на базе передовых научных изысканий, определяющих основы будущего наноробототехнического права. Синергетическое

© Гуляева П. С., 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.

развитие биомедицинских и смежных технологий, отраженное в моделях робоправа и робоэтики, рекомендовано дополнить относительно самостоятельными концептами наноробоправа и наноробоэтики.

Практическая значимость: на основе анализа действующей в России и за рубежом системы правового регулирования определены механизмы совершенствования отечественного законодательства, в том числе с учетом достижений правового краудсорсинга. В рамках социогуманитарной проблематики формируется вклад в развитие правовой, социологической, психологической науки. Подготовлена научно-методологическая база для дальнейших юридических исследований и правотворческой деятельности в сфере медицинской наноробототехники.

Для цитирования

Гуляева, П. С. (2023). Медицинские нанороботы в фокусе права. *Journal of Digital Technologies and Law*, 1(1), 89–122. <https://doi.org/10.21202/jdtl.2023.4>

Содержание

Введение

1. Медицинские роботы в макро-, микро- и наномасштабе: краткий обзор технологических решений
2. Типы нанороботов: коммуникации человека и робота в формате *in vivo*
 - 2.1. Нанороботы
 - 2.1.1. Молекулярные устройства
 - 2.1.2. Нанодвигатели
 - 2.1.3. ДНК-нанороботы
 - 2.2. Наноманипуляторы
 - 2.2.1. Наноманипуляторы с оптическими, магнитными или акустическими пинцетами
 - 2.2.2. Наноманипуляторы, основанные на атомной микроскопии
 - 2.2.3. Наноманипуляторы, основанные на электронной микроскопии
 - 2.3. Правовой конструкт в коммуникации человека и робота на уровне клетки
3. Три закона наноробототехники
 - 3.1. Первый закон наноробототехники
 - 3.2. Второй закон наноробототехники
 - 3.3. Третий закон наноробототехники
4. Медицинская наноробототехника: регуляторные подходы
5. Концепт медицинского наноробототехнического права: доктринальное осмысление
 - 5.1. Робоправо: зарубежный и отечественный опыт
 - 5.2. Три фундаментальные правовые проблемы будущего развития регуляторики
 - 5.2.1. Проблема определения правовой природы нанороботов
 - 5.2.2. Терминологическая проблема
 - 5.2.3. Деликтная проблема

Выводы

Введение

В результате эволюции социально-экономической сферы было сформировано пять технологических укладов: первая промышленная революция, затем эпохи пара, стали, нефти и телекоммуникаций. В 2000-х гг. ученые подтвердили, что человечество стоит на пороге следующего, шестого нанотехнологического уклада. Футурологи прогнозируют становление эры метакогнитивных технологий к середине XXI в., основой для которых станут качественно новые подходы к восприятию информации (Yuan et al., 2020; Xue, 2022). Шестой нанотехнологический уклад характеризуется конвергенцией сложных самоорганизующихся нано-, био-, инфотехнологических комплексов, порождающих усиление взаимодействия антропологической и технологической среды (Асеева, 2017; Пашенцев и др., 2021). Нанороботы, применяемые в медицине, являются особой сферой для социогуманитарного и правового исследования. Технологии, которые не подчиняются в полной мере законам макромира (законы классической физики) и применяются внутри человеческого организма, представляют интерес для ученых, в том числе в части этических аспектов и юридических рисков¹.

В рамках исследования разработаны базовые концепты и общие подходы к пониманию медицинского наноробототехнического права, включая исследование теоретико-правовых проблем и классификацию рисков. В научной работе сформулированы рекомендации по внесению изменений в российское законодательство.

В статье проведен сравнительно-правовой анализ регуляторных и общетеоретических моделей; в частности, исследован опыт России, Китая, США, Японии и Евросоюза. Российские и зарубежные разработки положены в основу рекомендаций по развитию отечественной теории и практики правового регулирования.

Правовой фокус исследования раскрывает технологическую сущность феномена медицинской наноробототехники. В частности, предложены комплексные междисциплинарные подходы к содержанию понятия медицинского наноробота на основе трех законов Айзека Азимова: приоритета жизни и здоровья человека перед интересами машины, обязанности устройства заботиться о самосохранении и подчинении людям (при условии соблюдения первого и второго правил).

В результате исследования проблем понятийно-категориального аппарата проведены различия и определены дефиниции биомедицинского робота, наноробототехнической системы и медицинского наноробота.

В статье определены фундаментальные проблемы, препятствующие развитию основ регулирования медицинской наноробототехники: вопрос об определении правовой природы нанороботов, терминологическая и деликтная проблемы.

Проведена классификация правовых и неправовых рисков, связанных с будущим регулированием применения медицинских нанороботов в клинической практике. Помимо правовой неопределенности, выделены коммуникативно-этические и коммуникативно-методологические риски, а также риски в области информационной и технологической безопасности.

Автором исследования подготовлены предложения по внесению изменений и дополнений в положения п. 3 ст. 34 Федерального закона от 21 ноября 2011 г. № 323-ФЗ

¹ Fosch-Villaronga, E., & Drukarch, Y. (2021, May). *On healthcare robots*. eLaw Center for Law and Digital Technologies. Leiden University, the Netherlands. <https://arxiv.org/ftp/arxiv/papers/2106/2106.03468.pdf>

«Об основах охраны здоровья граждан в Российской Федерации», в ст. 2 Порядка организации оказания высокотехнологичной медицинской помощи с применением единой государственной информационной системы в сфере здравоохранения, утвержденного приказом Министерства здравоохранения РФ от 2 октября 2019 г. № 824н «Об утверждении порядка оказания высокотехнологичной медицинской помощи с применением единой государственной информационной системы здравоохранения», в ст. 3 Положения об организации оказания специализированной, в том числе высокотехнологичной, медицинской помощи, утвержденного приказом Министерства здравоохранения РФ от 2 декабря 2014 г. № 796н «Об утверждении положения об организации оказания специализированной, в том числе высокотехнологичной, медицинской помощи», дополнить пунктом 6.1 Номенклатурную классификацию медицинских изделий по видам, утвержденную приказом Министерства здравоохранения РФ от 6 июня 2012 г. № 4н «Об утверждении номенклатурной классификации медицинских изделий».

Подготовлены методологические рекомендации по развитию законодательства в соответствии с иерархией нормативных правовых актов.

С точки зрения эволюции права так называемый технологический императив (Хабриева, Черногор, 2020) становится катализатором трансформации базовых концептов в юриспруденции, включая методологические подходы. Новейшие разработки интегрируют естественно-научные, технические, информационные, философские, правовые аспекты. В условиях прогрессирующей междисциплинарности особую актуальность приобретают надотраслевые методы NBICS (нано-, био-, инфо- и когнитивные науки, а также социогуманитарные направления) (Жолобова, Счастливцева, 2020; Jamali et al., 2018; Sweeney, 2020).

Эмпирическую основу статьи составляют зарубежные научные работы, посвященные исследованиям в области наноробототехники, робототехники, нанотехнологий. Список литературы также включает материалы, затрагивающие проблематику классической физики, биофизики, медицины, оптики, микрофлюидики, микробиологии. Такой подбор источников обусловлен необходимостью восполнить пробелы в терминологии как юридической, так и общенаучной. Дефиниция наноробота и медицинского наноробота является инновационной, особенно для гуманитарной и юридической сферы отечественного научного знания. Комплексный подход позволил рассмотреть технологическую природу наноробототехнических систем в правовом измерении. Междисциплинарный характер объекта исследования обусловил выбор конвергентных технологий в качестве методологической основы.

1. Медицинские роботы в макро-, микро- и наномасштабе: краткий обзор технологических решений

Медицинские роботы в последние десятилетия стали основой прорывных достижений в сфере клинической медицины (Fukuda et al., 2010). Новые технологии позволяют сопоставлять информацию о пациентах (результаты лабораторных тестов, диагностических исследований, включающих изображения, визуализацию) (Fortunato et al., 2010) и обобщенную информацию (анатомические атласы, статистика). В круг медицинских задач таких устройств входят хирургические вмешательства, реабилитация или помощь людям с ограниченными возможностями в повседневной жизни (Wenyan et al., 2022). Подобные манипуляции способна осуществлять макромасштабная медицинская робототехника, например, образцы известной фирмы

Da Vinci (Min Sun et al., 2022; Rong Liu et al., 2022). Роботы используются и непосредственно при осуществлении хирургических операций, повышают точность, ловкость, снижают фактор дрожания рук хирургов и обеспечивают возможность манипуляций с труднодоступными участками (Jamali, 2018; Norasi, 2022). Роботы значительно снижают травматизм при проведении операции, сохраняют ресурсы регенерации пациента и улучшают прогноз восстановления. В целях реабилитации послеоперационных больных или пострадавших в результате обширных нарушений были разработаны роботизированные устройства для восстановления функциональности пациентов с проблемами опорно-двигательного аппарата. Перспективным направлением в медицине стала «мягкая» робототехника, которая связана с биосовместимыми материалами и способностью механизмов к биомимикрии. Речь идет об устройствах, созданных из материалов, подобных тканям живых организмов и безопасных для работы непосредственно в контакте с человеком (Suulker et al., 2022; Bartkowski et al., 2022).

Перечисленные достижения в области разработки макромасштабной медицинской аппаратуры показывают влияние робототехники на клиническую медицину и здравоохранение. В таких условиях предполагается, что уменьшение размеров медицинских роботов позволит достигать качественно новых результатов и обеспечит открытия как в сфере клинической практики, так и в области биомедицины.

Для иллюстрации достижений мировой науки предлагается рассмотреть несколько проектов в сфере медицинской наноробототехники.

Наноробот Cyberplasm, разработанный командой медиков, биологов и инженеров, сконструирован по образцу морской миноги и, циркулируя в крови, выполняет диагностические задачи. Устройство обеспечивает свою деятельность благодаря энергии глюкозы в кровотоке².

Проект Bacteriorobot способен автономно определять злокачественные образования, а также способствует эффективной борьбе с ними. Специалисты генетически видоизменили бактерии сальмонеллы, притягивающиеся к раковым клеткам за счет вещества, которое они выделяют. Микроскопические роботы, расположенные в бактерии, автоматически впрыскивают лекарство. Препарат поставляется непосредственно в опухоль, избегая здоровых клеток³.

Также исследователями были разработаны (Marks & Cyr, 2018):

- механический тромбоцит для образования сгустков крови у пациентов с нарушениями свертываемости;
- наноробот для обнаружения тромбов;
- наножел для проведения хирургических вмешательств на отдельных нейронах;
- транспортный наноробот, изготовленный на основе дезоксирибонуклеиновой кислоты⁴ и способный доставить полезную нагрузку к клеткам-мишеням.

² Поезжаева, Е. В. (2020). *Искусственный интеллект в теории механизмов машин и робототехнике*: учебное пособие. В 3 ч. Ч. I. Пермь: Изд-во Пермского национального исследовательского политехнического университета.

³ Kriorus. <https://kriorus.ru/news/Yuzhnokoreyskim-uchenym-udalos-ispolzovat-nanoroboty-v-medicine>

⁴ Дезоксирибонуклеиновая кислота (ДНК) – макромолекула, обеспечивающая хранение и передачу информации из поколения в поколение и реализацию генетической программы развития и функционирования живых организмов. Молекула ДНК хранит биологическую информацию в виде генетического кода, состоящего из последовательности нуклеотидов.

Одним из главных вызовов при разработке нанороботов до недавнего времени оставалась проблема создания нанодвигателей, а именно энергоэффективного источника питания для устройства. В 2020 г. ученые приблизились к предельным минимальным размерам, создав нанодвигатель, имеющий диаметр примерно в 100 тысяч раз меньше человеческого волоса, который состоит всего из 16 атомов и является на сегодняшний день самым миниатюрным в мире. Двигатель способен вращаться в заданном направлении. Изобретение позволяет собирать энергию на атомном уровне, например, рассеянное тепло, чтобы затем преобразовывать ее в механическое движение, которое возможно использовать в различных целях, в том числе медицинских⁵.

Важно отметить, что сфера медицинской наноробототехники, хотя и является инновационной, но давно вышла за пределы форсайт-дискуссии: прототипы и серийные устройства тестируются пациентами по всему миру. Несмотря на наличие некоторого отставания в развитии технологий в нашей стране, вероятно, в скором будущем подобные проекты появятся и в России, кроме того, возможно применение образцов иностранного производства.

2. Типы нанороботов: коммуникации человека и робота в формате *in vivo*

Научные термины «*in vivo*» и «*ex vivo*» буквально переводятся с латыни как «внутри живого организма» и «вне живого организма». Высокотехнологичная медицина предусматривает все больше атравматичных *in vivo* методик направленного действия, исключающих повреждение здоровых органов, тканей и даже клеток.

Согласно Федеральному закону от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»⁶, высокотехнологичная помощь представлена в виде клеточных технологий, генной инженерии, инструментов с применением роботизированной техники (ст. 34, п. 3).

Медики подтверждают, что функционал микро- и нанороботов применим для различных биомедицинских и медицинских устройств, в том числе в целях клеточных манипуляций и имитации биосигналов, адресной доставки лекарств, минимально-инвазивной хирургии, медицинской диагностики, детоксикации (J. Li et al., 2017). Микророботы применяются в масштабе от отдельных молекул до систем и органов человеческого тела. Устройства способны зондировать ионы и небольшие молекулы, в том числе белки. Наноманипуляторы на основе пинцета пригодны для обработки биологических образцов размером от нескольких нанометров (например, белки) до десятков микрометров (например, клетки). После введения нанороботов в кровеносный сосуд такие устройства, несущие молекулы вещества, перемещаются в пораженные участки в организме, а затем высвобождают лекарство. Нанодвигатели могут не только зондировать отдельные клетки, но и проходить через биожидкости в желудочно-кишечном тракте в целях выполнения задач точечной хирургии (M. Li et al., 2021).

⁵ Создан нанодвигатель, состоящий всего из 16 атомов и работающий на границе между классической физикой и квантовой механикой. <https://www.atomic-energy.ru/news/2020/06/30/104950>

⁶ Об основах охраны здоровья граждан в Российской Федерации. № 323-ФЗ. (2011). *Собрание законодательства Российской Федерации*, 48, ст. 6724.

Исследователи предполагают, что до настоящего времени не существует стандартного определения терминов «микроробот» и «наноробот», но существует точка зрения, согласно которой более общий термин «микроробот» включает все смежные понятия и характеризует устройства размером от 1 нанометра (диаметр среднестатистического атома составляет примерно 0,1 нанометра) (Diller & Sitti, 2013).

В современной литературе принято понимать под наноробототехническими системами группы устройств, обозначенные как нанороботы и наноманипуляторы (Хабриева, Черногор, 2020).

2.1. Нанороботы

Группа нанороботов включает следующие типы устройств:

- молекулярные устройства размером 1–20 нанометров, способные совершать механические движения под воздействием внешних раздражителей;
- нанодвигатели размером от 10 нанометров до 10 мюметров, которые обладают способностью использовать световую, химическую, магнитную, ультразвуковую, электрическую и иную энергию окружающей среды;
- нанороботы, сконструированные по технологии так называемого ДНК-оригами, длиной 5–100 нанометров, пригодные для транспортировки лекарств с возможностью молекулярного распознавания.

2.1.1. Молекулярные устройства

Молекулярные устройства могут функционировать за счет взаимодействия отдельных молекул размером чуть более или менее нанометра. Естественным прототипом молекулярных устройств является, например, молекула АТФ (аденозинтрифосфат)⁷. Ученые признают, что искусственные молекулы не заменяют естественных, но помогают осуществлять с ними желаемые манипуляции. Молекулярные устройства пригодны для работы в липидных слоях в целях переноса ионов и способны исследовать внутриклеточное пространство, проходя сквозь клеточные мембраны. Наноробот удерживается на расстоянии от поверхности при помощи своих химических свойств и способен осуществлять автономное движение, а запуск осуществляется благодаря использованию энергии окислительно-восстановительных процессов, света и тепла (Erbaş-Cakmak et al., 2015; Chen et al., 2018).

2.1.2. Нанодвигатели

Нанодвигатели представляют собой наноразмерные устройства, предназначенные для выполнения отдельных механических движений (например, вращение, раскачивание, перемещение, доставка, сжатие) в ответ на определенные стимулы (Guix et al., 2014). Различные типы таких устройств широко применяются для имитации биосигналов, доставки лекарств, диагностики, изоляции раковых клеток (Wang & Pumera, 2015). Основной классификацией нанодвигателей является разделение на топливные и бестопливные механизмы. В 2015 г. был разработан

⁷ Аденозинтрифосфат, или аденозинтрифосфорная кислота, – универсальный источник энергии для всех биохимических процессов, протекающих в живых организмах.

магнитно-акустический гибридный бестопливный нанодвигатель⁸, который состоит из магнитной нанопружины и наноустройства и способен использовать энергию магнита или ультразвука. Разработка механизмов, способных работать в бестопливном режиме, является перспективной сферой научных исследований, в частности, растет интерес к использованию внешних полей, таких как магнитные, электрические, акустические или световые, для приведения в движение нано- или микроустройств (Villa & Pumera, 2019). Значительные усилия были направлены на создание двигателей с химическим приводом, основанных на поверхностном каталитическом разложении топлива, содержащегося в растворе перекиси водорода. Особое внимание было уделено каталитическим нанопроволочным и микротрубчатым двигателям. Такие устройства основаны на движущей силе пузырьков кислорода и обладают сравнительно высокой мощностью, необходимой для выполнения различных биомедицинских задач (Wang & Wei, 2012).

2.1.3. ДНК-нанороботы

ДНК-нанороботов часто относят к подгруппе нанодвигателей, которые функционируют «на базе принципов ДНК». На самом деле методика так называемого ДНК-оригами была создана в 2006 г. и представляет собой технологию, сконструированную на базе природного прототипа дезоксирибонуклеиновой кислоты. Такое устройство использует запрограммированные комбинации сотен коротких комплементарных олигонуклеотидов⁹. Фрагменты складываются посредством точных 2D- и 3D-форм в большую одиночную нить «каркасной» ДНК, стабилизированную тысячами пар оснований. ДНК-оригами позволяет осуществлять самосборку дискретных объектов снизу вверх с субнанометрическими точными характеристиками (размерами от нанометра до микрометра и массой молекул до гигадалтонного масштаба). С использованием ДНК-оригами был сконструирован широкий спектр функциональных статических наноструктур и динамических наноустройств (Rothemund, 2006).

2.2. Наноманипуляторы

Наноманипуляторы отличаются большими размерами по сравнению с группой нанороботов и представлены в виде:

- наноманипуляторов, оборудованных оптическим, магнитным или акустическим пинцетом, подобным концевому эффектору¹⁰, которые осуществляют бесконтактную обработку биологических образцов в наномасштабе;
- наноманипуляторов, оснащенных функционалом атомной микроскопии, которые манипулируют биологическими образцами в воздушной, жидкой и иных средах, имитируя концевой эффектор при помощи наноразмерного наконечника;
- наноманипуляторов, усиленных электронной микроскопией, которые осуществляют свою деятельность на основе электронной визуализации.

⁸ Разработан бестопливный наномотор. (2015, 30 июня). <https://www.the-submarine.ru/news/1653>

⁹ Олигонуклеотид – короткий фрагмент ДНК или РНК (рибонуклеиновая кислота), получаемый путем химического синтеза или расщеплением более длинных полинуклеотидов.

¹⁰ В молекулярной биологии и биохимии под термином «эффектор», или «эффекторная молекула», обычно понимается малая небелковая молекула, которая селективно связывается с теми или иными белками и регулирует их биологическую активность.

2.2.1. Наноманипуляторы с оптическими, магнитными или акустическими пинцетами

Наноманипуляторы с оптическими, магнитными или акустическими пинцетами позволяют проводить точные действия с биологическими образцами. Например, оптические пинцеты – это инструменты, основанные на плотно сфокусированном лазерном луче, который способен улавливать и манипулировать широким спектром частиц в своем фокусном пятне. С момента изобретения в 1970 г. оптические пинцеты широко применялись в таких научных областях, как атомная физика, оптика и биологические науки. Используя сильно сфокусированный луч света, оптические пинцеты могут функционировать как специальные конечные эффекторы роботов для захвата и бесконтактного перемещения объектов размером от десятков нанометров до десятков микрометров. Недавние исследования продемонстрировали возможности роботизированной системы оптического пинцета для манипуляций *in vivo* отдельными клетками в среде кровотока (X. Li et al., 2017).

Помимо клеток, оптические пинцеты способны манипулировать отдельными молекулами, такими как белки и нуклеиновые кислоты¹¹, что позволяет добиться значительных успехов в исследовании структурной динамики и информации о молекулах. Молекула крепится к оптически захваченному шарiku, в то время как свободный конец молекулы прикреплен к другому шарiku, который удерживается в независимой оптической ловушке. Перемещение оптически захваченного шарика приводит к растяжению или расслаблению молекулы. Такие исследования дают новое представление о различных молекулярных и клеточных изменениях: например, о связывании гормона и активации рецептора, молекулярных механизмах и двигателях, напряжении плазматических мембран¹² в клетках (Gardini et al., 2018).

Наноманипуляторы с магнитными и акустическими пинцетами являются объектом научных исследований в области классической физики, биофизики, оптики, микрофлюидики, микробиологии (Wang et al., 2022; Kuijpers et al., 2022; Jingui et al., 2020). Магнитные пинцеты в молекулярной биологии рассматриваются как аналог оптических пинцетов и представляют собой устройство, способное на манипуляции с условно тяжелыми образцами, если находятся в непосредственной близости от магнита (Neuman & Nagy, 2008). В современных условиях магнитные пинцеты используются для биологического обнаружения и адресной доставки благодаря своим уникальным характеристикам движения, способности без вреда для организма проникать через биологические ткани и возможности беспроводного дистанционного управления (Deng et al., 2023). При помощи акустического пинцета возможна трехмерная акустическая манипуляция с образцами в масштабе от миллиметра до нанометра. Акустические пинцеты представляют собой инновационную технологию, основанную на применении силы акустического излучения, создаваемого ультразвуковыми волнами (Qi et al., 2021).

¹¹ Нуклеиновая кислота – высокомолекулярное органическое соединение, биополимер, образованный остатками нуклеотидов. Нуклеиновые кислоты ДНК и РНК присутствуют в клетках всех живых организмов и выполняют важнейшие функции по хранению, передаче и реализации наследственной информации.

¹² Плазматическая мембрана (клеточная мембрана, цитолемма, плазмалемма) – эластическая молекулярная структура, состоящая из белков и липидов.

2.2.2. Наноманипуляторы, основанные на атомной микроскопии

Наноманипуляторы, основанные на атомной микроскопии, обеспечивают новый способ обработки биологических образцов, исследуемых в физиологических условиях (например, в жидкостях). Достижения последнего десятилетия показали, что такой наноманипулятор способен исследовать поведение отдельных клеток и молекул в клинических условиях. Интеграция атомной микроскопии с робототехникой позволяет создать наноробототехнический манипулятор, который может обрабатывать нанообъекты, открывая новые возможности для биомедицинского применения. На основе такой микроскопии с использованием дополненной реальности и методов тактильной и визуальной обратной связи оператор может управлять нанозондом. Роботизированный конечный эффектор позволяет осуществлять операции с нанообъектами с помощью джойстика, точно определяя положение наконечника зонда. Устройства могут выполнять механические манипуляции: толкание, резку, деформацию, прикосновение (M. Li et al., 2019).

В сочетании с микрофлюидикой¹³ такая процедура позволяет зонду доставлять лекарства в отдельные клетки и манипулировать ими с помощью микроканальных кантилеверов с наноразмерными отверстиями (Guillaume-Gentil et al., 2014), а также производить электрические измерения и анализ ионов и биомолекул (Aramesh et al., 2019). Для зондирования клетки с использованием наноманипулятора, основанного на атомной микроскопии, необходимо провести иммобилизацию клеток.

2.2.3. Наноманипуляторы, основанные на электронной микроскопии

Наноманипуляторы, основанные на электронной микроскопии, открывают новые возможности для роботизированных наноманипуляций. Система электронного микроскопа включает манипулятор как устройство, несколько микроскопий («глаза»), различные конечные эффекторы, в том числе консоли и пинцет («пальцы»), и различные типы датчиков.

Для обычного электронного микроскопа характерна низкая скорость обработки изображений и небольшая область сканирования, пропускная способность при этом ограничена (Shi et al., 2016). Кроме того, динамические процессы между наконечником и нанообъектами не могут быть непосредственно визуализированы. Сочетание робототехники с электронным микроскопом дает новый тип наноманипулятора, который визуально обеспечивает точную и быструю визуализацию и наноманипуляцию. Такие системы включают сканирующий электронный микроскопический наноматериал, просвечивающий электронный микроскопический наноматериал и сканирующую электронную микроскопию окружающей среды. Наноманипулятор позволяет воздействовать на отдельные биологические клетки и способен работать в газовой среде, дает возможность проводить морфологическую визуализацию биологических образцов, содержащих влагу (Muscariello et al., 2005).

¹³ Микрофлюидика – междисциплинарная наука, описывающая поведение малых объемов и потоков жидкостей.

2.3. Правовой конструкт в коммуникации человека и робота на уровне клетки

В научных исследованиях технологический контекст в понимании природы нанороботов нередко преобладает над правовыми и гуманитарными аспектами; по этой причине представляется особенно важным выявить юридические аспекты в содержании инновационного объекта. Правовая сущность медицинской наноробототехники раскрывается через изучение специфики общественных отношений, возникающих в результате практики применения устройств. Данные общественные отношения определяются следующими факторами:

- назначение устройств (терапевтический, диагностический, хирургический);
- субъектный состав участников разработки, обслуживания и применения устройства (медицинский персонал и специалисты с техническими компетенциями, сотрудники медицинских учреждений или организаций, занятых в производстве и обслуживании технологичных устройств);
- функционал медицинских нанороботов (прохождение сквозь среды, в том числе сквозь барьеры, транспортировка и высвобождение лекарств, таргетирование, имитация или, наоборот, удаление фрагментов, например, тромбоцитов, манипуляция биологическими образцами, детоксикация, интернализация и др.);
- качество автономности устройства (управляется непосредственно медицинским персоналом при помощи джойстика или внешнего излучения, работает на основе заложенной программы либо руководствуясь индивидуальными физиологическими показателями пациента).

Разнообразие возможностей и особые условия применения медицинских нанороботов обуславливают комплексный характер общественных отношений. Речь идет о взаимодействии робота и человека в условиях *in vivo*. Вопросы коммуникации наноробота и пациента, наноробота и врача, наноробота и технического специалиста, а также распределение ответственности между ними являются важнейшей сферой регулирования. Значимыми являются проблемы, связанные с применением наноустройств без волеизъявления человека, а также в условиях возможных религиозных и этических ограничений пациента или родственников.

3. Три закона наноробототехники

Для современной научной литературы, посвященной изучению роли и места цифровых инноваций в социальной реальности, характерно сочетание гуманитарных и технологических подходов. Так, в китайском исследовании отражена методология комплексного восприятия феномена микроскопических биомедицинских устройств на основе трех законов робототехники Айзека Азимова (T. Li et al., 2022). Предлагается исследовать данную модель в контексте наноробототехники.

3.1. Первый закон наноробототехники

Первый закон робототехники гласит: «Робот не может причинить вред человеку» (Azimov, 1942). В масштабе наноустройств, функционирующих в условиях *in vivo*, это указывает на необходимость обеспечения биосовместимости материалов, которую можно разделить на биологическую реакцию и реакцию материала. Биологическая реакция включает реакцию крови, иммунитета и тканей, возникающую в процессе

взаимодействия робота со средой. Реакция материала относится к изменениям физических и химических свойств устройства после попадания в организм человека. Согласно исследованиям, биосовместимый материал представляет собой соответствующие органические молекулы и полимеры с модулями и структурой, близкими к реальным биологическим клеткам и тканям. Биосовместимость материалов учитывает такие характеристики, как иммуногенность, токсичность используемых для изготовления веществ и отходов функционирования устройства, влияние излучений наноустройства на клетки и ткани. На современном этапе отмечается значительное количество исследований по тематике биосовместимости, а применение подобных материалов в биомедицине при разработке *in vivo* методик является инновационной областью научного знания (Naidoo, 2021).

В контексте обеспечения безопасности человека от угроз жизни или здоровью, а также правовых рисков, связанных с нарушением его прав, значимым является вопрос о репликации микроустройств, находящихся внутри организма пациента.

3.2. Второй закон наноробототехники

Второй закон робототехники, сформулированный для нанобиомедицины, подразумевает, что «наноробот должен поддерживать собственное существование, пока его самозащита не противоречит первому закону» (Azimov, 1942), что указывает на необходимость уклоняться от всего, что приведет к потере активности, до момента выполнения медицинской задачи.

В качестве примера можно привести китайское исследование противоопухолевого наноробота, который в обычных условиях должен пройти четыре стадии, чтобы проникнуть в опухолевые клетки (внутривенная инъекция в кровоток, накопление в месте опухоли за счет инфильтрации, эффекта удерживания или нацеливания, проникновение в опухолевую ткань, интернализация¹⁴) (Xu et al., 2017). Ученые отмечают, что на первом этапе нанороботы, вводимые внутривенно, должны обладать хорошей дисперсностью, чтобы сохранять способность циркулировать в крови в течение длительного времени. Однако, когда устройства попадают в кровь, их поверхность быстро покрывается молекулами белка, образуя «белковую корону» (Wan et al., 2021). Очевидно, что белковая корона изменит размер, стабильность и свойства поверхности нанороботов и таким образом повлияет на их способность нацеливаться, клеточное поглощение, внутриклеточный транспорт, фармакокинетику¹⁵, биологическое распределение и токсичность. Нанороботы также могут быть захвачены иммунными клетками в кровеносной системе, в тканях и органах. Препятствиями являются в том числе биологические барьеры, такие как гематоэнцефалический барьер¹⁶, осложняющий доставку некоторых видов нанороботов.

¹⁴ Интернализация (в контексте медицины) – погружение молекул внутрь клетки.

¹⁵ Фармакокинетика – раздел фармакологии, изучающий кинетические закономерности химических и биологических процессов, происходящих с лекарственным средством в организме животного или человека.

¹⁶ Гематоэнцефалический барьер участвует в поддержании систем саморегуляции мозга, защищает нервную ткань от циркулирующих в крови микроорганизмов, токсинов, различных факторов иммунной системы, которые воспринимают ткань мозга как чужеродную. Гематоэнцефалический барьер выполняет функцию высокоселективного фильтра, через который из артериального русла в мозг поступают питательные, биоактивные вещества и выводятся продукты жизнедеятельности нервной ткани.

3.3. Третий закон наноробототехники

Третий закон Айзека Азимова в измерении наноустройств заключается в том, что «наноробот должен подчиняться приказам, отдаваемым людьми, или посредством действий не допускать причинения вреда человеку, за исключением случаев, когда такие приказы или действия противоречат первому или второму закону» (Azimov, 1942). Это означает, что управляемость нанороботов включает в себя не только направление и траекторию автономного движения устройства, но также количество загружаемых лекарств и режим замедленного высвобождения вещества.

Разработано довольно большое количество способов таргетирования устройства, например, векторное поле может быть создано в физиологической среде с помощью внешнего сигнала. Тогда робот будет получать направленную движущую силу извне, чтобы управляемо перемещаться. При этом нанороботы остаются уязвимыми для вмешательства случайного броуновского движения (You et al., 2018).

В некоторых исследованиях разработаны хемотаксические¹⁷ устройства, способные «нацеливаться» в зависимости от градиента концентрации глюкозы, активных форм кислорода и факторов воспаления в физиологических поражениях (Ji et al., 2019).

Несмотря на огромный выбор способов таргетирования, невозможно предусмотреть все индивидуальные реакции организма человека при проведении медицинских процедур, например, отмечаются очевидные различия в стратегиях химического распознавания, т. е. уровни экспрессии рецепторов на поверхности пораженных клеток варьируются от индивидуума к индивидууму в зависимости от типа заболевания и патологического состояния (Taherkhani et al., 2014).

4. Медицинская наноробототехника: регуляторные подходы

Проблематика применения медицинских нанороботов является актуальной и дискуссионной темой, которая характеризуется высокими темпами обновления технологических решений. В целях предотвращения правового и административного вакуума предлагается сформулировать общие характеристики современных систем регулирования данной сферы:

- отсутствие специализированного федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере оборота и применения медицинских нанороботов;
- межведомственный характер инициатив и предложений рабочих групп, отвечающих за выработку концептуальных решений в рассматриваемой области;
- регулирование посредством подзаконных либо мягкоправовых актов;
- применение общих норм федерального законодательства о здравоохранении, например, норм о медицинских изделиях;
- проблемы юридической техники, например, отсутствие полноценного понятийно-категориального аппарата в сфере медицинской наноробототехники.

¹⁷ Хемотаксис – двигательная реакция микроорганизмов на химический раздражитель.

Международная повестка на начальном этапе была представлена деятельностью институтов Организации Объединенных Наций (далее – ООН) и отражена в докладе UNESCO 2008 г. «Нанотехнологии и этика: политика и направления деятельности»¹⁸; в документе сформулированы роль и значение нанотехнологий для мира и ООН, представлены этические, правовые и политические аспекты развития и применения инноваций, перспективы и риски для общества, науки и окружающей среды¹⁹.

В качестве примера зарубежной регуляторной практики и технологической политики предлагается рассмотреть успешный опыт Соединенных Штатов Америки (далее – США). Так, в 2000 г. была запущена Национальная нанотехнологическая инициатива²⁰, которая стала координатором более 20 правительственных департаментов и агентств, работающих над различными проектами в данной сфере. При этом регулирование не осуществляется специальным органом, а в основном двумя ведомствами: Управлением по контролю за продуктами питания и лекарствами США (далее – FDA), которое утверждает перечень медицинских изделий, и Управлением по патентам и товарным знакам США. Под эгидой FDA в 2006 г. была создана Целевая группа по нанотехнологиям, которая инициировала разработку механизма регулирования нанороботов и связанных с ними технологий. В декабре 2017 г. соответствующий проект руководства был выпущен Центром оценки и исследований лекарственных средств FDA и Центром оценки и исследований биологических препаратов, которые предположительно применимы для регулирования нанороботов. Проект включает нормы, касающиеся лекарственных средств и биологических продуктов, содержащих наноматериалы. В документе отмечается неопределенность относительно того, применимы ли указанные нормы к нанороботам и в какой степени. В проекте отражено, в частности, как с наноматериалами можно обращаться при разработке новых лекарственных средств. При этом в документах FDA нет установленных определений терминов «нанороботы», «нанотехнология», «наноматериал» (Norasi et al., 2022).

Европейская модель регулирования робототехники, получившая известность в мире благодаря емкому концепту RoboLaw²¹, содержит нормы о роботах, помогающих пожилым и больным людям в реабилитации и улучшении качества жизни, а также об устройствах, направленных на восстановление и компенсацию работы органов и тканей человека, в том числе «носимые на теле и имплантируемые»²².

В Китайской Народной Республике модель регулирования робототехники представлена в таких документах, как Глобальная государственная программа развития

¹⁸ Нанотехнологии и этика: политика и направления деятельности. (2008). https://unesdoc.unesco.org/ark:/48223/pf0000152146_rus

¹⁹ UNESCO. *The ethics and politics of nanotechnologies*. (2006). https://kelty.org/or/papers/Kelty_UNESCO_Ethics_PoliticsofNano_2006.pdf

²⁰ National Nanotechnology Initiative. (2000). <https://www.nano.gov>

²¹ RoboLaw. *Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics*. <https://www.robolaw.eu/projectdetails.htm>

²² Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Resolution 2015/2103 (INL) of the European Parliament of 16 February 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf

«Made in China 2025»²³ и План развития робототехнической отрасли. При этом в Китае отсутствует полноценный закон о роботах или иной концептуальный документ (Незнамов, Наумов, 2017).

Первой попыткой выработки норм о нанотехнологиях в России можно считать Постановление Правительства Российской Федерации от 23 апреля 2010 г. № 282 «О национальной нанотехнологической сети»²⁴. В документе, в частности, содержатся определения понятий «наноиндустрия», «наносистема», «нанотехнологии», «продукция наноиндустрии», «национальная нанотехнологическая сеть».

В части разработки концептуальных подходов интересным экспериментом стала Модельная конвенция о робототехнике и искусственном интеллекте 2017 г.²⁵ Рамочный документ определяет основные термины, нормы безопасности и этики в сфере робототехники, а также общие вопросы учета и оборота устройств. В числе прочего авторами ставится вопрос о правосубъектности роботов: указано, что в гражданском обороте робот может выступать субъектом права и являться собственником другого робота.

В части регулирования робототехники, применяемой в медицине, важным является Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»²⁶, который, в частности, определяет в ч. 3 ст. 34 содержание понятия высокотехнологичной медицинской помощи, включающего «клеточные технологии» и применение «роботизированной техники». Отраслевые подзаконные акты полностью дублируют текст указанной нормы федерального закона^{27, 28}.

Перечень конкретных медицинских устройств, представленный в Номенклатурной классификации медицинских изделий по видам, утвержденной приказом Министерства здравоохранения РФ от 6 июня 2012 г. № 4н «Об утверждении номенклатурной классификации медицинских изделий»²⁹, в частности, указывает в п. 6 на «медицинские изделия для манипуляций/восстановления тканей/органов человека»³⁰, разновидностью которых, согласно п. 6.3, являются «материалы для реконструкции тканей»³¹. Некоторые типы медицинских нанороботов могут быть

²³ *Made in China 2025: The Plan to Dominate Manufacturing and High-Tech Industrie*. (2022, June 22). <https://www.fdicchina.com/blog/made-in-china-2025-plan-to-dominate-manufacturing/>

²⁴ Постановление Правительства Российской Федерации № 282 от 23.04.2010. (2010). *Собрание законодательства Российской Федерации*, 18, ст. 2250.

²⁵ *Модельная конвенция о робототехнике и искусственном интеллекте*. <https://robopravo.ru/uploads/s/z/6/g/z6gj0wkwhv1o/file/6dbrNqgu.pdf>

²⁶ Об основах охраны здоровья граждан в Российской Федерации № 323-ФЗ от 21.11.2011. *Собрание законодательства Российской Федерации*, 48, ст. 6724.

²⁷ Приказ Министерства здравоохранения Российской Федерации № 824н от 02.10.2019. (2019, 25 ноября). <https://normativ.kontur.ru/document?moduleId=1&documentId=348761>

²⁸ Приказ Министерства здравоохранения Российской Федерации № 796н от 02.12.2014 (2015, 4 февраля). <https://base.garant.ru/70859232/>

²⁹ Приказ Министерства здравоохранения Российской Федерации от 6 июня 2012 г. № 4н. (2012). *Российская газета*, 245.

³⁰ Там же.

³¹ Там же.

отнесены к указанным наименованиям, однако для устройств, адресно доставляющих токсичные лекарства или осуществляющих хирургические задачи, такая формулировка представляется недостаточно точной и полной.

Среди проектов правовых актов можно отметить предложенный законодателю федеральный закон «Об обороте роботов, их составных частей (модулей)» (Бегишев, 2021). В документе представлен, в частности, понятийный аппарат, включающий дефиниции «робот», «робототехника», определены различные типы устройств, такие как «служебный робот» и «гражданский робот», сформулированы классификация роботов и требования к безопасности устройств, в том числе информационной. В проекте также отражены аспекты регулирования оборота военных и иных роботов специального назначения.

Вопросы регламентации применения медицинских нанороботов представляют собой комплексную область правовой регламентации, которая в достаточной степени не реализована ни на международном, ни на национальном уровне. В таком случае представляется важным подготовить научно-методологическую базу будущих законотворческих инициатив в сфере регулирования наноробототехники.

5. Концепт медицинского наноробототехнического права: доктринальное осмысление

В отечественной и зарубежной правовой доктрине не представлено достаточное количество академических статей и монографий, связанных с осмыслением роли наноробототехники, особенно медицинской. При этом существует множество работ, посвященных изучению основ регулирования робототехники и искусственного интеллекта, которые возможно экстраполировать на исследуемую область. Весь спектр подходов предлагается классифицировать следующим образом:

1. Научные работы в области отраслевого регулирования посвящены вопросам применения технологических решений и сфокусированы на гражданско-правовых и уголовно-правовых аспектах, включают вопросы ответственности, прикладной терминологии и регламентации применения устройств (Бегишев, Хисамова, 2018; Кибальник, Волосюк, 2018; Морхат, 2018a; Vale et al., 2022).

2. Научные статьи, касающиеся концептуальных подходов, в таких областях, как правовой статус автономных устройств, проблемы их гипотетической правосубъектности, прогнозирование и форсайт; данные материалы содержат положения о предлагаемых документах, фундаментальные исследования правовой природы технологий, теоретические подходы к пониманию дефиниций (Пашенцев, 2019; Khisamova & Begishev, 2019; Малько, 2019; Понкин, Редькина, 2019; Морхат, 2018b; Gellers, 2021; Mulgan, 2019).

5.1. Робоправо: зарубежный и отечественный опыт

В качестве примера зарубежных изысканий можно привести статью японского правоведа, которая пользуется особой популярностью среди ученых. В работе рассматриваются нормы законодательства и аспекты государственной политики Японии о роботах. Причиной разработок в данной сфере названа необходимость компенсировать снижение количества рабочей силы вследствие повышения среднего возраста населения. В исследовании представлен обзор правовых актов, содержащих актуальные

нормы: Закон о дорожном движении, Закон о радио, Закон о строительных стандартах, Закон об иностранной валюте и внешней торговле. Также рассмотрены вопросы правового статуса роботов, стандартизации, юридической ответственности, возникающей при использовании робототехники. В качестве медицинских устройств, значимых для японского общества и экономики, отмечены роботы-сиделки и роботы-помощники для сестринского ухода за больными или пожилыми людьми. По данной теме в работе отражены вопросы регулирования макроразмерных медицинских устройств без учета проблематики наноробототехники (Nambu, 2016).

В Японии, как и во всем мире, распространена методология так называемого робоправа, т. е. правового и этического регулирования сферы робототехники. Японская адаптация концепции к вопросам медицинских нанороботов включает меры гражданского, административного и уголовного воздействия; в частности, предложено разработать правовой механизм, сочетающий инструменты мягкого и жесткого права. В качестве нормативно-правовой базы предлагается создание единого Основопологающего закона о нанотехнологиях и робототехнике, а в части инструментов гражданского общества предложено сформировать кодекс так называемой наноэтики, или робоэтики (Katsunori, 2012).

Европейская модель робоправа исследует необходимость создания «особого случая» для робототехники из-за способности устройств к самостоятельным действиям (Palmerini et al., 2016). В зарубежной научной литературе отмечается, что наличие у программ и устройств значительной степени автономности позволяет говорить о признаках субъекта права (Mulgan, 2019; Frana & Klein, 2021).

В правовой дискуссии стран СНГ сохраняются опасения в отношении наделения автономных устройств качествами правосубъектности. В научной литературе отмечается, что автономные программы и устройства, несмотря на их инновационный характер, не следует «очеловечивать», поскольку технологии не обладают индивидуальностью, душой, сознанием, чувствами, морально и материально значимыми интересами (Понкин, Редькина, 2018). В фокусе медицинской наноробототехники вопрос об автономности видится иначе, в частности, в контексте вышеупомянутой модели, основанной на законах функционирования роботов Айзека Азимова. Критерий подчинения робота человеку и выполнения им своей функции в полном соответствии с программой или будучи управляемым можно считать важнейшим в данной сфере. В таком контексте представляется значимым вопрос о мерах безопасности и ограничениях, связанных с оборотом и применением медицинских нанороботов. Например, запрет или ограничения для так называемых репликаторов (роботов, способных к созданию собственных копий), поскольку в процессе такой деятельности возможно наступление непредвиденных и неблагоприятных последствий для здоровья или жизни пациента.

Критика робоправа основана на положении о снижении роли права и академической юридической науки в условиях цифровой трансформации. Сторонники такой точки зрения отмечают, что кодированное право вытеснит юристов и заменит их техническими специалистами. Вследствие тенденций к технологической сингулярности³² автоматизированное право займет место традиционных норм и судебных решений (Astromskis, 2018).

³² Технологическая сингулярность – гипотетический момент в будущем, когда научно-технический прогресс приведет к радикальным изменениям в функционировании человеческой цивилизации.

5.2. Три фундаментальные правовые проблемы будущего развития регуляторной среды

Актуальными инструментами развития законодательства на современном этапе являются методы правового моделирования, юридического прогнозирования и прогнозного правотворчества. В целях реализации принципов современной юридической методологии предлагается рассмотреть теоретико-правовые противоречия, которые могут негативно повлиять на развитие регуляторики в области медицинской наноробототехники.

5.2.1. Проблема определения правовой природы медицинских нанороботов

Вопросы правового статуса инновационных технологических разработок уходят корнями в дискуссию о гипотетической правосубъектности макророботов и искусственного интеллекта (Гуляева, 2022). В измерении проблематики медицинских нанороботов отмечаются следующие противоречия:

- проблема правового статуса медицинского наноробота с учетом степени автономности и самообучаемости устройства;
- гетерогенность правовых статусов устройств с различными техническими и функциональными характеристиками;
- вопросы разграничения содержания понятия наноробота как физического устройства либо как комплексного объекта, включающего программное обеспечение;
- сложности доктринального характера, связанные с отнесением медицинского наноробота к категориям объекта либо субъекта права;
- применимость к нанороботу категории квазисубъекта права, а также решение вопроса о гипотетической правосубъектности устройства.

5.2.2. Терминологическая проблема

Другое значимое теоретико-правовое противоречие касается проблем, обозначенных в рамках исследования вопросов унификации понятийного аппарата информационного права (Бачило, 2015, 2017). В контексте тематики статьи речь идет о следующих вопросах:

- отсутствие структурированного понятийно-категориального аппарата и понимания разницы между смежными понятиями и категориями разного уровня, например, «биомедицинский робот», «наноробототехническая система», «медицинский наноробот»;
- двойственность, связанная с правовой идентификацией сущности наноробота и его программного обеспечения;
- большое количество технологических терминов, не относящихся к терминологии юриспруденции и смежных гуманитарных наук.

5.2.3. Деликтная проблема

Вопрос о распределении ответственности за неблагоприятные последствия деятельности медицинского наноробота раскрывает следующие теоретико-правовые аспекты:

- разграничение ответственности за последствия деятельности самого устройства и его программного обеспечения;

– разграничение ответственности за последствия применения наноробота между медицинским персоналом, техническими специалистами, разработчиками.

Выводы

Медицинские нанороботы как объект исследования представляют собой сложный комплексный феномен, включающий различные технологические, этические, юридические аспекты. Междисциплинарный характер общественных отношений, формируемых новейшими биомедицинскими технологиями, распространяется далеко за пределы смежных гуманитарных и правовых наук. Предполагается, что трансформация юридической практики в будущем потребует от юристов специальных компетенций в сфере биомедицины. Вопросы коммуникации робота и человека представляются по-новому, когда наноустройства применяются буквально внутри человеческого тела (клетки) без прямого контроля со стороны медицинских работников, а только на основе опосредованного управления устройством или заранее установленной программы.

1. Модель понятийно-категориального аппарата

В целях совершенствования юридической техники и правотворческой практики рекомендуется использовать современный юридический инструментарий, в частности, правовой краудсорсинг. Большинство проектов нормативных правовых актов содержат перечень терминов, используемых в конкретном документе; при этом дефиниции нередко дублируются, противоречат друг другу и общей логике. Представляется полезным в рамках каждой законотворческой или нормотворческой инициативы формировать перечень дефиниций и публиковать его в едином открытом документе, обновляемом на регулярной основе.

В целях подготовки проекта Тезауруса по тематике медицинской наноробототехники (далее – Тезаурус) предлагаются следующие организационно-правовые меры:

- определить субъектов (далее – оператор Тезауруса), которые направляют термины для публикации (далее – проект) и порядок регистрации личного кабинета оператора Тезауруса, включающий ссылку на проект и его статус: принято/отклонено/в обработке;
- определить орган или структуру, которая занимается рассмотрением проектов, обобщением и публикацией терминов (далее – администратор Тезауруса);
- закрепить полномочия администратора Тезауруса в профильном нормативном правовом акте, содержащем правила о регулировании общественных отношений в сфере медицинской наноробототехники;
- в случае если администратором Тезауруса будет назначена организация, не относящаяся к органам государственной власти, назначить курирующее ведомство или должностное лицо;
- подготовить требования к проектам, вносимым в Тезаурус: название и реквизиты нормативного правового акта, перечень терминов с определениями;
- сформировать тематический рубрикатор разделов и подразделов Тезауруса;
- закрепить форматы поисковой выдачи терминов: в алфавитном порядке (по каждому документу) согласно тематике разделов и подразделов;
- указать порядок внесения изменений в опубликованные термины Тезауруса;

- рассмотреть вопрос о возможности рекомендовать или обязать субъектов право- и нормотворчества в области медицинской наноробототехники приводить терминологию разрабатываемых документов в соответствие с Тезаурусом;

- рекомендуется формировать Тезаурус с применением инструментария Legal Design.

В целях унификации понятийного аппарата предлагается проанализировать признаки медицинского наноробота и его место среди дефиниций данной категории и сформулировать предложения по внесению в Тезаурус базовых понятий медицинского наноробототехнического права: биомедицинский робот, наноробототехническая система, медицинская наноробототехническая система (медицинский наноробот).

Биомедицинский робот:

- микро-, макро- или наноразмерное устройство;
- владеет функциями движения, перемещения, захвата и манипуляции объектом;
- способен взаимодействовать с пациентом *in vivo* или *ex vivo* в зависимости от модели и назначения;

- пригоден для терапевтических и хирургических манипуляций непосредственно под контролем медицинского персонала либо автономно в соответствии с программой.

Наноробототехническая система (медицинский наноробот):

- величина сравнима с размером молекулы (самые миниатюрные образцы состоят из нескольких десятков атомов);

- способен двигаться, обрабатывать и передавать информацию, исполнять программы;

- реализован на базе механического устройства либо живого организма;

- включает подгруппы нанороботов и наноманипуляторов (нанороботы: молекулярные устройства, нанодвигатели и ДНК-нанороботы; наноманипуляторы, оснащенные соответственно различными технологиями, например, оптическими, акустическими, магнитными пинцетами либо атомной или электронной микроскопией);

- состоит из нескольких модулей: технологических, механических, на основе живого организма, программных.

Медицинская наноробототехническая система (медицинский наноробот):

- относится к наноробототехническим системам, включающим группы нанороботов и наноманипуляторов;

- движется, перемещается, осуществляет манипуляции в кровеносной системе человека, биожидкостях, внутри тканей и органов;

- автономность функции строго ограничена программой;

- взаимодействует с объектами в масштабе молекулы, иона, способен осуществлять манипуляции, имитировать биосигналы, доставлять лекарства конкретным клеткам, исходя из их функционального или органического состояния, осуществлять хирургические задачи, диагностику, детоксикацию;

- обеспечивает свою деятельность посредством энергии глюкозы в крови, света, тепла;

- методологически относится к группе микроустройств и может включать технологические, механические, программные модули, а также основанные на живых организмах.

Таким образом, в Тезаурус предлагается внести следующие термины:

- биомедицинский робот – это устройство, способное выполнять терапевтические, хирургические, диагностические или вспомогательные медицинские задачи как автономно, так и в качестве робота-помощника;
- наноробототехническая система – это наноразмерное устройство, включающее технологические, механические, программные модули и/или модули на основе живых организмов, и осуществляющее манипуляции в масштабе молекулы;
- медицинская наноробототехническая система (медицинский наноробот) – это наноразмерное устройство, функционирующее в условиях *in vivo* в достаточной степени автономно, способное получать энергию от среды (глюкоза в крови, свет, тепло, ультразвук) и осуществляющее функции движения, обработки и передачи информации, исполнения программ с целью проведения медицинских исследований или лечебных процедур, в том числе изучения биологических образцов в наномасштабах, зондирования небольших молекул (включая белки), прохождение через биожидкости для точечной хирургии.

В условиях технологического развития актуальным является дальнейшее исследование вопроса о роли и месте медицинского наноробота в ряду робототехнических устройств. С одной стороны, макророботы, как наиболее массовая технология, образуют нормативную основу, частично применимую к нанороботам; с другой – условия коммуникации с человеком в формате *ex vivo* у таких систем отличаются от устройств, функционирующих *in vivo*. Микророботы с регуляторной и методологической точки зрения схожи с нанороботами, но фактически имеют иной диапазон применения.

В условиях синергетического развития биомедицинских технологий и смежных инноваций предлагается дополнить концепт робоправа и робоэтики концептами наноробоправа и наноробоэтики, с тем чтобы сформулировать ценностное содержание медицинского наноробототехнического права и объединить ученых вокруг общей идеи.

2. Риски и безопасность

Учитывая масштабы и скорость технологического развития, представляется значимым обозначить общие подходы к классификации рисков в исследуемой сфере:

- коммуникативно-этические риски (вопросы коммуникации робота и человека в условиях *in vivo*, а также взаимодействия пациента и медицинских работников);
- риски в области информационной и технологической безопасности (связанные с несанкционированным доступом к программному обеспечению или иным способом воздействующие на процесс функционирования устройства);
- коммуникативно-методологические риски неправового характера (измерение и толкование результатов в сравнении с консервативными методами, а также степень влияния разработчиков устройства и программного обеспечения, технической поддержки);
- правовые риски (проблемы правового статуса медицинских устройств, вопросы разграничения ответственности за неблагоприятные последствия).

К важнейшим характеристикам безопасности медицинского наноробота можно отнести биосовместимость и специфическую автономность. Биосовместимость означает не только безопасность для человека, но и для самого робота, по крайней

мере, до момента выполнения медицинской процедуры. Автономность устройства отличается от общепринятого понимания данного качества робототехники. Медицинский наноробот должен быть способен обеспечить собственную энергетическую автономность, возможность проходить через различные среды и барьеры в организме, а также избегать иммунной провокации. При этом устройство полностью подчиняется медику, чтобы оставаться безопасным для пациента.

В контексте приоритета жизни и здоровья человека актуальным является вопрос об организационно-правовом контроле за возможной репликацией³³ наноробототехнических систем, находящихся внутри организма пациента.

3. Совершенствование законодательства

В части подходов к методологии разработки мер правового регулирования общественных отношений в сфере медицинской наноробототехники предполагается несколько принципов:

- концептуальный и опережающий характер правотворческой деятельности;
- учет трендов цифровизации правотворчества и нормотворчества при разработке подходов (Пашенцев и др., 2019);
- теоретико-правовое обоснование проектов нормативных актов;
- подготовка прогнозных моделей и правовой мониторинг на каждом этапе подготовки и реализации правовых норм;
- применение современных юридических технологий в право- и нормотворчестве (правовой эксперимент, юридическое прогнозирование, регуляторные песочницы, правовой краудсорсинг) (Залоило, Пашенцев, 2020);
- межотраслевой и междисциплинарный характер общественных отношений, связанных с применением медицинских нанороботов, позволяет предположить, что методология правотворческой деятельности в данной сфере потребует применения надотраслевых инструментов.

Предполагается, что при разработке правовых норм полезно выработать систему закрепления норм в российском законодательстве в соответствии с иерархией нормативных правовых актов:

- в федеральном законодательстве сформулировать базовые принципы регулирования (понятийный аппарат, классификацию устройств, меры безопасности, разграничение полномочий государственных органов);
- в законодательстве субъектов отразить нормы, призванные обеспечить интеграцию с локальной правовой практикой и с учетом местных особенностей, в том числе религиозных, национальных, этических;
- в подзаконных актах федеральных и региональных ведомств формулировать вариативные характеристики (например, критерии выдачи лицензии на осуществление определенных видов деятельности, связанных с применением медицинских нанороботов);
- сформировать профессиональные и этические стандарты (в сотрудничестве с профессиональными сообществами и институтами гражданского общества);

³³ Репликация (в вирусологии) – это процесс самовоспроизведения нуклеиновых кислот, генов, хромосом.

– в контексте регулирования наноробототехники и особенно ее медицинского применения рекомендуется сформировать словарь технологических терминов, закрепив его в ведомственном нормативном акте.

В сфере прикладных результатов исследования предлагается ряд правовых новаций и методологических рекомендаций. В частности, рекомендуется внести изменения в ст. 34 п. 3 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а именно дополнить перечень видов высокотехнологичной медицинской помощи формулировкой «включая медицинские наноробототехнические системы» после слов «роботизированной техники». Рассмотренные в научной работе ст. 2 Порядка организации оказания высокотехнологичной медицинской помощи с применением единой государственной информационной системы в сфере здравоохранения, утвержденного приказом Министерства здравоохранения РФ от 2 октября 2019 г. № 824н «Об утверждении порядка оказания высокотехнологичной медицинской помощи с применением единой государственной информационной системы здравоохранения», а также ст. 3 Положения об организации оказания специализированной, в том числе высокотехнологичной, медицинской помощи, утвержденного приказом Министерства здравоохранения РФ от 2 декабря 2014 г. № 796н «Об утверждении положения об организации оказания специализированной, в том числе высокотехнологичной, медицинской помощи», содержат идентичные нормы, полностью повторяющие текст вышеуказанного закона. По этой причине предлагается также внести в данные акты дополнения о наноробототехнических системах.

В целях совершенствования подзаконных актов предлагается дополнить приложение № 1, а именно Номенклатурную классификацию медицинских изделий по видам, утвержденную приказом Министерства здравоохранения РФ от 6 июня 2012 г. № 4н «Об утверждении номенклатурной классификации медицинских изделий», пунктом 6.1 «Медицинские наноробототехнические системы». Рассмотренное выше понятие наноробототехнических систем (вне контекста медицинского применения) может стать частью понятийно-категориального аппарата и номенклатурных перечней, касающихся нанотехнологий.

Предполагается, что дальнейшие меры по подготовке прикладных механизмов правового регулирования включают разработку стандартов оказания высокотехнологичной медицинской помощи в виде применения наноробототехнических систем. Рекомендуется сформулировать данные правила на основе системы стандартов, принятых в других областях медицины и зафиксированных в форме приказов Министерства здравоохранения³⁴.

Обязательство использовать биосовместимые материалы для изготовления медицинских нанороботов и ограничение репликации устройств предлагается закрепить на уровне норм федерального закона.

Сфера наноробототехники относится к новейшему, шестому технологическому укладу, меняющему рельеф правовой реальности. Вопросы коммуникации наноробота и человека в формате *in vivo* становятся принципиально новой областью общественных отношений, которые формируют запрос на нормативы нового типа.

³⁴ См., например: Приказ Минздрава России № 1468н от 24.12.2012. (2013, 10 июня). *Российская газета, спецвыпуск*, 123/1.

Этические правила и стандарты профессиональной деятельности выходят на первый план, не уступая в значимости гражданско-правовым и уголовно-правовым аспектам. В правовой доктрине под воздействием масштабной технологической модернизации происходит трансформация базовых концептов. Междисциплинарная методология необратимо меняет классический академический инструментарий ученого-исследователя. Образовательный процесс в юриспруденции раскрывает перспективы развития в условиях необходимости подготовки юристов, способных к правовой практике в сфере инновационной биомедицины.

Список литературы

- Асеева, И. А. (2017). Аксиологические приоритеты VI технологического уклада. *Эпистемология и философия науки*, 51(1), 124–137. EDN: <https://elibrary.ru/yqyrun>. DOI: <https://doi.org/10.5840/eps201751114>
- Бачило, И. Л. (2017). *Понятийный аппарат в информационном праве: сборник научных работ* (с. 12–28). Москва: Канон-Плюс.
- Бачило, И. Л. (2015). *Понятийный аппарат информационного права: сборник научных работ* (с. 8–17). Москва: Канон-Плюс.
- Бегишев, И. Р., Хисамова, З. И. (2018). Криминологические риски применения искусственного интеллекта. *Всероссийский криминологический журнал*, 12(6), 767–775. EDN: <https://elibrary.ru/yystvz>. DOI: [https://doi.org/10.17150/2500-4255.2018.12\(6\).767-775](https://doi.org/10.17150/2500-4255.2018.12(6).767-775)
- Бегишев, И. Р. (2021). Проект федерального закона «Об обороте роботов, их составных частей (модулей)». *Актуальные проблемы экономики и права*, 15(2), 379–391. EDN: <https://elibrary.ru/nxzfpk>. DOI: <https://doi.org/10.21202/1993-047X.15.2021.2.379-391>
- Гуляева, П. С. (2022). Квазиправосубъектность искусственного интеллекта: теоретико-правовые аспекты. *Вестник Московского государственного педагогического университета. Серия: Юридические науки*, 2(46), 58–69. EDN: <https://elibrary.ru/qbdkre>. DOI: <https://doi.org/10.25688/2076-9113.2022.46.2.06>
- Жолобова, Ю. В., Счастливецова, Е. А. (2020). НБИКС-технологии и проблема антропологической эволюции. *Вестник Вятского государственного университета*, 3(137), 7–19.
- Залоило, М. В., Пашенцев, Д. А. (ред.). (2020). *Современные юридические технологии в правотворчестве: научно-практическое пособие*. Москва: ИЗиСП: Норма: ИНФРА-М. <https://elibrary.ru/vtejsu>
- Кибальник, А. Г., Волосюк, П. В. (2018). Искусственный интеллект: вопросы уголовно-правовой доктрины, ожидающие ответов. *Юридическая наука и практика: Вестник Нижегородской академии МВД России*, 4(44), 173–178. EDN: <https://elibrary.ru/yszmpj>. DOI: <https://doi.org/10.24411/2078-5356-2018-10428>
- Малько, А. В. (2019). Проект концепции российской правовой политики в сфере искусственного интеллекта как доктринальный документ. *Балтийский гуманитарный журнал*, 8(29), 348–352. EDN: <https://elibrary.ru/sjqbob>. DOI: <https://doi.org/10.26140/bgз3-2019-0804-0081>
- Морхат, П. М. (2018a). *Правосубъектность юнитов искусственного интеллекта. Гражданско-правовое исследование: монография*. Москва: ЮНИТИ-ДАНА.
- Морхат, П. М. (2018b). Юнит искусственного интеллекта как электронное лицо. *Вестник Московского государственного областного университета. Серия: Юриспруденция*, 2, 61–73. <https://doi.org/10.18384/2310-6794-2018-2-61-73>
- Незнамов, А. В., Наумов, В. Б. (2017). Вопросы развития законодательства о робототехнике в России и в мире. *Юридические исследования*, 8, 14–25. EDN: <https://elibrary.ru/zcssfv>. DOI: <https://doi.org/10.25136/2409-7136.2017.8.23292>
- Пашенцев, Д. А. (2019). Лексико-семантические особенности языка правотворчества в условиях цифровизации. В сб. Д. А. Пашенцев, М. В. Залоило (ред.). *Язык правотворчества в условиях цифровизации общественных отношений: сборник научных трудов* (с. 143–148). Москва: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М.
- Пашенцев, Д. А., Залоило, М. В., Дорская, А. А. (2021). *Смена технологических укладов и правовое развитие России*. Москва: ИЗиСП: Норма: ИНФРА-М.
- Пашенцев, Д. А., Залоило, М. В., Иванюк, О. А., Головина, А. А. (2019). *Цифровизация правотворчества: поиск новых решений: монография*. Москва: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2019. <https://elibrary.ru/qrnijy>

- Понкин, И. В., Редькина, А. И. (2019). Цифровая формализация права. *International Journal of Open Information Technologies*, 7(1), 39–48.
- Понкин, И. В., Редькина, А. И. (2018). Искусственный интеллект с точки зрения права. *Вестник Российского университета дружбы народов. Серия: Юридические науки*, 22(1), 91–109. EDN: <https://elibrary.ru/yvxxkva>. DOI: <https://doi.org/10.22363/2313-2337-2018-22-1-91-109>
- Хабриева, Т. Я., Черногор, Н. Н. (2020). *Будущее права. Наследие академика В. С. Степина и юридическая наука*. Москва: Российская академия наук; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; ИНФРА-М. <https://doi.org/10.12737/1112960>
- Asimov, I. (1942). Runaround. In *Astounding Science Fiction*. New York.
- Aramesh, M., Forró, C., Dorwling-Carter, L., Luchtefeld, I., Schlotter, T., Ihle, S. J., Shorubalko, I., Hosseini, V., Momotenko, D., Zambelli, T., Klotzsch, E., & Vörös, J. (2019). Localized detection of ions and biomolecules with a force-controlled scanning nanopore microscope. *Nature nanotechnology*, 14(8), 791–798. <https://doi.org/10.1038/s41565-019-0493-z>
- Astromskis, P. (2018). In Critique of RoboLaw: The Model of SmartLaw. In V. Müller (Ed.). *Philosophy and Theory of Artificial Intelligence 2017. PT-AI 2017. Series Studies in Applied Philosophy, Epistemology and Rational Ethics*, 44. Springer, Cham.
- Bartkowski, P., Gawinski, F., & Pawliszak, L. (2022). E-Morph as a New Adaptive Actuator for Soft Robotics. *IEEE Robotics and Automation Letter*, 7(4), 8831–8836. <https://doi.org/10.1109/LRA.2022.3189169>
- Chen, S., Wang, Y., Nie, T., Bao, C., Wang, C., Xu, T., Lin, Q., Qu, D. H., Gong, X., Yang, Y., Zhu, L., & Tian, H. (2018). An Artificial Molecular Shuttle Operates in Lipid Bilayers for Ion Transport. *Journal of the American Chemical Society*, 140(51), 17992–17998. <https://doi.org/10.1021/jacs.8b09580>
- Deng, X. et al. (2023). Magnetic Micro/nanorobots for biological detection and targeted delivery. *Biosensors and Bioelectronics*, 222, 114960. <https://doi.org/10.1016/j.bios.2022.114960>
- Diller, E., & Sitti, M. (2013). Micro-Scale Mobile Robotics. *Foundations and Trends® in Robotics*, 2(3), 143–259. <http://dx.doi.org/10.1561/23000000023>
- Erbas-Cakmak, S., Leigh, D. A., McTernan, C. T., & Nussbaumer, A. L. (2015). Artificial Molecular Machines. *Chemical Reviews*, 115(18), 10081–10206. <https://doi.org/10.1021/acs.chemrev.5b00146>
- Fortunato, Gabriele Maria, Batoni, Elisa, Bonatti, Amedeo Franco, Giovanni, Vozzi, & Carmelo, De Maria. (2022). Surface reconstruction and tissue recognition for robotic-based in situ bioprinting. *Bioprinting*, 26, e00195. <https://doi.org/10.1016/j.bprint.2022.e00195>
- Frana, P. L., & Klein, M. J. (2021). *Encyclopedia of Artificial Intelligence: The Past, Present, and Future of AI*. Santa-Barbara, California. ABC-Clio.
- Fukuda, Toshio, Nakajima, Masahiro, & Kojima, Masaru. (2010). Micro-Nano Robotics and Automation System. *IFAC Proceedings Volumes*, 43(8), 20–25. <https://doi.org/10.3182/20100712-3-FR-2020.00005>
- Gardini, L., Heissler, S. M., Arbore, C., Yang, Y., Sellers, J. R., Pavone, F. S., & Capitanio, M. (2018). Dissecting myosin-5B mechanosensitivity and calcium regulation at the single molecule level. *Nature communications*, 9(1), 2844. <https://doi.org/10.1038/s41467-018-05251-z>
- Gellers, Joshua C. (2021). *Rights for Robots Artificial Intelligence, Animal and Environmental Law*. NY: Routledge.
- Guillaume-Gentil, O., Potthoff, E., Ossola, D., Franz, C. M., Zambelli, T., & Vorholt, J. A. (2014). Force-controlled manipulation of single cells: from AFM to FluidFM. *Trends in biotechnology*, 32(7), 381–388. <https://doi.org/10.1016/j.tibtech.2014.04.008>
- Guix, M., Mayorga-Martinez, C. C., & Merkoçi, A. (2014). Nano/micromotors in (bio)chemical science applications. *Chemical reviews*, 114(12), 6285–6322. <https://doi.org/10.1021/cr400273r>
- Jamali, Hamid R., Azadi-Ahmadabadi, Ghasem, & Asadi, Saeid. (2018). Interdisciplinary relations of converging technologies: Nano-Bio-Info-Cogno (NBIC). *Scientometrics*, 116(11), 1055–1073.
- Ji, Y., Lin, X., Wu, Z., Wu, Y., Gao, W., & He, Q. (2019). Macroscale Chemotaxis from a Swarm of Bacteria-Mimicking Nanoswimmers. *Angewandte Chemie International edition*, 58(35), 12200–12205. <https://doi.org/10.1002/anie.201907733>
- Jingui, Qian, Jifeng, Ren, Yi, Liu, Raymond, H. W. Lam, & Joshua E.-Y., Lee. (2020). Reusable acoustic tweezers enable 2D patterning of microparticles in microchamber on a disposable silicon chip superstrate. *IEEE SENSORS* (pp. 1–4). <https://doi.org/10.1109/sensors47125.2020.9278717>
- Katsunori, K. (2012). Nanotechnology and Medical Robotics; Legal and Ethical Responsibility. *Waseda Bulletin of Comparative Law*, 30, 1–6.
- Khisamova, Z. I., & Begishev, I. R. (2019). On Methods to Legal Regulation of Artificial Intelligence in the World. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 515–520. EDN: <https://elibrary.ru/pqjfk0>. DOI: <https://doi.org/10.35940/ijitee.A9220.119119>
- Kuijpers, Louis, van Laar, Theo, Janissen, Richard, & Dekker, Nynke H. (2022). Characterizing single-molecule

- dynamics of viral RNA-dependent RNA polymerases with multiplexed magnetic tweezers. *STAR Protocols*, 3(3), 101606, 1–19. <https://doi.org/10.1016/j.xpro.2022.101606>
- Li, J., Esteban-Fernández de Ávila, B., Gao, W., Zhang, L., & Wang, J. (2017). Micro/Nanorobots for Biomedicine: Delivery, Surgery, Sensing, and Detoxification. *Science Robotics*, 2(4), eaam6431. <https://doi.org/10.1126/scirobotics.aam6431>
- Li, M., Xi, N., Wang, Y. et al. (2019). Advances in atomic force microscopy for single-cell analysis. *Nano Research*, 12, 703–718. <https://doi.org/10.1007/s12274-018-2260-0>
- Li, M., Xi, N., Wang, Y., & Liu, L. (2021). Progress in Nanorobotics for Advancing Biomedicine. *IEEE transactions on bio-medical engineering*, 68(1), 130–147. <https://doi.org/10.1109/TBME.2020.2990380>
- Li, T., Mao, C., Shen, J., & Zhou, M. (2022). Three laws of design for biomedical micro/nanorobots. *Nano Today*, 45, 101560. <https://doi.org/10.1016/j.nantod.2022.101560>
- Li, X., Liu, C., Chen, S., Wang, Y., Cheng, S. H., & Sun, D. (2017). In Vivo Manipulation of Single Biological Cells With an Optical Tweezers-Based Manipulator and a Disturbance Compensation Controller, *IEEE Transactions on Robotics*, 33(5), 1200–1212. <https://doi.org/10.1109/TRO.2017.2718554>
- Marks, J. L. A., & Cyr, S. K. (2018). Government Regulation of Nanorobots in Medicine: How the FDA and PTO Handle These New Technologies. *The Journal of Robotics, Artificial Intelligence & Law*, 1(4), 217–230
- Min, Sun, Weisi, Lia, Cheng, Zhang, Shuangxi, Lia, Fayong, Zhou, Yuntao, Zhu, & Xiaoyang, Zhou. (2022). Da Vinci Xi™ robot-assisted liver resection. *Intelligent Surgery*, 1, 16–20. <https://doi.org/10.1016/j.isurg.2021.10.001>
- Mulgan, T. (2019). Corporate Agency and Possible Futures. *Journal of Business Ethics*, 154(4), 901–916. <https://doi.org/10.1007/s10551-018-3887-1>
- Muscariello, L., Rosso, F., Marino, G., Giordano, A., Barbarisi, M., Cafiero, G., & Barbarisi, A. (2005). A critical overview of ESEM applications in the biological field. *Journal of cellular physiology*, 205(3), 328–334. <https://doi.org/10.1002/jcp.20444>
- Naidoo, S. (2021). *Biocompatibility Testing of Medical Devices*. Burlington: Arcler Press.
- Nambu, T. (2016). Legal regulations and public policies for next-generation robots in Japan. *AI & SOCIETY*, 31, 483–500. <https://doi.org/10.1007/s00146-015-0628-1>
- Neuman, Keir C., Nagy, Attila. (2008). Single-molecule force spectroscopy: optical tweezers, magnetic tweezers and atomic force microscopy. *Nature Methods*, 5(6), 491–506.
- Norasi, Hamid, Tetteh, Emmanuel, Law, Katherine E., Sid, Ponnal, Hallbeck, Susan, & Tollefson, Matthew. (2022). Intraoperative workload during robotic radical prostatectomy: Comparison between multi-port da Vinci Xi and single port da Vinci SP robots. *Applied Ergonomics*, 104, 103826. <https://doi.org/10.1016/j.apergo.2022.103826>
- Palmerini, E., Bertolini, A., Battaglia, F., Koops, B.-J., Carnevale, A., & Salvini, P. (2016). RoboLaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*, 86, 78–85. <https://doi.org/10.1016/j.robot.2016.08.026>
- Qi, Hu, Teng, Ma, Qi, Zhang, Jimin, Wang, Ye, Yang, Feiyan, Cai, & Hairong, Zheng. (2021). 3-D Acoustic Tweezers Using a 2-D Matrix Array With Time-Multiplexed Traps. *IEEE Transactions on ultrasonics, ferroelectrics, and frequency control*, 68(12), 3646–3653. <https://doi.org/10.1109/TUFFC.2021.3098191>
- Rong, Liu, Guo-Dong, Zhao, Wen-Bo, Zou, Xiu-Ping, Zhang, Shuai, Xu, Yang, Wang, Yan-Zhe, Liu, Yuan-Xing, Gao, Zhi-Peng, & Zhoua, Yu-Yao Song. (2022). Single-port robot-assisted hepatic left lateral sectionectomy using the da Vinci SP® system: A case report. *Intelligent Surgery*, 2, 6–9. <https://doi.org/10.1016/j.isurg.2022.02.002>
- Rothemund, P. W. (2006). Folding DNA to create nanoscale shapes and patterns. *Nature*, 440(7082), 297–302. <https://doi.org/10.1038/nature04586>
- Shi, C., Luu, D. K., Yang, Q., Liu, J., Chen, J., Ru, C., Xie, S., Luo, J., Ge, J., & Sun, Y. (2016). Recent advances in nanorobotic manipulation inside scanning electron microscopes. *Microsystems & nanoengineering*, 2, 16024. <https://doi.org/10.1038/micronano.2016.24>
- Suulker, C., Skach, S., & Althoefer, K. (2022). Soft Robotic Fabric Actuator With Elastic Bands for High Force and Bending Performance in Hand Exoskeletons. *IEEE Robotics and Automation Letter*, 7(4), 10621–10627. <https://doi.org/10.1109/LRA.2022.3194883>
- Sweeney, Aldrin. (2020). Incorporating NBIC social/ethical issues into STEM teacher education programmes. *Canada-Caribbean Institute Journal*, 1(1): Proceedings of the Canada-Caribbean Research Symposium. Canada-Caribbean Institute. Brock University Open Journal System. 2020. <https://journals.library.brocku.ca/index.php/cancarib/article/view/2369#>
- Taherkhani, S., Mohammadi, M., Daoud, J., Martel, S., & Tabrizian, M. (2014). Covalent binding of nanoliposomes to the surface of magnetotactic bacteria for the synthesis of self-propelled therapeutic agents. *ACS Nano*, 8(5), 5049–5060. <https://doi.org/10.1021/nn5011304>

- Vale, Daniel, El-Sharif, Ali, & Muhammed, Ali. (2022). Explainable artificial intelligence (XAI) post-hoc explainability methods: risks and limitations in non-discrimination law. *AI and Ethics*, 2, 815–826. <https://doi.org/10.1007/s43681-022-00142-y>
- Villa, K., & Pumera, M. (2019). Fuel-free light-driven micro/nanomachines: artificial active matter mimicking nature. *Chemical Society Reviews*, 48(19), 4966–4978. <https://doi.org/10.1039/C9CS00090A>
- Wan, M., Liu, Z., Li, T., Chen, H., Wang, Q., Chen, T., Tao, Y., & Mao, C. (2021). Zwitterion-Based Hydrogen Sulfide Nanomotors Induce Multiple Acidosis in Tumor Cells by Destroying Tumor Metabolic Symbiosis. *Angewandte Chemie International Edition*, 60(29), 16139–16148. <https://doi.org/10.1002/anie.202104304>
- Wang, H., & Pumera, M. (2015). Fabrication of Micro/Nanoscale Motors. *Chemical Reviews*, 115(16), 8704–8735. <https://doi.org/10.1021/acs.chemrev.5b00047>
- Wang, Joseph, & Wei, Gao. (2012). Nano/Microscale Motors: Biomedical Opportunities and Challenges. *ACS Nano*, 6(7), 5745–5751.
- Wang, Qing, Shuhan, Chen, Jia, Zhou, & Antoine, Riaud. (2022). *Laser-guided acoustic tweezers*. National Natural Science Foundation of China, State Key Lab of ASIC and System, Fudan University (pp. 1–18). <https://arxiv.org/abs/2203.14497>
- Wenyan, Qiao, Linglin, Zhou, Zhihao, Zhao, Di, Liua, Shaoxin, Lia, Jie, Ana, Xinyuan, Lia, Yikui, Gao, Peiyuan, Yang, Jiaqi Liu, Zhong, Lin, Wang, & Jie, Wang. (2022). A self-powered vector motion sensor for smart robotics and personalized medical rehabilitation. *Nano Energy*, 104, 1–10. <https://doi.org/10.1016/j.nanoen.2022.107936>
- Xu, X., Saw, P. E., Tao, W., Li, Y., Ji, X., Bhasin, S., Liu, Y., Ayyash, D., Rasmussen, J., Huo, M., Shi, J., & Farokhzad, O. C. (2017). ROS-Responsive Polyprodrug Nanoparticles for Triggered Drug Delivery and Effective Cancer Therapy. *Advanced materials (Deerfield Beach, Fla.)*, 29(33), <https://doi.org/10.1002/adma.201700141>
- Xue, S. (2022). The Application of Virtual Metacognitive Network Model in Preschool Guiding Art Network Teaching, *6th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 672–675). <https://doi.org/10.1109/ICICCS53718.2022.9788219>
- You, M., Chen, C., Xu, L., Mou, F., & Guan, J. (2018). Intelligent Micro/nanomotors with Taxis. *Accounts of Chemical Research*, 51(12), 3006–3014. <https://doi.org/10.1021/acs.accounts.8b00291>
- Yuan, K., Aftoni, A., & Çobanoğlu, Ö. (2020). The Effect of Problem-Based Learning Model and Blended Learning Model to Metacognitive Awareness as a Reflection Towards a New Normal Era. *Jurnal Pendidikan Teknologi dan Kejuruan*, 26(2), 183–188. <https://doi.org/10.21831/jptk.v26i2.32783>

Сведения об авторе



Гуляева Полина Сергеевна – аспирант, Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации

Адрес: 117218, Российская Федерация, г. Москва, ул. Б. Черемушкинская, 34

E-mail: polina-gulyaeva2016@bk.ru

ORCID ID: <https://orcid.org/0000-0002-4108-6379>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/HKV-7341-2023>

Google Scholar ID: <https://scholar.google.com/citations?hl=en&user=gPHDfmAAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1002457

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 8 сентября 2022 г.

Дата одобрения после рецензирования – 17 января 2023 г.

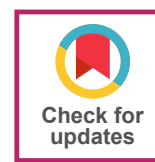
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.4>



Medical Nanorobots in the Focus of Law

Polina S. Gulyaeva 

Institute of Legislation and Comparative Law under the Government of the Russian Federation
Moscow, Russian Federation

Keywords

Digital technologies,
ethics,
healthcare,
in vivo,
Isaac Azimov,
law,
medical robot,
medicine,
nanorobot,
regulation,
robotics

Abstract

Objective: to form doctrinal bases and mechanics of legal regulation of using medical nanorobots; to conceptualize the idea of nanorobotics law within the frameworks of its basic definitions, safety norms, risks, typology of devices, and legal parameters of technological terminology.

Methods: the cognition tools are represented in the form of integration between general scientific and modern special legal methods (including the methods of comparative legal studies, legal modeling and juridical forecasting, NBICS-convergence), which, taken as a whole, allow distinguishing in the study object not only juridical proper, but also anthropological, biomedical, informational, and mechanistic research projections.

Results: the author's definition of the medical nanorobot concept was formulated; the legal content and quasi-legal aspects of the definition that are important for the theoretical and applied development of terminology were investigated; the signs of related concepts (biomedical robot, nanorobotic system, medical nanorobotic system) were identified and logical connections between them were established; the classification of the main types of risks associated with the practical use of medical nanorobots was carried out; the list of theoretical and legal contradictions that are potentially capable of negatively affecting the future development of regulatory practice was revealed; the Russian and foreign experience of legal regulation and doctrinal understanding of the problems of medical nanorobotics (by the examples of the USA, Japan, Europe, China) was considered.

Scientific novelty: under the lack of interdisciplinary research, an attempt was made to comprehensively consider the concept of a medical nanorobot in a technological, legal and communicative way ("human robot" on a nanoscale) based on the advanced scientific research that defines the foundations of the future nanorobotic law. It is recommended to supplement the synergetic development of biomedical and related technologies, reflected in the models of robot law and robot ethics, with relatively independent concepts of nanorobot law and nanorobot ethics.

© Gulyaeva P. S., 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: based on the analysis of the legal regulation system in force in Russia and abroad, mechanisms for improving domestic legislation were identified, including taking into account the achievements of juridical crowdsourcing. Within the framework of socio-humanitarian issues, a contribution to the development of legal, sociological, and psychological science is formed. A scientific and methodological basis was prepared for further legal research and law-making activities in the field of medical nanorobotics.

For citation

Gulyaeva, P. S. (2023). Medical nanorobots in the focus of law. *Journal of Digital Technologies and Law*, 1(1), 89–122. <https://doi.org/10.21202/jdtl.2023.4>

References

- Aramesh, M., Forró, C., Dorwling-Carter, L., Lüchtfeld, I., Schlotter, T., Ihle, S. J., Shorubalko, I., Hosseini, V., Momotenko, D., Zambelli, T., Klotzsch, E., & Vörös, J. (2019). Localized detection of ions and biomolecules with a force-controlled scanning nanopore microscope. *Nature nanotechnology*, 14(8), 791–798. <https://doi.org/10.1038/s41565-019-0493-z>
- Aseeva, I. A. (2017). Axiological priorities of the VI technological mode *Epistemology & Philosophy of Science*, 51(1), 124–137. (In Russ.). <https://doi.org/10.5840/eps201751114>
- Asimov, I. (1942). Runaround. In *Astounding Science Fiction*. New York.
- Astromskis, P. (2018). In Critique of RoboLaw: The Model of SmartLaw. In V. Müller (Ed.). *Philosophy and Theory of Artificial Intelligence 2017. PT-AI 2017. Series Studies in Applied Philosophy, Epistemology and Rational Ethics*, 44. Springer, Cham.
- Bachilo, I. L. (2015). *Conceptual framework of informational law*: collection of research works (pp. 8–17). Moscow: Kanon-Plyus. (In Russ.).
- Bachilo, I. L. (2017). *Conceptual framework of informational law*: collection of research works (pp. 12–28). Moscow: Kanon-Plyus. (In Russ.).
- Bartkowski, P., Gawinski, F., & Pawliszak, L. (2022). E-Morph as a New Adaptive Actuator for Soft Robotics. *IEEE Robotics and Automation Letter*, 7(4), 8831–8836. <https://doi.org/10.1109/LRA.2022.3189169>
- Begishev, I. R. (2021). Draft of a Federal Law “On circulation of robots and their components (modules)”. *Actual Problems of Economics and Law*, 15(2), 379–391. (In Russ.). <https://doi.org/10.21202/1993-047X.15.2021.2.379-391>
- Begishev, I. R., Khisamova, Z. I. (2018). Criminological Risks of Using Artificial Intelligence. *Vserossiiskii kriminologicheskii zhurnal = 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)
- Chen, S., Wang, Y., Nie, T., Bao, C., Wang, C., Xu, T., Lin, Q., Qu, D. H., Gong, X., Yang, Y., Zhu, L., & Tian, H. (2018). An Artificial Molecular Shuttle Operates in Lipid Bilayers for Ion Transport. *Journal of the American Chemical Society*, 140(51), 17992–17998. <https://doi.org/10.1021/jacs.8b09580>
- Deng, X. et al. (2023). Magnetic Micro/nanorobots for biological detection and targeted delivery. *Biosensors and Bioelectronics*, 222, 114960. <https://doi.org/10.1016/j.bios.2022.114960>
- Diller, E., & Sitti, M. (2013). Micro-Scale Mobile Robotics. *Foundations and Trends® in Robotics*, 2(3), 143–259. <http://dx.doi.org/10.1561/23000000023>
- Erbas-Cakmak, S., Leigh, D. A., McTernan, C. T., & Nussbaumer, A. L. (2015). Artificial Molecular Machines. *Chemical Reviews*, 115(18), 10081–10206. <https://doi.org/10.1021/acs.chemrev.5b00146>
- Fortunato, Gabriele Maria, Batoni, Elisa, Bonatti, Amedeo Franco, Giovanni, Vozzi, & Carmelo, De Maria. (2022). Surface reconstruction and tissue recognition for robotic-based in situ bioprinting. *Bioprinting*, 26, e00195. <https://doi.org/10.1016/j.bprint.2022.e00195>
- Frana, P. L., & Klein, M. J. (2021). *Encyclopedia of Artificial Intelligence: The Past, Present, and Future of AI*. Santa-Barbara, California. ABC-Clio.

- Fukuda, Toshio, Nakajima, Masahiro, & Kojima, Masaru. (2010). Micro-Nano Robotics and Automation System. *IFAC Proceedings Volumes*, 43(8), 20–25. <https://doi.org/10.3182/20100712-3-FR-2020.00005>
- Gardini, L., Heissler, S. M., Arbore, C., Yang, Y., Sellers, J. R., Pavone, F. S., & Capitanio, M. (2018). Dissecting myosin-5B mechanosensitivity and calcium regulation at the single molecule level. *Nature communications*, 9(1), 2844. <https://doi.org/10.1038/s41467-018-05251-z>
- Gellers, Joshua C. (2021). *Rights for Robots Artificial Intelligence, Animal and Environmental Law*. NY: Routledge.
- Guillaume-Gentil, O., Potthoff, E., Ossola, D., Franz, C. M., Zambelli, T., & Vorholt, J. A. (2014). Force-controlled manipulation of single cells: from AFM to FluidFM. *Trends in biotechnology*, 32(7), 381–388. <https://doi.org/10.1016/j.tibtech.2014.04.008>
- Guix, M., Mayorga-Martinez, C. C., & Merkoçi, A. (2014). Nano/micromotors in (bio)chemical science applications. *Chemical reviews*, 114(12), 6285–6322. <https://doi.org/10.1021/cr400273r>
- Gulyaeva, P. S. (2022). Quasi-legal personality of artificial intelligence: theoretical and legal aspects. *Bulletin of the Moscow City Pedagogical University. "Pedagogy and Psychology" Series*, 2(46), 58–69. (In Russ.). <https://doi.org/10.25688/2076-9113.2022.46.2.06>
- Jamali, Hamid R., Azadi-Ahmadabadi, Ghasem, & Asadi, Saeid. (2018). Interdisciplinary relations of converging technologies: Nano-Bio-Info-Cogno (NBIC). *Scientometrics*, 116(11), 1055–1073.
- Ji, Y., Lin, X., Wu, Z., Wu, Y., Gao, W., & He, Q. (2019). Macroscale Chemotaxis from a Swarm of Bacteria-Mimicking Nanoswimmers. *Angewandte Chemie International edition*, 58(35), 12200–12205. <https://doi.org/10.1002/anie.201907733>
- Jingui, Qian, Jifeng, Ren, Yi, Liu, Raymond H. W., Lam, & Joshua E.-Y., Lee. (2020). Reusable acoustic tweezers enable 2D patterning of microparticles in microchamber on a disposable silicon chip superstrate. *IEEE SENSORS* (pp. 1–4). <https://doi.org/10.1109/sensors47125.2020.9278717>
- Katsunori, K. (2012). Nanotechnology and Medical Robotics; Legal and Ethical Responsibility. *Waseda Bulletin of Comparative Law*, 30, 1–6.
- Khabriyeva, T., Chernogor, N. (2020). *The future of law: the legacy of academician V. S. Stepin and legal science*. Moscow: Rossiiskaya akademiya nauk; Institut zakonodatel'stva i sravnitel'nogo pravovedeniya pri Pravitel'stve Rossiiskoi Federatsii; INFRA-M. (In Russ.). <https://doi.org/10.12737/1112960>
- Khisamova, Z. I., & Begishev, I. R. (2019). On Methods to Legal Regulation of Artificial Intelligence in the World. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 515–520. <https://doi.org/10.35940/ijitee.A9220.119119>
- Kibalnik, A. G., Volosyuk, P. V. (2018). Artificial intelligence: doctrinal criminal law questions awaiting answers. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 4(44), 173–178. (In Russ.). <https://doi.org/10.24411/2078-5356-2018-10428>
- Kuijpers, Louis, van Laar, Theo, Janissen, Richard, & Dekker, Nynke H. (2022). Characterizing single-molecule dynamics of viral RNA-dependent RNA polymerases with multiplexed magnetic tweezers. *STAR Protocols*, 3(3), 101606, 1–19. <https://doi.org/10.1016/j.xpro.2022.101606>
- Li, J., Esteban-Fernández de Ávila, B., Gao, W., Zhang, L., & Wang, J. (2017). Micro/Nanorobots for Biomedicine: Delivery, Surgery, Sensing, and Detoxification. *Science Robotics*, 2(4), eaam6431. <https://doi.org/10.1126/scirobotics.aam6431>
- Li, M., Xi, N., Wang, Y. et al. (2019). Advances in atomic force microscopy for single-cell analysis. *Nano Research*, 12, 703–718. <https://doi.org/10.1007/s12274-018-2260-0>
- Li, M., Xi, N., Wang, Y., & Liu, L. (2021). Progress in Nanorobotics for Advancing Biomedicine. *IEEE transactions on bio-medical engineering*, 68(1), 130–147. <https://doi.org/10.1109/TBME.2020.2990380>
- Li, T., Mao, C., Shen, J., & Zhou, M. (2022). Three laws of design for biomedical micro/nanorobots. *Nano Today*, 45, 101560. <https://doi.org/10.1016/j.nantod.2022.101560>
- Li, X., Liu, C., Chen, S., Wang, Y., Cheng, S. H., & Sun, D. (2017). In Vivo Manipulation of Single Biological Cells With an Optical Tweezers-Based Manipulator and a Disturbance Compensation Controller, *IEEE Transactions on Robotics*, 33(5), 1200–1212. <https://doi.org/10.1109/TRO.2017.2718554>
- Malko, A. V. (2019). The draft concept of the Russian legal policy in the field of artificial intelligence as a doctrinal document. *Baltic Humanitarian Journal*, 8(29), 348–352. (In Russ.). <https://doi.org/10.26140/bgz3-2019-0804-0081>
- Marks, J. L. A., & Cyr, S. K. (2018). Government Regulation of Nanorobots in Medicine: How the FDA and PTO Handle These New Technologies. *The Journal of Robotics, Artificial Intelligence & Law*, 1(4), 217–230.
- Min, Sun, Weisi, Lia, Cheng, Zhang, Shuangxi, Lia, Fayong, Zhou, Yuntao, Zhu, & Xiaoyang, Zhou. (2022). Da Vinci Xi™ robot-assisted liver resection. *Intelligent Surgery*, 1, 16–20. <https://doi.org/10.1016/j.isurg.2021.10.001>

- Morkhat, P. M. (2018a). Artificial intelligence unit as electronic personality. *Bulletin MSRU. Series: Jurisprudence*, 2, 61–73. (In Russ.). <https://doi.org/10.18384/2310-6794-2018-2-61-73>
- Morkhat, P. M. (2018b). *Legal personality of a unit of artificial intelligence. Civil-legal research*. Moscow: Yuniti-Dana. (In Russ.).
- Mulgan, T. (2019). Corporate Agency and Possible Futures. *Journal of Business Ethics*, 154(4), 901–916. <https://doi.org/10.1007/s10551-018-3887-1>
- Muscariello, L., Rosso, F., Marino, G., Giordano, A., Barbarisi, M., Cafiero, G., & Barbarisi, A. (2005). A critical overview of ESEM applications in the biological field. *Journal of cellular physiology*, 205(3), 328–334. <https://doi.org/10.1002/jcp.20444>
- Naidoo, S. (2021). *Biocompatibility Testing of Medical Devices*. Burlington: Arcler Press.
- Nambu, T. (2016). Legal regulations and public policies for next-generation robots in Japan. *AI & SOCIETY*, 31, 483–500. <https://doi.org/10.1007/s00146-015-0628-1>
- Neuman, Keir C., Nagy, Attila. (2008). Single-molecule force spectroscopy: optical tweezers, magnetic tweezers and atomic force microscopy. *Nature Methods*, 5(6), 491–506.
- Neznamov, A., Naumov, V. (2017). On the regulation of robotics in Russia and in the world. *Legal Studies*, 8, 14–25. (In Russ.). <https://doi.org/10.25136/2409-7136.2017.8.23292>
- Norasi, Hamid, Tetteh, Emmanuel, Law, Katherine E., Sid, Ponnal, Hallbeck, Susan, & Tollefson, Matthew. (2022). Intraoperative workload during robotic radical prostatectomy: Comparison between multi-port da Vinci Xi and single port da Vinci SP robots. *Applied Ergonomics*, 104, 103826. <https://doi.org/10.1016/j.apergo.2022.103826>
- Palmerini, E., Bertolini, A., Battaglia, F., Koops, B.-J., Carnevale, A., & Salvini, P. (2016). RoboLaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*, 86, 78–85. <https://doi.org/10.1016/j.robot.2016.08.026>
- Pashentsev, D. A. (2019). Lexical and semantic features of the law-making language in the conditions of digitalization. In D. A. Pashentsev, M. V. Zaloilo (Eds.). *Law-making language within the context of digitalization of social relations. Collection of scientific articles* (pp. 143–148). Moscow: The Institute of Legislation and Comparative Law under the Government of the Russian Federation: INFRA-M. (In Russ.).
- Pashentsev, D. A., Zaloilo, M. V., Dorskaya, A. A. (2021). *Changing of Technological Orders and Legal Development of Russia*. Moscow: IZISP: Norma: INFRA-M. (In Russ.).
- Pashentsev, D. A., Zaloilo, M. V., Ivanyuk, O. A., Golovina, A. A. (2019). *The digitalization of law-making: the search for new solutions*. Moscow: Institut zakonodatel'stva i sravnitel'nogo pravovedeniya pri Pravitel'stve Rossiiskoi Federatsii: INFRA-M. (In Russ.).
- Ponkin, I. V., Redkina, A. I. (2018). Artificial Intelligence from the Point of View of Law. *RUDN Journal of Law*, 22(1), 91–109. (In Russ.). <https://doi.org/10.22363/2313-2337-2018-22-1-91-109>
- Ponkin, I., Redkina, A. (2019). Digital formalization of law. *International Journal of Open Information Technologies*, 7(1), 39–48. (In Russ.).
- Qi, Hu, Teng, Ma, Qi, Zhang, Jimin, Wang, Ye, Yang, Feiyan, Cai, & Hairong, Zheng. (2021). 3-D Acoustic Tweezers Using a 2-D Matrix Array With Time-Multiplexed Traps. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, 68(12), 3646–3653. <https://doi.org/10.1109/TUFFC.2021.3098191>
- Qing, Wang, Shuhan, Chen, Jia, Zhou, & Antoine, Riaud. (2022) *Laser-guided acoustic tweezers*. National Natural Science Foundation of China, State Key Lab of ASIC and System, Fudan University (pp. 1–18). <https://arxiv.org/abs/2203.14497>
- Rong, Liu, Guo-Dong, Zhao, Wen-Bo, Zou, Xiu-Ping, Zhang, Shuai, Xu, Yang, Wang, Yan-Zhe, Liu, Yuan-Xing, Gao, Zhi-Peng, & Zhoua, Yu-Yao Song. (2022). Single-port robot-assisted hepatic left lateral sectionectomy using the da Vinci SP® system: A case report. *Intelligent Surgery*, 2, 6–9. <https://doi.org/10.1016/j.isurg.2022.02.002>
- Rothemund, P. W. (2006). Folding DNA to create nanoscale shapes and patterns. *Nature*, 440(7082), 297–302. <https://doi.org/10.1038/nature04586>
- Shi, C., Luu, D. K., Yang, Q., Liu, J., Chen, J., Ru, C., Xie, S., Luo, J., Ge, J., & Sun, Y. (2016). Recent advances in nanorobotic manipulation inside scanning electron microscopes. *Microsystems & nanoengineering*, 2, 16024. <https://doi.org/10.1038/micronano.2016.24>
- Suulker, C., Skach, S., & Althoefer, K. (2022). Soft Robotic Fabric Actuator With Elastic Bands for High Force and Bending Performance in Hand Exoskeletons. *IEEE Robotics and Automation Letter*, 7(4), 10621–10627. <https://doi.org/10.1109/LRA.2022.3194883>
- Sweeney, Aldrin. (2020). Incorporating NBIC social/ethical issues into STEM teacher education programmes. *Canada-Caribbean Institute Journal*, 1(1): Proceedings of the Canada-Caribbean Research Symposium. Canada-Caribbean Institute. Brock University Open Journal System. 2020. <https://journals.library.brocku.ca/index.php/cancarib/article/view/2369#>

- Taherkhani, S., Mohammadi, M., Daoud, J., Martel, S., & Tabrizian, M. (2014). Covalent binding of nanoliposomes to the surface of magnetotactic bacteria for the synthesis of self-propelled therapeutic agents. *ACS Nano*, 8(5), 5049–5060. <https://doi.org/10.1021/nn5011304>
- Vale, Daniel, El-Sharif, Ali, & Muhammed, Ali. (2022). Explainable artificial intelligence (XAI) post-hoc explainability methods: risks and limitations in non-discrimination law. *AI and Ethics*, 2, 815–826. <https://doi.org/10.1007/s43681-022-00142-y>
- Villa, K., & Pumera, M. (2019). Fuel-free light-driven micro/nanomachines: artificial active matter mimicking nature. *Chemical Society Reviews*, 48(19), 4966–4978. <https://doi.org/10.1039/C9CS00090A>
- Wan, M., Liu, Z., Li, T., Chen, H., Wang, Q., Chen, T., Tao, Y., & Mao, C. (2021). Zwitterion-Based Hydrogen Sulfide Nanomotors Induce Multiple Acidosis in Tumor Cells by Destroying Tumor Metabolic Symbiosis. *Angewandte Chemie International Edition*, 60(29), 16139–16148. <https://doi.org/10.1002/anie.202104304>
- Wang, H., & Pumera, M. (2015). Fabrication of Micro/Nanoscale Motors. *Chemical Reviews*, 115(16), 8704–8735. <https://doi.org/10.1021/acs.chemrev.5b00047>
- Wang, Joseph, & Wei, Gao. (2012). Nano/Microscale Motors: Biomedical Opportunities and Challenges. *ACS Nano*, 6(7), 5745–5751.
- Wenyan, Qiao, Linglin, Zhou, Zhihao, Zhao, Di, Liua, Shaoxin, Lia, Jie, Ana, Xinyuan, Lia, Yikui, Gao, Peiyuan, Yang, Jiaqi Liu, Zhong, Lin, Wang, & Jie, Wang. (2022). A self-powered vector motion sensor for smart robotics and personalized medical rehabilitation. *Nano Energy*, 104, 1–10. <https://doi.org/10.1016/j.nanoen.2022.107936>
- Xu, X., Saw, P. E., Tao, W., Li, Y., Ji, X., Bhasin, S., Liu, Y., Ayyash, D., Rasmussen, J., Huo, M., Shi, J., & Farokhzad, O. C. (2017). ROS-Responsive Polyprodrug Nanoparticles for Triggered Drug Delivery and Effective Cancer Therapy. *Advanced materials (Deerfield Beach, Fla.)*, 29(33), <https://doi.org/10.1002/adma.201700141>
- Xue, S. (2022). The Application of Virtual Metacognitive Network Model in Preschool Guiding Art Network Teaching, *6th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 672–675). <https://doi.org/10.1109/ICICCS53718.2022.9788219>
- You, M., Chen, C., Xu, L., Mou, F., & Guan, J. (2018). Intelligent Micro/nanomotors with Taxis. *Accounts of Chemical Research*, 51(12), 3006–3014. <https://doi.org/10.1021/acs.accounts.8b00291>
- Yuan, K., Aftoni, A., & Çobanoğlu, Ö. (2020). The Effect of Problem-Based Learning Model and Blended Learning Model to Metacognitive Awareness as a Reflection Towards a New Normal Era. *Jurnal Pendidikan Teknologi dan Kejuruan*, 26(2), 183–188. <https://doi.org/10.21831/jptk.v26i2.32783>
- Zaloilo, M. V., Pashentsev, D. A. (Ed.). (2020). *Modern legal technologies in law-making*. Moscow: IZISP: Norma: INFRA-M. (In Russ.).
- Zholobova, Yu. V., Schastlivceva, E. A. (2020). NBICS-technologies and the problem of anthropological evolution. *Herald of Vyatka State University*, 3(137), 7–19. (In Russ.).

Author information



Polina S. Gulyaeva – Post-graduate student of the Institute of Legislation and Comparative Law under the Government of the Russian Federation

Address: 34 Bolshaya Cheremushkinskaya Str., 117218 Moscow, Russian Federation

E-mail: polina-gulyaeva2016@bk.ru

ORCID iD: <https://orcid.org/0000-0002-4108-6379>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/HKV-7341-2023>

Google Scholar ID: <https://scholar.google.com/citations?hl=en&user=gPHDfmAAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1002457

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – September 8, 2022

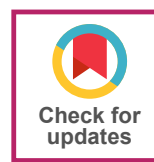
Date of approval – January 17, 2022

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 34:336:004
EDN: <https://elibrary.ru/rizoks>
DOI: <https://doi.org/10.21202/jdtl.2023.5>



Цифровые активы: правовое регулирование и оценка рисков

Светлана Владимировна Мурадян 

Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя
г. Москва, Российская Федерация

Ключевые слова

Биткоин,
блокчейн,
криптовалюта,
право,
регулирование,
риск,
токен,
финансы,
цифровая валюта,
цифровой актив

Аннотация

Цель: обоснование необходимости создания основанного на единообразной категоризации цифровых активов и авторского понимания концепции риска цифровых активов унифицированного механизма правового регулирования цифровых валют и токенизированных активов для обеспечения безопасности их оборота правовыми средствами и эффективного развития в будущем цифровой экономики на глобальном уровне.

Методы: исследование проводилось посредством комбинированного сочетания разноуровневых средств познания: от философских до частнонаучных, ключевое место среди которых отводится системному подходу, методу сравнительного правоведения и формально-юридическому анализу нормативного материала.

Результаты: представленное исследование закладывает концептуальную основу построения глобальной системы правового регулирования оборота цифровых активов и способствует определению и решению ключевых вопросов, которые необходимо возникают при анализе действующих механизмов правового регулирования на национальном уровне и оценке законности различных видов цифровых активов.

Научная новизна: заключается в комплексном рассмотрении сущности и особенностей правовой природы различных видов цифровых активов, обладающих наряду с существенными преимуществами высокими рисками как с правовой, так и с финансовой точек зрения. На основе противоречивых подходов и выявленных пробелов в правовом регулировании различных видов цифровых активов автором предлагается единообразная категоризация цифровых активов, обосновывается концепция риска цифровых активов, предпринимается попытка обоснования необходимости создания унифицированного механизма правового регулирования цифровых валют и токенизированных активов, что позволит сформировать эффективную систему способов защиты права собственности на них и обеспечить безопасность их оборота.

© Мурадян С. В., 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: обусловлена отсутствием в настоящее время унифицированного подхода и возможности применения действующих правовых норм в отношении инновационных цифровых активов, учитывающих их специфику, несмотря на их трансграничный характер. Основные положения и выводы исследования могут быть использованы для совершенствования механизмов правового регулирования оборота цифровых активов.

Для цитирования:

Мурадян, С. В. (2023). Цифровые активы: правовое регулирование и оценка рисков. *Journal of Digital Technologies and Law*, 1(1), 123–151. <https://doi.org/10.21202/jdtl.2023.5>

Содержание

Введение

1. Сущность и особенности правовой природы цифровых активов
 - 1.1. Технология блокчейн как основа построения цифровой экосистемы
 - 1.2. Сущность и классификация цифровых активов, функционирующих на основе распределенного реестра
 - 1.2.1. Отличия цифровых активов от других нематериальных активов
 - 1.2.2. Классификация цифровых активов
 - 1.3. Особенности построения правовой системы регулирования токенизированных цифровых активов в Российской Федерации
 - 1.4. Регулирование рынка ICO
 - 1.5. Регулирование оборота активов, непосредственно созданных в распределенных реестрах
 - 1.5.1. Сущность цифровых валют центральных банков государств
 - 1.5.2. Криптовалюты как объект гражданских прав и предмет преступления
 - 1.5.3. Правовая защита лиц, являющихся собственниками виртуальной валюты и виртуального имущества в Российской Федерации
2. Оценка рисков, возникающих в процессе оборота цифровых активов
 - 2.1. Риск волатильности
 - 2.2. Риск неправильной оценки
 - 2.3. Риск ликвидности
 - 2.4. Технологический риск
 - 2.5. Риск жесткого форка (hardfork)
 - 2.6. Криминальные риски, связанные с оборотом цифровых активов
 - 2.7. Операционный риск
 - 2.8. Кредитный риск и риск контрагента
 - 2.9. Специфические риски, связанные с хранением цифровых активов
 - 2.10. Особые риски, связанные с токенизированными ценными бумагами, токенами ценных бумаг или ценными бумагами на основе DLT
 - 2.11. Правовые риски

Выводы

Список литературы

Введение

В последние несколько десятилетий международная финансовая система демонстрирует тенденцию к усложнению. Экономисты определяют эту сложность в виде большего разнообразия новых финансовых инструментов и типов финансовых посредников. В основе сложной паутины битов и байтов, которую представляет собой современная финансовая система, лежит возможность обмена и передачи капитала между различными участниками экономики. Заемщики, кредиторы, инвесторы и предприниматели образуют, по сути, четыре угла квадрата. До недавнего времени государство, находясь на вершине этой четырехугольной пирамиды, регулировало деятельность всех субъектов у ее основания. Однако с появлением цифровых активов возможности такого регулирования резко сократились. Реакция государств на подобные изменения сильно варьируется ([Hendrickson & Luther, 2021](#)), поскольку достижения в области цифровых технологий и технологии распределенных реестров для финансовых услуг, которые и привели к резкому росту рынков цифровых активов, имеют глубокие последствия в возможностях защиты потребителей, инвесторов и бизнеса, включая конфиденциальность и безопасность данных, финансовую стабильность, национальную безопасность, последствия от преступных действий и т. д.

Сложившаяся практика демонстрирует, что подходы государств ([González-Gallego & Pérez-Cárceles, 2021](#)), основанные на попытках игнорирования существующих тенденций и возникающих проблем, лишь усугубляют положение в их финансовых системах. Намного более позитивным выглядит подход, позволяющий создать системное правовое регулирование на внутригосударственных уровнях, согласованное с разрабатываемыми международными стандартами. Подобное регулирование должно быть направлено на предотвращение масштабных рисков для населения, экономики и финансовой системы государств, возникающих в результате использования цифровых активов. Идеальные цели такого регулирования в сфере финтеха и криптовалют заключаются в продвижении инноваций, защите целостности рынка и обеспечении оптимального уровня ясности на рынке, хотя регуляторы часто не могут достичь всех трех целей одновременно ([Yadav & Brummer, 2019](#)). Связано это с тем, что изначально цифровые децентрализованные системы создавались с целью избежать такого регулирования и контроля и исключить государственные органы и банки из своего контура «денежного» обращения и подтверждения транзакций и прав.

1. Сущность и особенности правовой природы цифровых активов

1.1. Технология блокчейн как основа построения цифровой экосистемы

Цифровые активы функционируют как часть сложной и взаимосвязанной цифровой экосистемы. Основой экосистемы является блокчейн – тип распределенной бухгалтерской книги, в которой регистрируются транзакции и участники совершают сделки с другими участниками и децентрализованными приложениями. Технология блокчейн – это радикальная инновация, способная бросить вызов или даже заменить существующие бизнес-модели, полагающиеся на доверие третьих сторон ([Beck & Müller-Bloch, 2017](#)). Концепция блокчейна была представлена в 2008 г.

с выходом документа «Биткойн»¹ и в первые годы использовалась в качестве технологии, лежащей в основе криптовалют. Однако, поскольку он не обладает полной программируемостью, в 2014 г. было представлено второе поколение блокчейнов, которое позволяет программировать и исполнять программное обеспечение – так называемые смарт-контракты – на всех участвующих узлах блокчейна. Наибольшую популярность среди них приобрел Ethereum, который, как и другие блокчейны смарт-контрактов, такие как Solana, Terra, BSC, позволяет сдавать свой блокчейн (хранящий смарт-контракты и транзакции) и свою виртуальную машину (необходимую для чтения и выполнения смарт-контрактов) в аренду проектам, которые хотят использовать децентрализованную среду (далее – DeFi) без необходимости поддерживать инфраструктуру блокчейна (Hugo & De Quenetain, 2022). DeFi – это новая форма финансовых приложений, ориентированных на потребителя и состоящих из смарт-контрактов, развернутых на технологии блокчейн без разрешений (Jensen et al., 2021). Следовательно, любой пользователь получает возможность создавать и внедрять программы на общей глобальной инфраструктуре².

На сегодняшний день правовое регулирование блокчейн в разных странах идет совершенно по разному пути. Немедленное широкоформатное регулирование рынков децентрализованного финансирования на государственном уровне, которые находятся еще в ранней стадии созревания, может привести к ошибкам в регулировании и частым изменениям в законодательстве, что мы и наблюдаем в ряде государств. Более того, многие продукты децентрализованного финансирования плохо вписываются в существующую систему финансового регулирования многих стран (Ozili, 2022). Однако, учитывая, что проблемы регулирования децентрализованных финансов приобрели характер мировых, представляется необходимым скоординировать усилия регуляторов по созданию правил и процедур их обращения под эгидой некоего глобального института управления финансами в лице Международного валютного фонда, Группы разработки финансовых мер по борьбе с отмыванием денег (далее – ФАТФ), Базельского комитета по банковскому надзору, Международной организации Комиссии по ценным бумагам.

1.2. Сущность и классификация цифровых активов, функционирующих на основе распределенного реестра

Цифровые активы – это цифровые представления любых видов активов, ценных бумаг, прав, валют или учетных единиц, зарегистрированных в распределенной бухгалтерской книге, такой как блокчейн. Не существует общей системы категоризации для цифровых активов, что является серьезным препятствием для регулирования

¹ Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System (White Paper)*. The official site of the United States Sentencing Commission. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

² Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper Journal*, 3. https://scholar.google.co.kr/citations?view_op=view_citation&hl=en&user=DLP9gTAAAAAJ&citation_for_view=DLP9gTAAAAAJ:lJCSPb-OGc4C ; Wood, G. (2017). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 1–32. <https://membres-ljk.imag.fr/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/Ethereum/ethereum-yellowpaper.pdf>

и управления цифровыми активами, которые часто существуют в международной и мультиюрисдикционной среде. Классификация цифровых активов должна зависеть от их природы и сущности, т. е. в соответствии с правами и обязанностями, которые они налагают на владельца, а также от их основного экономического назначения и функции актива. Изменение формы актива не обязательно меняет его юридическую сущность, но может привести к появлению новых механизмов создания, хранения, доставки и передачи актива, что влечет за собой правовые последствия. Это легко проиллюстрировать на примере цифровой облигации: хотя природа актива сохранится, цифровая форма может повлиять на способ ее передачи и, следовательно, повлечь за собой иные правовые последствия³.

1.2.1. Отличия цифровых активов от других нематериальных активов

В отличие от других нематериальных активов, основанных на внутренних электронных системах учета (например, дематериализованных акций), ключевыми характеристиками анализируемых «новых» цифровых активов являются:

а) расширяемость: права и обязательства могут быть непосредственно закодированы в активах и автоматически исполняться;

б) управляемость с помощью криптографических ключей: криптографические ключи необходимы для доступа к активам и подписания транзакций, чтобы инициировать передачу активов;

с) совместимость: цифровые активы могут, за исключением искусственных ограничений, свободно перемещаться по системе, в которой они были выпущены, и взаимодействовать с другими цифровыми активами, существующими в тех же границах.

1.2.2. Классификация цифровых активов

Цифровые активы включают с учетом корреляции понятий, используемых российским законодателем и общепринятых в IT-терминологии, виртуальные активы, т. е. активы, непосредственно созданные в распределенных реестрах, а также токенизированные цифровые активы, существующие в реальном выражении, права на которые помещены в цифровую среду. Подобная классификация важна в первую очередь именно для определения правового статуса каждого из них и возможных мер правовой защиты пользователей. Однако с точки зрения международного подхода чаще всего используется классификация цифровых активов на токены, в рамках которой сложно выделить критерии, позволяющие соотнести терминологию, применяемую в зарубежных законодательствах, с отечественной.

Да и в ряде зарубежных государств имеются некоторые противоречия, несмотря на существование устоявшейся классификации токенов, де-факто одни и те же токены в одной стране мира могут признаваться служебными токенами, а в другой – инвестиционными. Что в итоге приводит к несоразмерной защите прав граждан, участвующих в обороте цифровых активов в различных юрисдикциях.

³ Allen, G. J., Rauches, M., Blanding, A., & Bear, K. (2020). *Legal and Regulatory Considerations for Digital Assets*. Cambridge Center for Alternative Finance. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>

Глобальная система правового регулирования оборота цифровых активов, по крайней мере, сможет заложить унифицированную терминологию, основы единой классификации, исходя из того круга прав и обязанностей, которые могут предоставить те или иные цифровые активы, а значит, придерживаясь подобной концепции, будет возможно создать единые механизмы правовой защиты участников правоотношений в области оборота цифровых активов. Безусловно, государства вправе создать свои собственные правовые механизмы в регулировании отдельных аспектов оборота тех или иных цифровых активов, однако, учитывая их трансграничный характер, унифицированная основа в любом случае необходима.

Отдельно следует выделить невзаимозаменяемые, или нефунгицидные, токены (далее – NFT). NFT – это новый тип уникальных и неделимых токенов на основе блокчейна. Изначально начавшись как художественный/игровой эксперимент, NFT породили новую форму предпринимательства в виртуальном мире с огромными преимуществами и возможностями (Chandra, 2022). Они отличаются от других цифровых активов, таких как токены и монеты, тем, что неразрывно связаны с базовым активом. Каждый NFT уникален, его нельзя разделить или объединить⁴. NFT в основном используются в качестве подтверждения права собственности на физические активы (предметы роскоши, автомобили) или цифровые товары (виртуальные игровые активы, цифровые произведения искусства и лицензии на программное обеспечение)⁵. Такие токены регулярно обмениваются пользователями для подтверждения того, что активы, уникальность которых трудно доказать (например, цифровые изображения), находятся в исключительной собственности⁶.

В то время как взаимозаменяемые токены позволили создать новые сценарии использования, например первичные предложения монет, потенциал NFT как ценного компонента до сих пор полностью неясен. С правовой точки зрения не существует унифицированных правовых стандартов, отвечающих на вопрос, чем на самом деле владеет держатель NFT, базовым активом, его долей или только правом на интеллектуальные права на него. Если речь идет о праве на интеллектуальные права, тогда необходимо определиться и с объемом ограничений, наложенных на них. В последнее время произошли некоторые положительные изменения – например, суды Сингапура и Англии недавно признали NFT имуществом (Mezei, 2022), которое может быть защищено судебным запретом и постановлением о замораживании.

⁴ Voshmgir, S. (2018, September 23). *Fungible Tokens vs. Non-Fungible Tokens*. <https://medium.com/token-kitchen/fungible-tokens-vs-non-fungible-tokens-69871b0e37a9>

⁵ Griffin, J. (2018, April 12). *Software licences as non-fungible tokens*. <https://medium.com/collabs-io/software-licences-as-non-fungible-tokens-1f0635913e41>

⁶ Bella, Giampaolo, Cantone, Domenico, Longo, Cristiano, Asmundo, Marianna Nicolosi, & Santamaria, Daniele. (2021). *Blockchains through ontologies: the case study of the Ethereum ERC721 standard in \ ONT\} (Extended Version)*. https://www.researchgate.net/publication/354435217_Blockchains_through_ontologies_the_case_study_of_the_Ethereum_ERC721_standard_in_ONT_Extended_Version

1.3. Особенности построения правовой системы регулирования токенизированных цифровых активов в Российской Федерации

Токенизация способствует финансиализации актива путем создания моста между активом и его цифровым аватаром (т. е. токеном). По сути, основные преимущества токенизации напрямую связаны с преимуществами технологии распределенных реестров (далее – DLT). Именно поэтому повышение эффективности, повышение ликвидности (Chokor & Alfieri, 2021) и прозрачности, вероятно, являются одними из самых упоминаемых преимуществ токенизации активов и ценных бумаг.

При попытке урегулирования оборота таких объектов Российская Федерация, исходя из традиций построения правовой системы в нашей стране, пошла по своему собственному пути, переименовав токен в «цифровое право». По сути, оно не является новым объектом права, а, как и токен, представляет собой новую форму фиксации существующих прав.

Придерживаясь позиции выработки унифицированной терминологии в рамках действующего законодательства, можно утверждать, что удостоверенные токенами права на объекты гражданских прав, представляя собой цифровые права, могут быть защищены гражданско-правовыми способами и одновременно, в случае посягательства на них, могут быть признаны предметом хищений в уголовном праве. Соотнесем существующие токены с цифровыми правами в соответствии со ст. 141.1 Гражданского кодекса Российской Федерации (далее – ГК РФ)⁷.

Вступивший в силу с 1 января 2020 г. Федеральный закон от 2 августа 2019 г. № 259-ФЗ (ред. от 14 июля 2022 г.) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» ввел понятие утилитарных цифровых прав⁸. Предполагалось, что они должны быть точной копией служебных токенов. Но по смыслу закона получается, что последние могут быть приравнены к утилитарным цифровым правам, только если созданы на платформе, отвечающей всем стандартам вышеназванного Федерального закона. В случае если компания в любой точке мира отказывается произвести такие изменения, которые от нее требует Федеральный закон Российской Федерации, права лица, имеющего токены в рамках такой цифровой платформы, защите на территории Российской Федерации не подлежат.

Согласно Федеральному закону от 31 июля 2020 г. № 259-ФЗ (ред. от 14 июля 2022 г.) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», еще одним видом

⁷ Гражданский кодекс Российской Федерации (часть первая). № 51-ФЗ (1994). <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXYahdpr&cacheid=C3BA75257675D5072BCC4E7ECE908376&mode=splus&rnd=bEJ38g&base=LAW&n=410306#AN2c5ETP7HDTbfU6>

⁸ О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ. (2019). <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXYahdpr&cacheid=3574F9E534E3295CF57286D2146F42E7&mode=splus&rnd=bEJ38g&base=LAW&n=422183#giik5ET2GqHWqfYA1>

цифровых прав в России признаются цифровые финансовые активы⁹, т. е. инвестиционные токены. Они могут быть представлены денежными требованиями к эмитенту, а также представлять собой право участия в капитале непубличного акционерного общества и права по эмиссионным ценным бумагам, включая требования их передачи.

На данный момент Банк России зарегистрировал три платформы, которые могут выпускать подобные активы в обращение: Atomyze, Сбербанк и Lighthouse. А вот обеспечивать заключение сделок с цифровыми финансовыми активами (обмен, покупка, продажа, погашение) могут лишь компании из реестра операторов обмена, который будет вести Центральный Банк России. Однако на данный момент ни один такой оператор обмена в реестре не числится.

Весьма сомнительной представляется позиция законодателя согласно пояснительной записке к законопроекту от 26 марта 2018 г. № 424632-7 «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» о том, что цифровые права необходимо регулировать как «важную для экономики сущность», а «бонусы, виртуальные предметы и т. п. не надо, поскольку они не имеют существенного значения для экономики»¹⁰. В случае с бонусами речь идет о так называемых токенах-вознаграждениях. В последнее время все большую популярность приобретают маркетплейсы, которые активно используют подобные токены вместо баллов за лояльность. Таким образом, пропадает страх потерять карту лояльности, а у интернет-площадок появляется возможность токенизировать свой бизнес, воспользовавшись всеми преимуществами блокчейн-технологий.

Существуют также токены-пожертвования – это просто своеобразные баллы без каких-либо обязательств и функциональной нагрузки. Они начисляются за пожертвования в пользу проекта.

Можно сделать вывод, что часть служебных токенов, токены-вознаграждения и токены-пожертвования законодателем не отнесены к категории цифровых прав, что весьма странно, учитывая, что в пояснительной записке к вышеупомянутому законопроекту от 26 марта 2018 г. № 424632-7 вводится базовое понятие «цифровое право» вместо термина «токен» в новом современном его значении, как шифр, владение которым дает в сети определенные возможности¹¹.

Предполагаем, что подобное решение обусловлено в том числе и тем, что токены-вознаграждения и токены-пожертвования не открывают доступ к функционалу блокчейна и не дают права собственности на что-либо, поэтому законодатель их обошел при конструировании понятия «цифрового права».

При пристальном изучении можно сказать, что подход российского законодателя схож с международным. Наиболее близкой к внедренной в российскую правовую

⁹ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ. (2020). <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E14508391CB5EC1A9DF3236C4497BB05&mode=splus&rnd=bEJ38g&base=LAW&n=422194#bKfe5ETZtZtV2pdS>

¹⁰ Пояснительная записка к законопроекту № 424632-7 от 26.03.2018 «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации». (2018). <https://sozd.duma.gov.ru/bill/424632-7?ysclid=I6ncm2y5pu318025418>

¹¹ Там же.

систему классификации «цифровых прав» является классификация токенов, разработанная Комиссией по ценным бумагам и биржам Соединенных Штатов Америки (далее – SEC) и Службой по надзору за финансовыми рынками Швейцарии (далее – FINMA). Интеграция позиции FINMA, направленной на оценку экономической функции токена, с позицией SEC, основанной на оценке степени родства токена с ценными бумагами, позволила классифицировать их на платежные токены или криптовалюты, токены-активы или инвестиционные токены (токены безопасности) и потребительские (служебные) токены (Рожкова, 2020).

Виртуальные активы включают в себя криптовалюты (согласно российскому законодательству, цифровые валюты) и другие токены оплаты, токены, созданные путем ICO (Initial Coin Offering – предложение цифровых токенов или монет с использованием технологии блокчейн (Zetzsche et al., 2018)). Подтверждение согласованности позиции российского законодателя с общемировыми трендами можно увидеть и в том, какие криптографически защищенные цифровые активы ICO эмитент может продавать:

А. Криптовалюту – финансовый инструмент, задействующий современное шифрование для проверки и защиты онлайн-транзакций, который может быть использован для оплаты в сделках с любым человеком, готовым их принять (Kopaliani, 2022). Такие цифровые активы работают на уникальном распределенном реестре и образуют вместе с ним общую платежную систему. Единица подобных криптовалют – монета или коин.

Б. Инвестиционный токен, представляющий собой обычную ценную бумагу, которая регистрируется и обменивается на блокчейне для снижения транзакционных издержек и создания записи о праве собственности (при этом базовые активы могут варьироваться от товаров до валют, недвижимости или даже корпоративных акций). Они дают владельцу право на участие в будущих доходах эмитента и в некоторых случаях право голоса или другие права участия¹².

В. Утилитарный токен, который дает его владельцу потребительские права на доступ к продукту или услуге.

То есть токены-пожертвования и токены-вознаграждения выступают инструментом при сборе средств в рамках краудфандинга, но не краудинвестинга.

1.4. Регулирование рынка ICO

Рассматривая токен в рамках ICO, необходимо оценивать его исключительно как средство инвестирования, а последующий оборот таких токенов требует разработки самостоятельных правил. Финансирование для бизнес-проектов привлекается через выпуск и размещение среди неограниченного круга инвесторов собственных цифровых активов-токенов в обмен на ликвидную криптовалюту¹³, которая в дальнейшем

¹² European Parliament. (2021). *Briefing "Understanding initial coin offerings. A new means of raising funds based on blockchain"*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI\(2021\)696167_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf)

¹³ Аксаков, А. (2017, 9 декабря). Понятие «токен» может быть определено законодательно. Комитет Государственной Думы по финансовому рынку. <https://komitet2-12.km.duma.gov.ru/Novosti-Komiteta/item/14060239?ysclid=I6vd095wkt214089722>

может быть конвертирована в «фиатные» денежные средства. При этом потенциальные риски для вкладчиков здесь максимально велики (Hsieh & Brennan, 2022). Они могут потерять свои активы как в связи с неблагоприятной финансовой ситуацией, например, в результате провала стартапа, так и в связи с совершением противоправных действий со стороны эмитентов, например, мошенничества, когда полученные средства используются не только для целей развития проекта.

Федеральный закон от 2 августа 2019 г. № 259-ФЗ не предусматривает возможности осуществлять инвестирование посредством криптовалют, хотя в целом допускает его¹⁴. В этой связи отсутствие должного правового регулирования приводит к тому, что эмитенты выбирают для реализации ICO-проектов иностранные юрисдикции с прозрачной законодательной позицией и благоприятным налоговым режимом. Однако иностранные государства также стараются всячески урегулировать и обезопасить рынок ICO. Анализ судебной практики Соединенных Штатов Америки (далее – США) показывает, что ряд платежных токенов суды США признают ценными бумагами, стремясь распространить на них соответствующее правовое регулирование. Оговариваясь при этом, что вложение денег в криптовалюту, используемую членами децентрализованного сообщества, функционирующего на основе технологии блокчейн, которая сама управляется этим сообществом пользователей, а не общим предприятием, вряд ли будет считаться ценной бумагой в соответствии с известным тестом, изложенным в *S.E.C. против W.J. Howey Co.*, 328 U.S. 293, 298-99 (1946)¹⁵. Однако в ряде случаев, когда эмитенты предпринимают попытки избежать федеральных законов США о ценных бумагах, маркируя свой продукт криптовалютой или цифровым токеном, такие действия лиц признаются незаконными и эмитентов обязуют вернуть денежные средства инвесторам. Так, продажа Telegram и TON 2,9 миллиарда Граммов 175 покупателям в обмен на 1,7 миллиарда долларов является частью более крупной схемы по распределению этих Граммов на вторичном публичном рынке. Учитывая экономические реалии в соответствии с тестом Хоуи, суд США посчитал, что в контексте этой схемы перепродажа Граммов на вторичном публичном рынке является неотъемлемой частью продажи ценных бумаг без обязательного заявления о регистрации¹⁶. При решении вопроса о том, является ли цифровой актив ценной бумагой, SEC сравнивает его с «инвестиционным контрактом»¹⁷, предполагающим «широкий спектр многосторонних инвестиционных отношений»¹⁸ (Jackson, 1999). Если цифровой актив выражен в коде, сопутствующие факты и обстоятельства,

¹⁴ О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ. (2019). <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=3574F9E534E3295CF57286D2146F42E7&mode=splus&rnd=bEJ38g&base=LAW&n=422183#giik5ET2GqHWqfYA1>

¹⁵ SEC v. W.J. Howey Co., 328 U.S. 293 (1946). <https://supreme.justia.com/cases/federal/us/328/293/>

¹⁶ United States District Court against Telegram Group Inc. and Ton Issuer Inc. Southern district of New York, 1:19-cv-09439-PKC. (2020). <https://cases.justia.com/federal/district-courts/new-york/nysdce/1:2019cv09439/524448/227/0.pdf?ts=1585128306>

¹⁷ Hinman, William. (2018, June, 14). *Digital Asset Transactions: When Howey Met Gary (Plastic)*. U.S. Sec. & Exch. Comm'n. <https://www.sec.gov/news/speech/speech-hinman-061418>

¹⁸ SEC v. W. J. Howey Co., 328 U.S. 293, 298 (1946) [defining «investment contract»]. <https://www.lexisnexis.com/community/casebrief/p/casebrief-sec-v-w-j-howey-co>

включая способ его распространения, могут указывать на инвестиционную деятельность (Goforth, 2021). Некоторые цифровые активы на основе блокчейна считаются товарами. Примером могут служить криптовалюты, которые служат средством хранения и передачи стоимости и «могут колебаться в цене, как и любой товар»¹⁹. Однако даже если цифровой актив является товаром, «любой конкретный цифровой актив может подпадать или не подпадать под действие законов о ценных бумагах», а «многие ценные бумаги являются товарами, к которым применяются законы о ценных бумагах»²⁰.

В целях единообразия подходов государств к регулированию оборота цифровых активов необходимо перевести в цифровой формат все традиционные процессы финансирования и инвестирования, а также соответствующую инфраструктуру. Задача состоит в том, чтобы объединить знания о механике рынков капитала, нормативно-правовых требованиях и технологических возможностях в прибыльную бизнес-модель, признанную по всему миру, которая принесет пользу всем участникам базовой экосистемы (Egloff & Turnes, 2021).

1.5. Регулирование оборота активов, непосредственно созданных в распределенных реестрах

Согласно позиции ФАТФ, виртуальные активы являются средством цифрового выражения стоимости, которое может торговаться или переводиться цифровым образом и может быть использовано для целей платежей или инвестиций. При этом они не включают в себя средства цифрового выражения фиатных валют, ценных бумаг и других финансовых активов²¹.

1.5.1. Сущность цифровых валют центральных банков государств

Такое выделение цифровых валют центральных банков государств из общего концепта регулирования вполне объяснимо, учитывая совершенно другую природу данного инструмента и возможных рисков. Изучение возможности создания цифровой валюты центрального банка (CBDC) было приоритетным для многих стран в течение последних нескольких лет. CBDC представляется следующим шагом в развитии глобального валютного режима, при этом многие страны уже используют или тестируют программу CBDC (Mack, 2022). Так, например, создаваемый в России цифровой рубль существенно отличается от иных виртуальных активов. Во-первых, согласно Докладу для общественных консультаций Банка России, цифровой рубль выполняет все функции денег, являясь средством обращения, платежа, мерой стоимости

¹⁹ SEC v. Telegram Inc., 19-cv-9439 (PKC), 2020 U.S. Dist. LEXIS 53846 (S.D.N.Y. Mar. 24, 2020). <https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2019cv09439/524448/227/>

²⁰ Schwartz, Robert A. (2020). [Letter to the Hon. P. Kevin Castel]. SEC v. Telegram Group, Inc., et al., No. 1:19-cv-09439 (PKS). <https://www.docdroid.net/okmUUBS/cftc-letter-in-telegram-case.pdf>

²¹ Международный учебно-методический центр финансового мониторинга. (2021, октябрь). Обновленное руководство ФАТФ по применению риск-ориентированного подхода в отношении виртуальных активов и провайдеров услуг в сфере виртуальных активов. <https://mumcfm.ru/d/ZMaQyboDDR Xwu6OnbQGfEJE8X3HwM82WP5oRyrZ>

и средством сбережения. Во-вторых, он имеет эмитента, гарантирующего надежность и ответственность процесса выпуска и обращения цифрового рубля. В-третьих, цифровой рубль – это обязательство государства, стоимость которого эквивалентна наличной и безналичной формам рубля²².

1.5.2. Криптовалюты как объект гражданских прав и предмет преступления

Все возрастающие масштабы использования криптовалют (Orr, 2023), сопряженные с высокими рисками их применения для отмыwania доходов, финансирования терроризма, а также для обслуживания теневого сектора экономики (Remolina, 2022), потребовали от законодателя разработать публично-правовые установления, в том числе некие требования к обеспечению безопасности соответствующего оборота, и с 1 января 2021 г. вступил в силу Федеральный закон от 31 июля 2020 г. № 259-ФЗ, в котором было дано определение цифровых валют и сделаны шаги по урегулированию их оборота²³. Тем не менее все большее число противоречий, возникающих в процессе гражданско-правовой квалификации цифровых валют, а также квалификации противоправных действий с их использованием или в отношении криптовалют, дали законодателю основание полагать, что предпринятая попытка была недостаточно плодотворной. Уже в феврале 2022 г. Правительство Российской Федерации утвердило Концепцию законодательного регулирования оборота цифровых валют, в которой признало, что в настоящее время в России отсутствует законодательное регулирование такого высокорискованного финансового инструмента, как цифровая валюта (криптовалюта)²⁴.

В этой связи вполне закономерно наблюдать следующие позиции судов. Орджоникидзевский районный суд г. Екатеринбурга в своем решении от 14 июля 2021 г. по делу № 2-2582/2021 о взыскании задолженности по договору займа и процентов за пользование займом, предметом которого явились криптовалюты, сделал вывод, что использование криптовалют при совершении сделок является основанием для рассмотрения вопроса об отнесении таких сделок (операций) к сделкам (операциям), направленным на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма²⁵. В связи с этим все операции с использованием данного инструмента производятся участниками гражданского

²² Банк России. (2020, октябрь). *Цифровой рубль. Доклад для общественных консультаций*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E857D3D7DAC98A55137DBF16CDDA25F2&mode=splus&rnd=bEJ38g&base=LAW&n=364913#2ETe5ETILns7qxqQ1>

²³ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ. (2020). <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E14508391CB5EC1A9DF3236C4497BB05&mode=splus&rnd=bEJ38g&base=LAW&n=422194#bKfe5ETZtZtV2pdS>

²⁴ Концепция законодательного регламентирования механизмов организации оборота цифровых валют. (2022). <https://static.government.ru/media/files/Dik7wBqAubc34ed649ql2Kg6HuTANrqZ.pdf>

²⁵ Росфинмониторинг. (2014, 6 февраля). *Об использовании криптовалют*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=569654B8A75A572436E6B27A04580986&mode=splus&rnd=bEJ38g&base=LAW&n=158661#Teqe5ET0268ebgBn>

оборота на свой риск. При этом судебная защита по их требованиям не предоставляется вне зависимости от того, насколько они являются обоснованными²⁶.

Криптовалюты обладают потенциалом для облегчения и обработки небольших сумм денег с большой скоростью и низкими затратами²⁷. Однако криптовалюту нельзя отнести к чисто финансовым активам, поскольку она не является деньгами, а также долевым инструментом другой организации, она не порождает договорного права для владельца получить денежные средства или финансовые активы в будущем, и это не договор, расчеты по которому будут или могут быть осуществлены собственными долевыми инструментами²⁸. Вместе с тем криптовалюта может быть квалифицирована как объект гражданских прав, так как она способна к обособлению и имеет имущественную ценность, признаваемую оборотом²⁹.

Анализ имеющейся практики позволяет утверждать, что криптовалюта регулярно выступает предметом обязательств, а также подлежит защите со стороны норм деликтного права. Конечный вопрос, лежащий в основе большинства дел, касается имущественно-правового режима криптоактивов, который является предварительным вопросом для решения других вопросов материального и процессуального права. Этот вопрос определяет две другие тенденции. Во-первых, наблюдается тенденция к более тесному взаимодействию с некоторыми из последующих вопросов, связанных с режимом криптоактивов в праве собственности. Во-вторых, в мире гражданского права наблюдается тенденция к поиску обходных путей для облегчения упорядоченного правового режима криптоактивов в более ограничительных концептуальных схемах, характерных для гражданского права собственности (Allen et al., 2022).

На наш взгляд, можно согласиться с позицией, что криптовалюту целесообразно относить к «иному имуществу» по смыслу ст. 128 ГК РФ. И тогда криптовалюты могут признаваться предметом преступления, что особенно актуально, учитывая их финансовую привлекательность. При этом позиции судов в этом вопросе иногда носят совершенно полярный характер.

Так, в приговоре Солнечногорского городского суда Московской области от 7 октября 2020 г. № 1-227/2020 суд приравнивает криптовалюту к электронным средствам платежа³⁰. Хотя, согласно ч. 5 ст. 14 Федерального закона от 31 июля 2020 г.

²⁶ Орджоникидзевский районный суд города Екатеринбурга. (2021). *Решение от 14.07.2021 по делу № 2-2582/2021*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=183F7C58A28644AB4D573FF3D3536288&mode=splus&rnd=bEJ38g&base=AOUR&n=6488711#ZJVg5ETwq0onclzK>

²⁷ Popescu, Andrei-Dragos. (2021). Financial Technology (FinTech) as a Driver for Financial Digital Assets. *Analele Universitatii Ovidius Constanta*, XX, 1055. https://www.researchgate.net/publication/350004620_Financial_Technology_FinTech_as_a_Driver_for_Financial_Digital_Assets

²⁸ Министерство финансов РФ. (2015). *Международный стандарт финансовой отчетности (IAS) 32 «Финансовые инструменты: представление»*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=848D0A4D7FDF20D0993D13EE13A0802B&mode=splus&rnd=bEJ38g&base=LAW&n=374637#prwg5ETCqLhbSNVG>

²⁹ Минюст назвал криптовалюту «иным имуществом». <https://cryptonews.net/ru/news/regulation/65650/?ysclid=I6vck3v9l8673770654>.

³⁰ Солнечногорский городской суд Московской области. (2020). *Приговор от 07.10.2020 № 1-227/2020*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=5EA18D3245367237670AA08F26D4C0BA&mode=splus&rnd=bEJ38g&base=AOKI&n=8961537#mHTj5ETOkQz5RvN81>

№ 259-ФЗ, юридические и физические лица в Российской Федерации не вправе принимать цифровую валюту в качестве встречного предоставления за передаваемые ими товары, выполняемые ими работы, оказываемые ими услуги или иного способа, позволяющего предполагать оплату цифровой валютой товаров (работ, услуг)³¹.

Совершенно иной позиции придерживается Санкт-Петербургский городской суд, который при рассмотрении апелляционной жалобы П. на приговор Петроградского районного суда г. Санкт-Петербурга от 20 декабря 2021 г., которым П. был признан виновным в совершении преступления, предусмотренного п. «б» ч. 3 ст. 161 Уголовного кодекса Российской Федерации, не согласился с доводами защиты. Защита просила устранить допущенные судом первой инстанции нарушения уголовно-процессуального закона и исключить из объема обвинения хищение криптовалюты как предмета с отсутствием правового статуса. Санкт-Петербургский городской суд посчитал, что цифровая валюта в виде биткоинов, битшейресов и дигибайтов, похищенных П. и Е., может быть признана имуществом, поскольку использовалась и используется как средство платежа, инвестиций и накопления сбережений, т. е. представляет экономический интерес, а также имеет материальную ценность³².

Третий кассационный суд общей юрисдикции мнение Санкт-Петербургского городского суда поддержал, указав, что по сути основным отличием криптоденег от денег является только способ их возникновения, а поскольку понятие криптовалюты не закреплено законодательно, то следует согласиться с отнесением ее в обвинении, предъявленном осужденным, к «иному имуществу»³³. Подобные позиции судов позволяют защитить уголовно-правовыми средствами нарушенные права собственников криптовалюты в условиях правовой неопределенности.

Ранее Санкт-Петербургский городской суд уже находил интересный выход из ситуации, где цифровая валюта выступала предметом посягательства. Так, в Апелляционном определении от 20 декабря 2021 г. по делу № 1-19/2021, 22-5752/2021 суд указал, что не принимает доводы стороны защиты о том, что биткоин и иные виды криптовалюты не являются предметом вымогательства, поскольку стоимость их не зафиксирована государством, и оборот криптовалюты не регулируется государством, поскольку изначально В. А. вымогал деньги, а криптовалюта была только способом сокрытия перечисления этих денег³⁴.

³¹ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ. 31.07.2020. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E14508391CB5EC1A9DF3236C4497BB05&mode=splus&rnd=bEJ38g&base=LAW&n=422194#bKfe5ETZtV2pdS>

³² Санкт-Петербургский городской суд. (2022). Апелляционное определение от 16.05.2022 № 22-2616/2022, 1-257/2021. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=97DB8B72DCA899C7D5889FF7721CEB2D&mode=splus&rnd=bEJ38g&base=AOSZ&n=5081238#2sej5ETY3DZGLB171>

³³ Третий кассационный суд общей юрисдикции. (2021). Кассационное определение от 24.06.2021 № 77-1411/2021. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=C10D4B31598CBB37FEAF6E5C8A378287&mode=splus&rnd=bEJ38g&base=KSOJ003&n=35963#Tfkj5ET46wqfhZ3J>

³⁴ Санкт-Петербургский городской суд. (2021). Апелляционное определение от 20.12.2021 по делу № 1-19/2021, 22-5752/2021. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=8BB30E68700B55EA5B0F59C18D4256C8&mode=splus&rnd=bEJ38g&base=AOSZ&n=4878364#kijv5ETBUjWxl0fD>

Находящийся на данный момент на доработке проект федерального закона «О цифровых валютах», разработанный Министерством финансов Российской Федерации, предусматривает легализацию криптовалютной сферы в Российской Федерации. Учитывая, что в условиях санкций криптовалюта является одним из наиболее быстрых, удобных и эффективных способов расчета, согласно данному законопроекту, планируется разрешить оплату внешнеторговой деятельности юридических лиц и предпринимателей за товары, работы, услуги и интеллектуальную деятельность с помощью цифровых валют. Законопроект также предусматривает введение лицензий оператора обмена цифровых валют и оператора цифровой платформы, т. е. в Российской Федерации появится возможность регистрации криптобирж и криптообменников. Однако в рамках законопроекта пока не определены санкции за нарушение предложенного порядка оборота криптовалют и противоправные действия его участников. В целом анализ указанного законопроекта позволяет утверждать, что процесс урегулирования оборота криптовалют в России будет схож с положениями законодательства о регулировании рынка ценных бумаг, т. е. установит достаточно жесткие требования и стандарты.

1.5.3. Правовая защита лиц, являющихся собственниками виртуальной валюты и виртуального имущества в Российской Федерации

К другим токенам оплаты относятся виртуальные валюты (Vandezande, 2017). Европейский центральный банк обозначил их как вид нерегулируемых, цифровых денег, которые выпускаются и обычно контролируются их разработчиками, а также используются и принимаются среди членов определенного виртуального сообщества³⁵. По сути, виртуальные валюты предназначены для использования в конкретных виртуальных сферах или мирах, таких как глобальные многопользовательские онлайн-игры³⁶.

Несмотря на то, что виртуальная валюта легально не подлежит обмену на фиатную валюту, практика показывает, что предметом посягательства при компьютерном мошенничестве, помимо безналичных и электронных денег, является именно виртуальная валюта (Савельев, 2014). Соответственно, вопрос урегулирования ее оборота на территории Российской Федерации позволит создать условия для правовой защиты лиц, являющихся собственниками такой валюты.

В судебной практике все чаще встречаются иски, напрямую связанные с массовыми многопользовательскими ролевыми онлайн-играми³⁷. Однако судебные решения по ним в Российской Федерации по большей части ограничиваются ссылкой

³⁵ European Central Bank. (2012, October). *Virtual Currency Schemes*. Report (p. 13). <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

³⁶ Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма. (2014, июнь). *Отчет ФАТФ «Виртуальные активы». Ключевые определения и потенциальные риски в сфере ПОД/ФТ*. https://eurasiangroup.org/files/FATF_docs/Virtualnye_valuty_FATF_2014.pdf

³⁷ Рожкова, М. А. (2020, 6 декабря). *Виртуальное имущество и многопользовательская онлайн-игра – как различать возникающие по их поводу отношения?* Закон.ру. https://zakon.ru/blog/2020/12/6/virtualnoe_imuschestvo_i_mnogopolzovatel'skaya_onlajn-igra__kak_razlichat_voznikayushchie_po_ih_povodu

на ст. 1062 ГК РФ и утверждают, что онлайн-игра является игрой, в силу определения и целей ее создания, которые указаны в Лицензионном соглашении, а значит, к ней подлежит применение ст. 1062 ГК РФ³⁸, согласно которой не подлежат судебной защите требования граждан и юридических лиц, связанные с организацией игр или пари и участия в них³⁹.

Однако встречаются судебные решения, которые рассматривают виртуальные валюты в рамках исков по защите прав потребителей. Так, Лефортовский районный суд г. Москвы признал, что внутриигровая валюта является единицей измерения объема прав использования дополнительного функционала компьютерной онлайн-игры, предоставленного пользователю путем отражения на внутриигровом лицевом счете аккаунта определенного количества единиц измерения прав игрока, которые могут приобретаться как за плату, так и без внесения денежных средств (начислением бесплатно в качестве бонуса за определенные активности в игре, например, участие во внутриигровом аукционе). Однако в этой связи начисленное количество «виртуальной валюты» на внутриигровой счет аккаунта не отражает движение реальных денежных средств между администрацией игры (ответчиком) и владельцем аккаунта⁴⁰.

Вопрос урегулирования оборота «виртуального имущества» стоит не менее остро, учитывая скорость коммерциализации рынка многопользовательских онлайн-игр. «Виртуальное имущество» в основе своей представляет собой всего лишь компьютерный код, который направлен преимущественно на имитацию объектов реального (физического) мира в цифровом пространстве. Исключительно виртуальная форма существования таких объектов не мешает осуществлять их обращение, которое затрагивает интересы реальных потребителей, поскольку процесс их приобретения и отчуждения основан на явно выраженной потребительской ценности (Русскевич и Фролов, 2020).

Все вышесказанное позволяет утверждать, что современный мир криптоактивов и децентрализованных финансов продолжает стремительно развиваться, характеризуясь богатым сочетанием инноваций, рисков (Almaqableh et al., 2022) и нормативных проблем. И именно унифицированные правовые подходы к регулированию оборота цифровых активов по всему миру способны указанные риски минимизировать.

³⁸ Четвертый кассационный суд общей юрисдикции. (2022). *Определение от 01.03.2022 по делу № 88-5695/2022*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXYahdpr&cacheid=F31C60CE0A5B986B5B1D27E2386915C6&mode=splus&rnd=bEJ38g&base=KSOJ004&n=72541#SKBk5ETF XI55CyV1>

³⁹ *Гражданский кодекс Российской Федерации (часть вторая)*. № 14-ФЗ. (1996). <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXYahdpr&cacheid=FCB3B26F22A203831458B5022A803D40&mode=splus&rnd=bEJ38g&base=LAW&n=377025&dst=102595#bCYc5ETs90x4mjl1>

⁴⁰ Лефортовский районный суд города Москвы. (2015). *Решение от 09.06.2015 по делу № 2-1619/2015-М-998/2015*. <https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXYahdpr&cacheid=17CCF72FEDE8E3A35215CEF4D7EAE3BF&mode=splus&rnd=bEJ38g&base=AOCN&n=4479817#B8Ok5ETUF 6RrfQ2j1>

2. Оценка рисков, возникающих в процессе оборота цифровых активов

С целью выработки глобальных правовых основ регулирования указанного рынка необходимо прежде всего оценить риски (He et al., 2022), которые возникают в процессе оборота цифровых активов. Понимание концепции риска цифровых активов может привести к эффективным результатам как для инвесторов, так и для регуляторов.

2.1. Риск волатильности

Стоимость цифровых активов подвержена высокой волатильности, т. е. их цена может как стремительно падать, так и расти в любой день, в том числе на внутрисдневной основе (Naeem et al., 2022). В этой связи инвестиции в цифровые активы считаются высокоспекулятивными инвестициями. Существует риск существенных или полных потерь при покупке или продаже цифровых активов (Shen et al., 2022). Рыночные цены могут существенно отличаться от справедливой стоимости компании или инвестиционной возможности в случае неликвидных/низколиквидных активов. Хотя волатильность цифровых активов так высока и значительно варьируется, она может увеличиваться, исходя из изменений и достижений в области технологий, мошенничества, краж и кибератак (Tsuchiya & Hiramoto, 2021; Caporale et al., 2021), от которых в условиях существующего правового нигилизма у пользователей нет достаточных средств правовой защиты. С другой стороны, резкие изменения в нормативно-правовом регулировании могут еще больше увеличить волатильность цифровых активов, повышая потенциал инвестиционных прибылей и потерь. Кроме того, цифровые активы не имеют исторического опыта других валют или товаров, таких как золото, по которому можно было бы определить, являются ли текущие уровни волатильности типичными или нетипичными.

2.2. Риск неправильной оценки

Порядок оценки токенов напрямую зависит от их вида. Так, цена платежных токенов зависит от динамики спроса и предложения на глобальном уровне и не опирается на традиционные методы оценки, используемые для ценных бумаг, что существенно затрудняет определение их объективной стоимости. Цифровые валюты существуют только виртуально в компьютерной сети и не имеют физического эквивалента, соответственно, установить их стоимость сложно, поскольку она зависит от ожиданий и доверия к тому, что они смогут быть использованы для будущих платежных операций. Проверенных методов оценки служебных токенов и вовсе не существует. Некоторые из выпускаемых служебных токенов не имеют внутренней ценности, кроме возможности использовать их для доступа или использования услуги/продукта, который будет разработан эмитентом. При этом нет никакой гарантии, что услуги/продукты будут успешно разработаны. Ситуация с оценкой инвестиционных токенов более понятна. Влияние на нее оказывают такие общеизвестные факторы, как анализ дисконтированных денежных потоков, премия за ликвидность или неликвидность в зависимости от срока существования компании и торговых площадок. Однако токены активов несут риски, связанные с базовой компанией или активом, поскольку многие компании, привлекающие средства, являются частными компаниями, не зарегистрированными на фондовом рынке.

2.3. Риск ликвидности

Рыночная капитализация индустрии криптоактивов в основном возглавляется биткоином, на долю которого приходится более 50 % общей рыночной капитализации (Wu et al., 2018). На рынке цифровых активов, отличных от биткоина, могут наблюдаться периоды снижения ликвидности или даже периоды неликвидности. Нет гарантии, что частная компания успешно проведет первичное публичное размещение акций или предоставит альтернативную стратегию выхода для инвестированного капитала. Относительно инвестиционных токенов риск ликвидности представляет собой вероятность, что компания не будет способна исполнять свои финансовые обязательства при наступлении срока их погашения. Приобретатель токенов активов может понести финансовые потери при их продаже в процессе обращения по ожидаемой цене, в том числе по причине отсутствия достаточного спроса или недостаточного объема операций, а также отсутствия репрезентативного рыночного уровня цен (Arsi et al., 2021).

2.4. Технологический риск

Технологии, связанные с цифровыми активами, находятся на ранней стадии развития. Соответственно, технологические достижения в области криптографии, взлома кодов, квантовых вычислений и т. д. могут представлять риск для безопасности цифровых активов. Кроме того, могут появиться альтернативные технологии, которые сделают некоторые цифровые активы менее актуальными или устаревшими. Функционирование цифровых активов основывается на программном обеспечении с открытым исходным кодом, в который в процессе программирования могут быть внесены ошибки. Также разработчики могут прекратить разработку программного обеспечения с открытым исходным кодом потенциально на критическом этапе, когда требуется обновление безопасности, в результате чего цифровые активы будут подвержены недостаткам и ошибкам программирования, также повысится риск мошенничества, краж и кибератак (Corbet et al., 2020). Некоторые сети цифровых активов за последние несколько лет пережили резкий рост числа транзакций. Увеличение количества транзакций в сочетании с неспособностью внедрить изменения в технологию цифровых активов может привести к замедлению времени обработки транзакций или значительному увеличению комиссий за транзакции с цифровыми активами, выплачиваемыми майнерам за облегчение их обработки.

2.5. Риск жесткого форка (hardfork)

Поскольку не существует центрального органа (например, центрального банка или правительственного агентства), контролирующего развитие технологий, связанных с цифровыми активами, функционирование цифровых активов и их дальнейшее совершенствование (например, возможность увеличить количество транзакций, сократить время обработки, уменьшить комиссию за транзакции, внедрить обновления безопасности) зависит от сотрудничества и консенсуса различных заинтересованных сторон, в том числе разработчиков, улучшающих программное обеспечение с открытым исходным кодом, связанное с цифровым активом, или майнеров,

облегчающих обработку транзакций. Любое разногласие между заинтересованными сторонами в форме внесения существенных изменений в код протокола блокчейн-проекта может привести к разделению сети цифровых активов на две или более несовместимые версии (Schär, 2020). В результате торговые площадки, на которых торгуются цифровые активы, могут приостановить возможность торговли определенной версией цифрового актива.

2.6. Криминальные риски, связанные с оборотом цифровых активов

Особые характеристики цифровых активов (например, они существуют только виртуально в компьютерной сети, операции с цифровыми активами необратимы и осуществляются анонимно) делают их привлекательной целью для мошенничества, краж и кибератак (Caporale et al., 2019). Существуют различные тактики для кражи цифровых активов или нарушения технологии цифровых активов («атака 51», когда противник может получить контроль над технологией цифровых активов, предоставив 51 % компьютерной мощности в сети цифровых активов, причем в настоящее время в мире не существует законов, прямо предусматривающих наказание за атаку на 51 % (Conklin et al., 2022); «атака на отказ в обслуживании» (Smurf Attack), когда злоумышленник пытается сделать ресурсы сети цифровых активов недоступными, перегружая ее запросами на обслуживание; Sybil-атаки, когда один человек пытается захватить одноранговую сеть, создав несколько учетных записей, узлов или компьютеров⁴¹; спуфинг-атака (подмена), когда мошенник выдает себя за какой-либо надежный источник; атаки вредоносных программ (Higbee, 2018)). Так, 8 октября 2022 г. Binance, крупнейшая в мире криптовалютная биржа, подтвердила, что в результате взлома управляемой ею блокчейн-сети были похищены криптовалюты на общую сумму 570 млн долларов США (Conklin et al., 2022). В последнее время широкое распространение получили случаи вымогательства криптовалют, связанные с кибератаками на объекты критической информационной инфраструктуры.

Существуют и иные возможные варианты реализации преступного поведения субъектов в сфере оборота цифровых активов. Чаще всего криптовалюты используются в целях легализации (отмывания) денежных средств или иного имущества, приобретенных лицом в результате совершения преступления, выступают предметом взятки. Однако из-за отсутствия должного правового регулирования в рассматриваемой области возможности привлечения к уголовной ответственности за подобные преступления ограничены.

Кроме того, цифровые активы подвержены более высокому, чем обычно, риску злоупотреблений на рынке, манипулирования рынком и инсайдерских сделок со стороны участников рынка в связи с имеющимися недостатками в регулировании, надзоре, контроле рынка и ликвидности.

⁴¹ Douceur, J. R. (2002). The Sybil attack. Lecture Notes in Computer Science. Conference: 1st International Workshop on Peer-to-Peer Systems, 2429, 251–260. https://www.researchgate.net/publication/299267832_The_Sybil_attack

2.7. Операционный риск

Транзакции базового уровня в DLT или другой распределенной бухгалтерской книге являются необратимыми и окончательными, а историю транзакций вычислительно невозможно изменить. Как следствие, если пользователь иницирует или запросит перевод цифровых активов, используя неверный адрес распределенной бухгалтерской книги, будет невозможно идентифицировать получателя и отменить дефектную транзакцию. Кроме того, существенные риски неправомерного использования информации возникают вследствие публичности действий в общедоступной распределенной бухгалтерской книге.

2.8. Кредитный риск и риск контрагента

В случае токенизированных ценных бумаг риск дефолта или банкротства базового эмитента является существенным в соответствии с частными инвестициями в акционерный капитал и/или частными долговыми инвестициями.

2.9. Специфические риски, связанные с хранением цифровых активов

Владение цифровым активом эквивалентно владению закрытым ключом (код, сопряженный с адресом блокчейна), который дает доступ к нему. Потеря или кража закрытого ключа, связанного с определенным адресом блокчейна, делает невозможной для владельца такого закрытого ключа идентификацию себя как законного владельца цифровых токенов, записанных на соответствующем адресе блокчейна.

2.10. Особые риски, связанные с токенизированными ценными бумагами, токенами ценных бумаг или ценными бумагами на основе DLT

Токенизированные ценные бумаги учитываются вне традиционной системы кастодианов, и их передача подвержена правовой неопределенности. Право собственности на токенизированные ценные бумаги определяется по записи цифровых токенов, связанных с этими ценными бумагами, в децентрализованной бухгалтерской книге, которую ведет сообщество пользователей. Технология блокчейн появилась недавно. Во многих юрисдикциях правовой и регулятивный режим, применимый в случае использования этой технологии в финансовом секторе, остается дискуссионным. Поэтому нельзя исключать споры относительно некоторых аспектов приобретения и передачи токенизированных ценных бумаг в форме цифровых токенов, таких как, например, действительность передачи. Традиционные рамки борьбы с отмыванием денег и финансированием терроризма не распространяются на токенизированные ценные бумаги. Размещение и хранение токенизированных ценных бумаг может осуществляться без привлечения профессиональных кастодианов, а посредством передачи цифровых токенов, записанных в децентрализованной бухгалтерской книге. Поэтому механизмы, обычно применяемые для предотвращения отмывания денег и финансирования терроризма, как правило, не применяются. Чтобы иметь возможность определить источник привлеченного капитала и избежать того, чтобы стать получателем средств незаконного происхождения, эмитент обычно полагается на стандарты по противодействию отмыванию денег (AML).

При этом реально существующие токенизированные активы с точки зрения оценки рисков намного позитивнее воспринимаются государствами, чем созданные непосредственно в распределенных реестрах, за счет большей безопасности при их обороте. Это подтверждается и мнением экспертов Базельского комитета по банковскому надзору, которые в июне 2021 г., призывая анализировать природу конкретного криптоактива при установлении значения риска, классифицировали их на три группы. Наименьшими рисками при этом обладают материальные и нематериальные активы группы 1а, включающей традиционные активы, отображенные в форме токенов⁴².

2.11. Правовые риски

До сих пор не найден международный консенсус по стандартам регулирования оборота цифровых активов. Существующее законодательство подвержено постоянным изменениям, которые могут повлечь за собой различную реакцию регулирующих или других государственных органов и повлиять на выпуск тех или иных цифровых активов, возможность торговли ими на внутреннем и международном рынках, а также на возможность передачи или конвертации цифровых активов, что потенциально увеличивает риск полной или частичной потери единиц или снижения их стоимости (включая снижение до нуля). По мере развития регулирования по всему миру существует также риск несоответствия регулирования в различных юрисдикциях, что может привести к признанию определенных операций законными в одной юрисдикции и незаконными в другой⁴³. На сегодняшний день все государства по принципу выбранного ими пути регулирования криптовалют можно было условно разделить на игнорирующие, одобряющие и запрещающие. Последних пока не так много, но среди них оказался Китай. Основной акцент данные государства делают на необходимость введения цифровой валюты центральных банков в своих юрисдикциях и обеспечения ее трансграничного оборота. Первая группа государств является наиболее многочисленной. Они избрали разные способы сосуществования с новыми финансовыми инструментами – это и режимы «песочниц», и частичная адаптация существующего законодательства под новые реалии, и введение собственной наиболее приемлемой для данных государств классификации токенов. В любом случае их позиция основана на четкой уверенности, что не стоит торопить события и принимать специальные нормативные правовые акты, направленные на регулирование криптовалют, пока в мире не выработаны какие-либо единые стандарты. И третья группа государств, признающая приоритет преимуществ криптовалют над рисками, связанными с их обращением, предполагающая неизбежность увеличения объемов рынка криптовалют и предпринимающая попытки признания за собой статуса мирового криптохаба.

⁴² The Bank for International Settlements. (2021, September 10). *Consultative Document of Basel Committee on Banking Supervision. Prudential Treatment of Cryptoasset Exposures*. <https://www.bis.org/bcbs/publ/d519.pdf>

⁴³ Choo, T., Hodgins, P., Bacon, L., Guang, Z. L., & Lester, A. (2022, September). *Managing digital asset and cryptocurrency risk*. Financier. Worldwide. <https://www.financierworldwide.com/managing-digital-asset-and-cryptocurrency-risk#.Y0su4y96BQI>

Проблемы, которые финансовые инновации ставят перед государственной политикой и нормативно-правовой базой в обеспечении финансовой стабильности, огромны, и их нельзя упускать из виду. Поэтому надзорный подход должен учитывать как преимущества, так и риски, сопровождающие финансовые инновации, а также адекватность мер регулирования. С точки зрения центральных банков, задача обеспечения финансовой стабильности остается важнейшей. В свете меняющегося финансового ландшафта можно сказать, что финансовая стабильность зависит от адекватности систем управления рисками и контроля участниками рынка, с одной стороны, и от надлежащих надзорных мер регулятора – с другой. Поэтому государству как регулятору необходимо взять на себя более активную роль, используя сочетание как предписывающего, так и ориентированного на рынок подходов.

Законодательное регулирование цифрового экономического пространства и обеспечение защиты информации и безопасности осуществления цифровых финансовых операций, а также совершенствование системы правового регулирования непосредственно цифровых активов позволят минимизировать экономические риски в финансовых системах государств.

Выводы

1. Цифровые активы, будучи новыми объектами имущественных экономических отношений, существующими в информационно-телекоммуникационной сети Интернет, являются на данный момент основным инструментом цифровой экономики, подверженным значительным рискам.

2. Цифровые активы – это последние технологические инновации, внедренные с помощью Blockchain и DLT, которые приводят к революции и новым парадигмальным изменениям в сфере финансовых услуг. Эта технология меняет способ управления и создания богатства, а также взаимодействие между пользователями и деньгами или финансовыми продуктами.

3. Отсутствие сильной и целостной нормативно-правовой базы для цифровых активов усиливает уязвимости цифровой экосистемы. Многие элементы экосистемы цифровых активов разработаны таким образом, чтобы избежать регулирования. Цифровые активы не вписываются в существующую нормативно-правовую базу. Кроме того, контролирующее влияние часто скрыто (например, в DeFi) или рассредоточено (например, валидаторы блокчейна). Регулирующим органам следует сосредоточиться на сути базового актива и связанных с ним прав, а не на его форме, если только форма не меняет существенную природу актива.

4. Критически важным условием развития цифровой экономики в России становится обеспечение уверенности всех экономических субъектов в своей защищенности в цифровом пространстве. Этого можно добиться в первую очередь за счет формирования и развития нормативно-правовой базы, обеспечивающей защиту прав участников оборота цифровых активов, реализации механизмов противодействия преступлениям в этой сфере.

5. Необходимо установить, каким образом цифровые активы и криптоактивы могут быть объектами права собственности в законодательстве соответствующих юрисдикций, будь то путем внесения поправок в общие положения или создания изолированного специального режима.

6. Для того чтобы понять, имеет ли (и каким образом) работа с цифровым токеном юридические последствия для прав в реальном мире, может потребоваться дальнейшее разъяснение со стороны национальных законодательств относительно юридического признания чисто цифровых объектов. В частности, можно ли признать нематериальное, цифровое представление объектом имущественных прав.

7. На сегодняшний день, учитывая риски, проанализированные в рамках данного исследования, представляется наиболее верной позиция той группы государств, которые избрали для себя некую «игнорирующую», даже скорее «выжидательную», позицию, когда они следят за развитием событий, стремятся умерить рынки криптовалют и минимизировать ущерб, подводя их под обычное финансовое регулирование, продолжая при этом специальное регулирование для борьбы с отмыванием денег и финансированием терроризма.

8. Разработка глобального правового регулирования оборота цифровых активов позволит избежать ситуаций, когда цифровой актив признается не подлежащим защите, и принудительного исполнения в той или иной юрисдикции, а также упростит задачу по выявлению и принудительному взысканию цифровых активов в случае установления факта совершения преступлений в их отношении или с их использованием.

Список литературы

- Рожкова, М. А. (2020). Значимые для целей правового регулирования различия между криптовалютой на базе публичного блокчейна, «криптовалютой» частного блокчейна и национальной криптовалютой. *Хозяйство и право*, 1, 3–12. <https://elibrary.ru/lyaknd>
- Русскевич, Е. А., Фролов, М. Д. (2020). *Мошенничество в сфере компьютерной информации*. Москва: ИНФРА-М. <https://elibrary.ru/ndwyzw>
- Савельев, А. И. (2014). *Электронная коммерция в России и за рубежом: правовое регулирование*. Москва: Статус. <https://elibrary.ru/uljdvz>
- Allen, J. G., Wells, H., & Mauer, M. (2022, August 1). Cryptoassets in Private Law: Emerging Trends and Open Questions from the First 10 Years. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4206250>
- Almaqableh, L., Reddy, K., Pereira, V., Ramiah, V., Wallace, D., & Francisco Veron, J. (2022). An investigative study of links between terrorist attacks and cryptocurrency markets. *Journal of Business Research*, 147, 177–188. <https://doi.org/10.1016/j.jbusres.2022.04.019>
- Arsi, S., Khelifa, S., Ghabri, Y., & Mzoughi, H. (2021). *Cryptocurrencies: Key Risks and Challenges*. https://doi.org/10.1142/9789811239670_0007
- Beck, R., & Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. *HICSS*. <https://doi.org/10.24251/HICSS.2017.653>
- Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2019). Non-Linearities, Cyber Attacks and Cryptocurrencies. *Finance Research Letters*. <https://doi.org/10.1016/j.frl.2019.09.012>
- Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2021). Cyber-attacks, spillovers and contagion in the cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money*, 101298. <https://doi.org/10.1016/j.intfin.2021.101298>
- Chandra, Y. (2022). Non-fungible token-enabled entrepreneurship: A conceptual framework. *Journal of Business Venturing Insights*, 18, e00323. <https://doi.org/10.1016/j.jbvi.2022.e00323>
- Chokor, A., & Alfieri, E. (2021). Long and short-term impacts of regulation in the cryptocurrency market. *The Quarterly Review of Economics and Finance*, 81, 157–173. <https://doi.org/10.1016/j.qref.2021.05.005>
- Conklin, M., Elzweig, B., & Trautman, L. J. (2022). Legal Recourse for Victims of Blockchain and Cyber Breach Attacks. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4251666>
- Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The destabilising effects of cryptocurrency cybercriminality. *Economics Letters*, 191, 108741. <https://doi.org/10.1016/j.econlet.2019.108741>
- Egloff, P., & Turnes, E. (2021). *A guide through Security Token Offerings (STO) Part 1: Key benefits*. <https://doi.org/10.13140/RG.2.2.14112.71685>

- Goforth, C. R. (2021). Regulation of Crypto: Who Is the Securities and Exchange Commission Protecting?. *American Business Law Journal*, 58(3), 643–705. <https://doi.org/10.1111/ablj.12192>
- González-Gallego, N., & Pérez-Cárceles, M. C. (2021). Cryptocurrencies and illicit practices: The role of governance. *Economic Analysis and Policy*, 72, 203–212. <https://doi.org/10.1016/j.eap.2021.08.003>
- He, J., Li, T., Li, B., Lan, X., Li, Z., & Wang, Y. (2021). An immune-based risk assessment method for digital virtual assets. *Computers & Security*, 102, 102134. <https://doi.org/10.1016/j.cose.2020.102134>
- Hendrickson, J. R., & Luther, W. J. (2021). Cash, crime, and cryptocurrencies. *The Quarterly Review of Economics and Finance*, 85, 200–207. <https://doi.org/10.1016/j.qref.2021.01.004>
- Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, 7, 13–15. [https://doi.org/10.1016/s1361-3723\(18\)30064-2](https://doi.org/10.1016/s1361-3723(18)30064-2)
- Hsieh, S.-F., & Brennan, G. (2022). Issues, risks, and challenges for auditing crypto asset transactions. *International Journal of Accounting Information Systems*, 46, 100569. <https://doi.org/10.1016/j.accinf.2022.100569>
- Hugo, I., & De Quenetai, S. (2022, September 25). *Managing Risk in DeFi Portfolios*. <http://dx.doi.org/10.2139/ssrn.4228899>
- Jackson, H. E. (1999, May 1). Regulation in a Multi-Sector Financial Services Industry: An Exploratory Essay. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.166651>
- Jensen, J. R., von Wachter, V., Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). *Complex Systems Informatics and Modeling Quarterly*, 26, 46–54. <https://doi.org/10.7250/csimq.2021-26.03>
- Kopaliani, A. (2022, September 10). The Digital Currency Revolution: A Cost-Benefit Analysis and Future Manifestations. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4215586>
- Mack, N. (2022, September). Obstacles to Successful Introduction of a U.S. Central Bank Digital Currency. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4213821>
- Mezei, P. (2022). Hop on the Roller Coaster – New Hopes for Digital Exhaustion?. *GRUR International*, 71(11), 1017–1018. <https://doi.org/10.1093/grurint/ikac111>
- Naeem, M. A., Lucey, B. M., Karim, S., & Ghafoor, A. (2022). Do financial volatilities mitigate the risk of cryptocurrency indexes? *Finance Research Letters*, 50, 103206. <https://doi.org/10.1016/j.frl.2022.103206>
- Orr, D. A. (2023). Cryptocurrency: Its Impact and Forensic Worth. *Encyclopedia of Forensic Sciences* (3rd Ed., pp. 709–716). <https://doi.org/10.1016/b978-0-12-823677-2.00073-8>
- Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, 6, 117–133. <https://doi.org/10.1007/s42786-022-00044-x>
- Remolina, N. (2022, October 10). Decentralized Finance: Implications of the So-Called Disintermediation of Financial Services. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4243544>
- Schär, F. (2020). Blockchain Forks: A Formal Classification Framework and Persistency Analysis. *Singapore Economic Review*, 101712, 1–22. <https://doi.org/10.1142/S0217590820470025>
- Shen, Y., Hu, W., & Zhang, Y. (2022). Digital Finance, Household Income and Household Risky Financial Asset Investment. *Procedia Computer Science*, 202, 244–251. <https://doi.org/10.1016/j.procs.2022.04.032>
- Tsuchiya, Y., & Hiramoto, N. (2021). How cryptocurrency is laundered: Case study of Coincheck hacking incident. *Forensic Science International: Reports*, 4, 100241. <https://doi.org/10.1016/j.fsir.2021.100241>
- Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review*, 33(3), 341–353. <https://doi.org/10.1016/j.clsr.2017.03.011>
- Wu, K., Wheatley, S., & Sornette, D. (2018). Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations. *Royal Society Open Science*, 5(9), 180381. <https://doi.org/10.1098/rsos.180381>
- Yadav, Y., & Brummer, C. (2019). Fintech and the Innovation Trilemma. *Georgetown Law Journal*, 107(2), 235.
- Zetsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2018, July 24). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.3072298>

Сведения об авторе



Мурадян Светлана Владимировна – кандидат юридических наук, заместитель начальника кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий, Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя

Адрес: 117437, Российская Федерация, г. Москва, ул. Академика Волгина, 12

E-mail: lanamuradyan@gmail.com

ORCID ID: <https://orcid.org/0000-0002-1366-5074>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/34838406>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57917943100>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=694064

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 14 ноября 2022 г.

Дата одобрения после рецензирования – 6 января 2023 г.

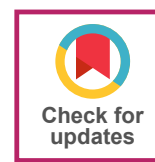
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.5>



Digital Assets: Legal Regulation and Estimation of Risks

Svetlana V. Muradyan 

Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
Moscow, Russian Federation

Keywords

Bitcoin,
blockchain,
cryptocurrency,
digital assets,
digital currency,
finance,
law,
regulation,
risk,
token

Abstract

Objective: to substantiate the need to create a universal mechanism of legal regulation of digital currencies and tokenized assets, based on a uniform categorization of digital assets and the author's interpretation of the conception of digital assets risk, in order to ensure their safe circulation with legal means and effective development of the global digital economy in the future.

Methods: the research was carried out with a combination of cognition techniques of various levels: from philosophical to private scientific; the key position among them belongs to a systemic approach, a comparative legal method and a formal-juridical analysis of normative materials.

Results: the present research lays the conceptual basis for building a global system of legal regulation of digital assets circulation and facilitates identifying and resolving the key issues, necessarily emerging in the analysis of the current mechanisms of legal regulation at national level and in the estimation of various types of digital assets.

Scientific novelty: consists in a comprehensive consideration of the essence and features of the legal nature of various types of digital assets, possessing, alongside with significant advantages, high risks from legal and financial viewpoints. Based on contradictory approaches and revealed gaps in the legal regulation of various types of digital assets, the author proposes a uniform categorization of digital assets, substantiates the concept of digital assets risk, attempts to substantiate the need to create a universal mechanism of legal regulation of digital currencies and tokenized assets, which would allow forming an effective system of means to protect property right to them and ensure safety of their circulation.

© Muradyan S. V., 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: is due to the current absence of a unified approach and a possibility to apply the existing legal norms in relation to innovative digital assets, taking into account their specificity, despite their trans-border character. The main provision and conclusions of the research can be used to improve the mechanisms of legal regulation of digital assets circulation.

For citation

Muradyan, S. V. (2023). Digital Assets: Legal Regulation and Estimation of Risks. *Journal of Digital Technologies and Law*, 1(1), 123–151. <https://doi.org/10.21202/jdtl.2023.5>

References

- Allen, J. G., Wells, H., & Mauer, M. (2022, August 1). Cryptoassets in Private Law: Emerging Trends and Open Questions from the First 10 Years. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4206250>
- Almaqableh, L., Reddy, K., Pereira, V., Ramiah, V., Wallace, D., & Francisco Veron, J. (2022). An investigative study of links between terrorist attacks and cryptocurrency markets. *Journal of Business Research*, 147, 177–188. <https://doi.org/10.1016/j.jbusres.2022.04.019>
- Arsi, S., Khelifa, S., Ghabri, Y., & Mzoughi, H. (2021). *Cryptocurrencies: Key Risks and Challenges*. https://doi.org/10.1142/9789811239670_0007
- Beck, R., & Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. *HICSS*. <https://doi.org/10.24251/HICSS.2017.653>
- Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2019). Non-Linearities, Cyber Attacks and Cryptocurrencies. *Finance Research Letters*. <https://doi.org/10.1016/j.frl.2019.09.012>
- Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2021). Cyber-attacks, spillovers and contagion in the cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money*, 101298. <https://doi.org/10.1016/j.intfin.2021.101298>
- Chandra, Y. (2022). Non-fungible token-enabled entrepreneurship: A conceptual framework. *Journal of Business Venturing Insights*, 18, e00323. <https://doi.org/10.1016/j.jbvi.2022.e00323>
- Chokor, A., & Alfieri, E. (2021). Long and short-term impacts of regulation in the cryptocurrency market. *The Quarterly Review of Economics and Finance*, 81, 157–173. <https://doi.org/10.1016/j.qref.2021.05.005>
- Conklin, M., Elzweig, B., & Trautman, L. J. (2022). Legal Recourse for Victims of Blockchain and Cyber Breach Attacks. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4251666>
- Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The destabilising effects of cryptocurrency cybercriminality. *Economics Letters*, 191, 108741. <https://doi.org/10.1016/j.econlet.2019.108741>
- Egloff, P., & Turnes, E. (2021). *A guide through Security Token Offerings (STO) Part 1: Key benefits*. <https://doi.org/10.13140/RG.2.2.14112.71685>
- Goforth, C. R. (2021). Regulation of Crypto: Who Is the Securities and Exchange Commission Protecting? *American Business Law Journal*, 58(3), 643–705. <https://doi.org/10.1111/ablj.12192>
- González-Gallego, N., & Pérez-Cárceles, M. C. (2021). Cryptocurrencies and illicit practices: The role of governance. *Economic Analysis and Policy*, 72, 203–212. <https://doi.org/10.1016/j.eap.2021.08.003>
- He, J., Li, T., Li, B., Lan, X., Li, Z., & Wang, Y. (2021). An immune-based risk assessment method for digital virtual assets. *Computers & Security*, 102, 102134. <https://doi.org/10.1016/j.cose.2020.102134>
- Hendrickson, J. R., & Luther, W. J. (2021). Cash, crime, and cryptocurrencies. *The Quarterly Review of Economics and Finance*, 85, 200–207. <https://doi.org/10.1016/j.qref.2021.01.004>
- Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, 7, 13–15. [https://doi.org/10.1016/s1361-3723\(18\)30064-2](https://doi.org/10.1016/s1361-3723(18)30064-2)
- Hsieh, S.-F., & Brennan, G. (2022). Issues, risks, and challenges for auditing crypto asset transactions. *International Journal of Accounting Information Systems*, 46, 100569. <https://doi.org/10.1016/j.accinf.2022.100569>
- Hugo, I., & De Quenetai, S. (2022, September 25). *Managing Risk in DeFi Portfolios*. <http://dx.doi.org/10.2139/ssrn.4228899>

- Jackson, H. E. (1999, May 1). Regulation in a Multi-Sector Financial Services Industry: An Exploratory Essay. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.166651>
- Jensen, J. R., V. von Wachter, & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). *Complex Systems Informatics and Modeling Quarterly*, 26, 46–54. <https://doi.org/10.7250/csimq.2021-26.03>
- Kopaliani, A. (2022, September 10). The Digital Currency Revolution: A Cost-Benefit Analysis and Future Manifestations. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4215586>
- Mack, N. (2022, September). Obstacles to Successful Introduction of a U.S. Central Bank Digital Currency. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4213821>
- Mezei, P. (2022). Hop on the Roller Coaster – New Hopes for Digital Exhaustion? *GRUR International*, 71(11), 1017–1018. <https://doi.org/10.1093/grurint/ikac111>
- Naeem, M. A., Lucey, B. M., Karim, S., & Ghafoor, A. (2022). Do financial volatilities mitigate the risk of cryptocurrency indexes? *Finance Research Letters*, 50, 103206. <https://doi.org/10.1016/j.frl.2022.103206>
- Orr, D. A. (2023). Cryptocurrency: Its Impact and Forensic Worth. In *Encyclopedia of Forensic Sciences* (3rd Ed., pp. 709–716). <https://doi.org/10.1016/b978-0-12-823677-2.00073-8>
- Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, 6, 117–133. <https://doi.org/10.1007/s42786-022-00044-x>
- Remolina, N. (2022, October 10). Decentralized Finance: Implications of the So-Called Disintermediation of Financial Services. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.4243544>
- Rozhkova, M. A. (2020). Differences between the cryptocurrency based on public blockchain, the “cryptocurrency” based on private blockchain, and national cryptocurrency, essential for the purposes of legal regulation. *Khozyaistvo i pravo*, 1, 3–12. (In Russ.).
- Russkevich, E. A., & Frolov, M. D. (2020). *Fraud in the sphere of computer information*. Moscow: INFRA-M. (In Russ.).
- Savel'ev, A. I. (2014). *Digital commerce in Russia and abroad: legal regulation*. Moscow: Status. (In Russ.).
- Schär, F. (2020). Blockchain Forks: A Formal Classification Framework and Persistency Analysis. *Singapore Economic Review*, 101712, 1–22. <https://doi.org/10.1142/S0217590820470025>
- Shen, Y., Hu, W., & Zhang, Y. (2022). Digital Finance, Household Income and Household Risky Financial Asset Investment. *Procedia Computer Science*, 202, 244–251. <https://doi.org/10.1016/j.procs.2022.04.032>
- Tsuchiya, Y., & Hiramoto, N. (2021). How cryptocurrency is laundered: Case study of Coincheck hacking incident. *Forensic Science International: Reports*, 4, 100241. <https://doi.org/10.1016/j.fsir.2021.100241>
- Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review*, 33(3), 341–353. <https://doi.org/10.1016/j.clsr.2017.03.011>
- Wu, K., Wheatley, S., & Sornette, D. (2018). Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations. *Royal Society Open Science*, 5(9), 180381. <https://doi.org/10.1098/rsos.180381>
- Yadav, Y., & Brummer, C. (2019). Fintech and the Innovation Trilemma. *Georgetown Law Journal*, 107(2), 235.
- Zetsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2018, July 24). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.3072298>

Author information



Svetlana V. Muradyan – PhD (Law), Deputy Head of the Department for Counteracting Crimes in the sphere of Information-communication Technologies, Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia

Address: 12 Akademika Volgina Str., 117437 Moscow, Russian Federation

E-mail: lanamuradyan@gmail.com

ORCID ID: <https://orcid.org/0000-0002-1366-5074>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/34838406>

ScopusAuthorID: <https://www.scopus.com/authid/detail.uri?authorId=57917943100>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=694064

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – November 14, 2022

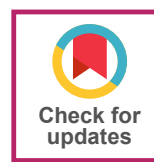
Date of approval – January 6, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 34:75:069:004
EDN: <https://elibrary.ru/jmlrdf>
DOI: <https://doi.org/10.21202/jdtl.2023.6>



Правовая природа воспроизведения музейных предметов в цифровой форме NFT

Вероника Дмитриевна Бурдова

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

Ключевые слова

NFT,
интеллектуальная
собственность,
искусство,
метавселенная,
музей,
право,
токен,
цифровые активы,
цифровые права,
цифровые технологии

Аннотация

Цель: посредством выявления правовой природы невзаимозаменяемого токена (NFT) предложение решения актуальных вопросов правового регулирования отношений, возникающих в сегменте онлайн-рынка и на интернет-площадках, связанных с воспроизведением и использованием в дальнейшем в виртуальной среде токенизированных цифровых копий оригинала произведений искусства.

Методы: в основе проведенного исследования находятся формально-юридический и сравнительно-правовой анализ, применяемые вместе со способами толкования права.

Результаты: сделан вывод о том, что воспроизведение музейного предмета в цифровой форме NFT не тождественно воспроизведению музейного предмета в простом цифровом формате, поскольку содержит в себе обязательные критерии в виде уникальности экземпляра, неделимости и дефицитности конкретного токена. NFT-объект выступает в качестве цифрового подлинника аналогового оригинала музейного предмета в цифровой среде и метавселенной, а не новой формы медиаискусства. Выраженный в форме сертификата уникальности цифрового объекта, NFT-объект по своей правовой природе и с целью правового регулирования сделок с ним относится к «иному имуществу» среди объектов гражданского права, что позволяет музеям использовать соответствующие договорные конструкции при структурировании таких сделок.

Научная новизна: предложен авторский подход к рассмотрению, совершенствованию правового регулирования, учета и хранения NFT-объектов в качестве виртуальных музейных предметов, так называемых цифровых эквивалентов вещей, обладающих признаками индивидуально-определенного характера и уникальности экземпляра, отличных от простых цифровых копий, цифровых произведений искусства, 3D mapping и др.

© Бурдова В. Д., 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: результаты проведенного исследования могут быть использованы для совершенствования правового регулирования музейной деятельности, корректировки гражданского и музейного законодательства, в частности, определения виртуальных музейных предметов; в процессе реализации права, например, при заключении сделок по использованию и продаже NFT-объектов в части уточнения содержания и объема полномочий правообладателей невзаимозаменяемого токена.

Для цитирования

Бурдова, В. Д. (2023). Правовая природа воспроизведения музейных предметов в цифровой форме NFT. *Journal of Digital Technologies and Law*, 1(1), 152–174. <https://doi.org/10.21202/jdtl.2023.6>

Содержание

Введение

1. Правовая природа NFT

2. Формирование правового регулирования NFT в музейной среде

3. Роль NFT в воспроизведении музейных предметов

4. Результаты исследования

Выводы

Список литературы

Введение

Прежде чем рассматривать роль музея в цифровой среде, необходимо обратиться непосредственно к определению понятия музея.

На внеочередной Генеральной ассамблее Международного совета музеев (International Council of Museums – ICOM) в 2022 г. открытым голосованием было принято новое определение понятия «музей» как некоммерческой постоянно действующей организации на службе обществу, которая исследует, собирает, сохраняет, интерпретирует и демонстрирует материальное и нематериальное наследие. Обладая признаками открытости, доступности и инклюзивности, музеи способствуют разнообразию и устойчивости¹.

Российский законодатель также относит музей к некоммерческому учреждению культуры, созданному собственником для хранения, изучения и публичного представления музейных предметов и музейных коллекций, включенных в состав Музейного фонда Российской Федерации, а также для достижения иных целей,

¹ Принято новое определение понятия музей. (2022, 26 августа). *The Art Newspaper Russia*. <https://www.theartnewspaper.ru/posts/20220826-jord/>

определенных законом². Таким образом, музей по своей сути является некоммерческой организацией, ориентированной в первую очередь на социокультурные цели.

Помимо законодательного наделения музеев специальными правами в области регулирования использования изображений музейных предметов, в рамках развития своей просветительско-образовательной деятельности, а также привлечения дополнительных источников дохода музей может популяризировать свою музейную коллекцию через цифровизацию музейных предметов.

Итогом такой цифровизации будет либо результат воспроизведения музейного предмета как объекта интеллектуальной собственности для коммерческого использования, либо токенизация цифрового произведения, которая сопровождается как простым воспроизведением изображения, так и созданием производного произведения в виде арт-объекта.

Основная задача музейной организации – сохранить культурную функцию и привлечь дополнительный источник дохода, установив баланс между своей миссией и запросами пользователей.

1. Правовая природа NFT

Музей выступает в роли собственника музейного предмета – культурной ценности, качество либо особые признаки которой делают необходимым для общества ее сохранение, изучение и публичное представление, устанавливая специальный правовой режим для таких объектов³, в том числе осуществляя их последующую токенизацию.

Токенизация представляет собой процесс перевода прав на материальные ценности в токены, т. е. создание цифровых аналогов реальных вещей для повышения защищенности данных объектов при их обращении в сегменте онлайн-рынка (Новоселова, 2017). Для оцифровки музейных предметов в силу особенностей индивидуально-определенного характера и уникальности экземпляра используются невзаимозаменяемые токены (Non-Fungible Token, NFT), хранящиеся в системе распределенного реестра. Такие токены обладают свойствами исключительности, дефицитности конкретного токена и неделимости⁴.

Существует мнение, что для регулирования отношений в виртуальном мире закон не является уже достаточно эффективным средством, его роль снижается (Залоило, Пашенцев, 2019). Вместе с тем определить правовую природу NFT, а также объем правомочий на такие объекты необходимо для единообразного регулирования правоотношений, эффективной правовой защиты и безопасного оборота.

На сегодняшний день в России отсутствует специальное правовое регулирование рынка NFT. Однако предпринимаются попытки законодательного регулирования. В данном случае цифровизация оказывает существенное воздействие на регулятор общественных отношений (Пашенцев, 2020), поскольку появление новых объектов способствует формированию нового правового поля и регулированию отношений

² О Музейном фонде Российской Федерации и музеях в Российской Федерации. № 54-ФЗ (1996). СПС «КонсультантПлюс». https://www.consultant.ru/document/cons_doc_LAW_10496/

³ Там же.

⁴ Non-fungible tokens (NFT). *ethereum.org*. <https://ethereum.org/en/nft/>

в нем между субъектами. Так, в Государственную Думу внесен на рассмотрение законопроект, где предлагают внести в ст. 1225 ГК РФ NFT в качестве результата интеллектуальной деятельности⁵.

Вместе с тем NFT представляет собой сертификат уникальности цифрового объекта, который состоит из кода и автоматически генерируется системой. Тем самым отсутствует творческий характер деятельности при его создании, что уже не отвечает установленным законом условиям охраноспособности (Рожкова, 2020). NFT рассматривается как техническое средство, позволяющее облечь объект интеллектуальной собственности в форму токена, состояние которого фиксируется в единственно возможной, неизменной форме (Долганин, 2021).

Возвращаясь к вопросу соотношения реального и виртуального искусства, первое сохраняет свою ценность при наличии определенной социокультурной миссии, художественной идеи, которая не будет противоречить установленным в обществе принципам культуры (Королева, 2018). Культурные права подлежат особой защите, поскольку имеют своей целью сохранение культурного наследия и общего культурного развития государства (Жуков, 2020). Цифровизация культуры позволяет открыть новые возможности для реализации творческих проектов (Андрейко, Мужжавлева, 2021), обеспечивает активное вовлечение музейных организаций нового поколения, ориентированных на цифровой формат восприятия информации.

Между тем в каждом правовом порядке в виртуальной эпохе сохраняется своя специфика в зависимости от национально-культурной идентичности (Гаврилова, 2021).

Затрагивая область развития общества в контексте взаимодействия и соотношения виртуальной реальности с реальным миром, NFT-объекты могут стать связующим звеном, способным переводить материальные объекты – реальные вещи в цифровые объекты, наделенные теми же ценностными характеристиками, что и аналоговые объекты. Однако в некотором роде имеющими большую долю сохранности.

Но что же такое сам NFT и какое место этот объект занимает в системе действующих правоотношений? На сегодняшний день NFT-объекты являются непоименованными объектами, которые законодательно не легализованы.

Так, Ю. В. Брисов, А. А. Победкин и другие исследователи считают возможным относить NFT к цифровому активу («иному имуществу»), основываясь на такой критерии NFT, как индивидуальная определенность (Брисов, Победкин, 2022), принимая во внимание в том числе правоподтверждающую функцию невзаимозаменяемого токена, его создание без участия операторов и без соблюдения требований законодательства о цифровых финансовых активах. Схожего мнения о возможности отнесения NFT к иному имуществу, но до принятия специального законодательства придерживаются в своей работе Д. С. Емельянов и И. С. Емельянов (Емельянов, Емельянов, 2021).

Другие авторы занимают иную позицию отнесения NFT к объектам интеллектуальной собственности, исходя из нематериальной природы таких объектов, к которым должны применяться положения ч. 4 ГК РФ⁶. NFT выступает в качестве

⁵ О внесении изменений в статью 1225 части четвертой Гражданского кодекса Российской Федерации (в части расширения перечня охраняемых результатов интеллектуальной деятельности в виде невзаимозаменяемых токенов). <https://sozd.duma.gov.ru/bill/126586-8>

⁶ Больше чем собственность: NFT пытаются вписать в российский закон. (2022, 21 мая). <https://iz.ru/1337541/ekaterina-korinenko/bolshe-chem-sobstvennost-nft-pytaiutsia-vpisat-v-rossiiskii-zakon>

программного кода, подпадающего под действие норм авторского права в качестве программы для ЭВМ.

Однако отнесение данных объектов к объектам авторского права противоречит их правовой природе, поскольку отсутствует творческий характер деятельности при создании токена. Е. Портман считает, что с точки зрения правовой природы NFT-токены сопоставимы с категорией цифровых прав⁷. По терминологическому смыслу слова и согласно закрепленным в ст. 128 ГК РФ объектам гражданского права можно было бы предположить, что NFT-объекты подпадают под категорию цифровых прав. Невзаимозаменяемый токен как сертификат уникальности цифрового объекта содержит в себе только URL-адрес, который показывает место его размещения в распределенном реестре. Тем самым NFT содержит в себе определенные метаданные, связывающие строчку кода в блокчейне с исходным файлом – предметом искусства.

Исходя из норм действующего законодательства цифровыми правами признаются обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей конкретным признакам⁸. Существует две разновидности цифровых прав: цифровые финансовые активы и утилитарные цифровые права.

Вместе с тем NFT нельзя относить к цифровым правам, поскольку основная функция невзаимозаменяемого токена – удостоверяющая. NFT – это цифровая запись, позволяющая связать цифровое произведение искусства, в нашем случае цифровую копию оригинала картины, с ее владельцем. Каждая транзакция, относящаяся к NFT и связанному с ним произведению искусства, хранится в реестре с помощью алгоритма Proof-of-Work (PoW) (англ. «доказательство работы»), что позволяет легко и надежно передавать цифровые активы и подтверждать право собственности на произведение искусства (Vasan et al., 2022).

Вопросы правовой природы NFT отражаются и в зарубежной судебной практике. Так, в Китае суд Ханчжоу признал NFT уникальными цифровыми активами, которые относятся к категории виртуальной собственности, т. е. обладают такими характеристиками, как цена, редкость, управляемость, контроль над цифровым активом (владение) и возможность торговли (распоряжение), и подлежат правовой защите как имущество⁹. Тем самым невзаимозаменяемые токены подпадают под определение собственности с приставкой «виртуальная», что практически не отличает их от традиционных объектов.

Неоднозначно мнение научного сообщества и о соотношении авторского и вещного права. Е. Авакян¹⁰ отмечает, что NFT – это удобный способ продавать в цифровой среде вещи, наделенные индивидуальными признаками, не добавляя новшеств институту интеллектуального права. Учитывая независимость интеллектуальных прав

⁷ Правовой статус NFT-токенов не определен. <https://www.kommersant.ru/doc/4869155>

⁸ Гражданский кодекс Российской Федерации, часть первая. СПС «КонсультантПлюс». <https://www.consultant.ru/>

⁹ Спор, связанный с транзакцией цифровой коллекции. <https://mp.weixin.qq.com/s/WWnZAxqilVJ-dHO90eoBVw>

¹⁰ Эрмитаж продает свою коллекцию в NFT. (2021, 20 августа). Vc.ru. <https://vc.ru/ipquorum/284386-ermitazh-prodaet-svoyu-kollekciyu-v-nft>

от права собственности на материальный носитель (вещь), в котором выражены соответствующие результаты интеллектуальной деятельности, М. А. Рожковой¹¹ была предложена концепция имущественных прав на новые нематериальные объекты, основная идея которой состоит в том, что приобретатель NFT получает не исключительные права, а иные имущественные права, аналогичные праву собственности на материальный носитель такого результата, размещенного на конкретной веб-странице (URL). Такая конструкция, на наш взгляд, представляется верной, поскольку, проводя аналогию с приобретением материального предмета, воплощающего в себе тот или иной результат интеллектуальной деятельности, покупателю автоматически не переходят исключительные права.

В зарубежной практике существует прецедент о разграничении прав на материальный носитель и на произведение, выраженное в нем. Так, коммерческий суд в Барселоне (Juzgado de lo Mercantil) рассмотрел спор между брендом одежды Mango и испанским коллективным обществом художников VEGAP (Visual Entidad de Gestión de Artistas Plásticos)¹². Суть спора заключалась в том, что бренд Mango создал одежду, используя произведения искусства. Общество художников подало в суд от имени художников за нарушение авторских прав, выразившихся в создании и демонстрации NFT. Позиция бренда состояла в том, что Mango реализует права собственника произведений, поскольку владеет материальными носителями, и не нарушает исключительных прав художников на переработку. Кроме того, воспроизведения произведений не было, поскольку NFT является иной формой произведений искусства. Однако суд встал на сторону общества художников, установив, что владение материальным носителем не приравнивается к наличию исключительных прав на выраженное в нем произведение. Тем самым можно сделать вывод, что NFT рассматривается как способ воспроизведения произведения в цифровой среде, а наличие прав на материальный носитель самого предмета, воплощающего произведение, не наделяет правообладателя исключительными правами на него.

В этой связи как российское законодательство, так и зарубежное на сегодняшний день не содержат в себе прямых правовых положений, позволяющих регулировать отношения субъектов по поводу обращения цифровых объектов, сертифицированных по стандартам NFT. Однако формирование практики происходит за счет договорных конструкций и судебных споров.

Невзаимозаменяемые токены обладают признаками уникальности и единичности конкретного цифрового объекта, неделимости и дефицитности, что существенно отличает их от цифровых финансовых активов и цифровой валюты, которые могут быть заменены в любой момент на подобные объекты. Таким образом, взаимозаменяемость, выраженная в возможности обмена одно на другое того же типа, является основным свойством валюты, цифровой валюты.

Сделки по приобретению и продаже NFT осуществляются на определенных интернет-площадках, называемых маркетплейсами. Эти платформы основывают свою работу на смарт-контрактах, закрепляющих соглашение между сторонами

¹¹ Рожкова М. А. (2021, 13 декабря). NFT – что это такое? / What is NFT (Non Fungible Tokens)? *Закон.ру*. https://zakon.ru/blog/2021/12/13/nft_что_это_такое_what_is_nft_non_fungible_tokens

¹² Решение коммерческого суда Барселоны. <https://www.poderjudicial.es/search/AN/openDocument/fb7c927281ec693aa0a8778d75e36f0d/20221121>

по поводу возникновения, изменения или прекращения тех или иных обязательств, условия которых записываются, исполняются и/или обеспечиваются компьютерным алгоритмом автоматически посредством осуществления программных операций (Григорьев и др., 2021).

При таких особенностях работы с NFT-объектами повышается уровень защищенности и прозрачности проводимых сделок с цифровыми предметами искусства, закрепленными в токен-оболочку. Поскольку записи хранятся в распределенном реестре, то подделка или копирование таких объектов сводится к минимуму. Неслучайно NFT-систему сегодня рассматривают не только в рамках продажи объектов цифрового искусства, но и в вопросах удостоверения иных прав (Dowling, 2022).

И если проблему подделывания можно решить посредством NFT, то проблема копирования объекта на сегодняшний день существует и решается возможностями искусственного интеллекта. Отсутствует не только законодательное регулирование, но и общая система по борьбе с созданием копий уникальных объектов. Речь идет не о копировании записи в блокчейне, а непосредственно цифрового объекта, выраженного в NFT. Поскольку, если мы говорим о продаже соответствующего токена, то происходит полная передача единственного цифрового кода с последующим внесением изменений в смарт-контракт, т. е. исключается возможность одновременно использования разными лицами, тогда как результат воспроизведения музейного предмета в простой цифровой форме для коммерческого использования, содержащийся в компьютерном файле, можно копировать и передавать неограниченное число раз, в том числе передавая электронный объект другим лицам, и не исключается возможность использования его самому. Тем самым стирается грань между единственно возможным правообладателем токена и другими лицами.

Таким образом, исходя из анализа приведенных позиций исследователей и судебной практики сформирован наш авторский взгляд на правовую природу NFT, который заключается в следующем.

NFT не относится к цифровым правам (цифровым финансовым активам, утилитарным цифровым правам) и цифровой валюте, поскольку обладает критериями уникальности и невзаимозаменяемости, а также правоподтверждающей функцией, а не платежной.

Наиболее оптимальной правовой конструкцией, на наш взгляд, учитывая особенность и отличительные характеристики таких объектов, будет применение норм, связанных с «иным имуществом», перечень которых на сегодняшний день является открытым и согласуется со ст. 128 ГК РФ в качестве цифровых активов, требующих специального законодательного регулирования, включающего распространение на них норм вещного права и налоговых норм в части продажи иного имущества в соответствии с гл. 23 Налогового кодекса РФ. В контексте музейного законодательства музейное имущество будет рассматриваться как виртуальный музейный предмет, на который будет распространяться право собственника – музея.

Что касается содержания правомочий правообладателя невзаимозаменяемого токена, то можно выделить основные права, которые возникают у приобретателя NFT: владения, пользования и распоряжения, что по своему содержанию также соотносится с обычными правами на имущество.

Проанализировав практику сделок с музейными предметами в формате NFT, можно выделить основной объем правомочий приобретателя таких объектов. Владение невзаимозаменяемым токеном выражается в фактическом обладании цифровым кодом с внесением соответствующих данных в смарт-контракт. Использование

объекта возможно в личных целях и посредством демонстрации, в том числе в коммерческих и некоммерческих целях, например, организовывать выставки в цифровом виде. Что касается распоряжения, то правообладатель имеет право перепродать NFT единственно возможному покупателю, поскольку происходит полная передача объекта без возможности его использования другими лицами. Для перехода к правообладателю исключительных прав на объект интеллектуальной собственности, в отношении которого был выпущен NFT, необходимо заключить договор об отчуждении исключительных прав или лицензионный договор, поскольку самого по себе факта приобретения NFT недостаточно.

2. Формирование правового регулирования NFT в музейной среде

Без проработки вопросов правового регулирования NFT сложно представить развитие музейного дела в метавселенной. Помимо определения правовой природы невзаимозаменяемых токенов, в которых выражены произведения искусства, необходимо разрешить вопросы учета и хранения музейных предметов в цифровой среде и т. д.

Согласно нормам музейного законодательства, отражение музейных предметов на балансе музея не допускается¹³. В бухгалтерском учете такие объекты отражаются за балансом.

На примере сделки по продаже NFT коллекции Эрмитажа, о которой будем говорить далее, следует отметить, что учет и хранение таких объектов распространяются как на простые результаты интеллектуальной деятельности без упоминания NFT-формата, которые были переданы на аппаратном кошельке – физическом электронном устройстве, которое использует генерацию случайных чисел для создания публичных и приватных ключей, хранящихся на самом устройстве без доступа в Интернет. Такой способ хранения обеспечивает безопасный доступ к виртуальной коллекции музея на блокчейн-платформе (Цыгулева, 2021).

Рассмотрение NFT коллекции как совокупность отдельных результатов интеллектуальной деятельности без указания цифрового формата позволило музею учитывать их в качестве нематериальных активов, подпадающих под критерии прогнозируемой экономической выгоды, полезного потенциала от использования и т. д.¹⁴ При этом выставленные на продажу NFT не были учтены как нематериальные активы. Авторское право на цифровые произведения при этом принадлежит Эрмитажу и является неотчуждаемым.

Интересна конструкция обладания исключительными правами на произведение, включающее результат воспроизведения музейного предмета, изображение которого находится в общественном достоянии. Однако такая схема не подойдет под токенизацию музейных предметов без создания новых арт-объектов. Эрмитаж выступил

¹³ О Музейном фонде Российской Федерации и музеях в Российской Федерации. № 54-ФЗ (1996). СПС «КонсультантПлюс». https://www.consultant.ru/document/cons_doc_LAW_10496/

¹⁴ Инструкция по применению Единого плана счетов бухгалтерского учета для органов государственной власти (государственных органов), органов местного самоуправления, органов управления государственными внебюджетными фондами, государственных академий наук, государственных (муниципальных) учреждений, утвержденной приказом Министерства финансов Российской Федерации от 1 декабря 2010 года № 157н7. <https://base.garant.ru/12180849/>

в качестве новатора, тогда как зарубежные музеи пошли по пути простой оцифровки коллекции из собрания музея в NFT-формат.

Кроме того, несмотря на упоминание формирования именно виртуальной коллекции музея, речь о рассмотрении ее в качестве музейных предметов не идет, что не позволяет в полной мере называть ее коллекцией, значение которой четко определено музейными нормами. Под музейной коллекцией понимается совокупность культурных ценностей, которые приобретают свойства музейного предмета, только будучи соединенными вместе в силу характера своего происхождения и других признаков.

Учитывая ранее предложенное определение NFT как иного имущества с распространением общих норм гражданского законодательства, видится необходимым установить специальные нормы музейного законодательства в части рассмотрения таких объектов как виртуальных музейных предметов без отражения их на балансе учреждения и учтенных, например, в экспериментальном фонде музея. В таком фонде в настоящий момент могут находиться музейные предметы, выполненные в оригинальных современных техниках с применением компьютерных и иных технологий, которые в дальнейшем могут быть переведены в основной фонд музея¹⁵.

Тем самым такие объекты будут подпадать под определение музейной коллекции, обеспечивать хранение которой можно по аналогии с хранением токенов Эрмитажем. На сегодняшний день вопросы хранения цифровых музейных предметов решены путем размещения файлов в специально организованном защищенном электронном архиве – цифровом репозитории. Необходимо лишь внести соответствующее уточнение и разграничение понятий «виртуальный» и «цифровой музейный предмет», который уже упоминается в законодательстве.

3. Роль NFT в воспроизведении музейных предметов

В ситуации с включением музейных организаций в цифровизацию своей коллекции в NFT имеется, помимо единственно возможного приобретателя токенизированной цифровой копии оригинала картины или созданного производного арт-объекта, еще и сам музей, выступающий в роли так называемого генерального правообладателя на результат воспроизведения соответствующего музейного предмета и использования его в дальнейшем. Продажа цифровой копии оригинала в NFT-формате не лишает музейную организацию возможности создавать на базе данного произведения и другие токенизированные объекты, представляющие также уникальные объекты цифрового искусства в виде арт-проектов.

Музеи активно включаются в цифровизацию своей коллекции, выпускают цифровые открытки, организуют выставки, сопровождаемые продажей цифровых шедевров искусства в неограниченном количестве. Однако существует позиция, что с развитием и масштабированием виртуального пространства выпуск музеями NFT-объектов может привести в дальнейшем к потере цифровой копии оригинала картины из собрания музея безвозвратно, называя это термином «цифровой деакцессией»¹⁶. И это, действительно, может быть правдой, поскольку NFT выступает

¹⁵ Приказ Минкультуры России № 827 от 23.07.2020. <https://docs.cntd.ru/document/542672925>

¹⁶ Art Analytics. <https://www.artnome.com/art-analytics>

в качестве цифрового подлинника аналогового оригинала картины, это не новая форма цифрового искусства, а способ цифровой фиксации.

Благодаря оцифровке активов на основе NFT активы в реальном мире могут быть сопоставлены с блокчейном и обеспечивать циркуляцию и оценку стоимости в цифровом мире (Wang et al., 2021). Все происходящие процессы начинаются и завершаются в системе распределенного реестра в соответствии со смарт-контрактом, который осуществляет свою работу автоматически, обеспечивая при этом прозрачность сделок по передаче NFT объектов, их безопасность и определенность во избежание возможных рисков, связанных с человеческим фактором. Однако не исключаются проблемы с идентификацией лиц и потерей доступа к системе блокчейн.

Сейчас мы наблюдаем ситуацию, когда искусство рождает новый вид – медиаискусство (Савчук, 2017). В вопросах определения правовой природы NFT важно учитывать точное определение данного понятия, поскольку в цифровом пространстве имеются и другие цифровые объекты, например, DAW (Digital Art Work – цифровое произведение искусства) – запатентованная технология, защищающая цифровую копию оригинала картины от копирования, подделки и кражи по последнему слову криптографии, что очень близко по смысловому содержанию с NFT¹⁷.

DAW относится к области медиаискусства, где используются информационные (компьютерные) технологии, в результате которых реализуется воспроизведение музейных предметов в цифровой форме. Они по своей правовой природе приближены к простым цифровым копиям оригиналов произведений, выраженным в электронном формате, но не в децентрализованной системе. Сюда можно отнести обычную оцифровку или сканирование произведения, а также произведения искусства, которые были модифицированы с помощью компьютерных средств.

Говоря о различиях NFT и DAW, можно привести пример недавней выставки в лондонской галерее Unit, где были оцифрованы с помощью определенной технологии зашифрованных цифровых произведений искусства, разработанной компанией Cinello, и проданы факсимильные копии известных шедевров таких художников, как Модильяни «Голова молодой девушки», Леонардо да Винчи «Женщина с распущенными волосами» и «Портрет музыканта», Караваджо «Корзина с фруктами», Рафаэль Санти «Мадонна со щеглом», Франческо Хайес «Поцелуй».

Приобретатель такого цифрового произведения, в отличие от приобретателя NFT, где передается уникальный цифровой код, получил материальные носители: экран, встроенный накопитель, который генерирует изображение, реплику оригинальной рамы и сертификат подлинности. Кроме того, он получил непосредственно криптографический сертификат – NFT и логин для входа в приложение для регистрации себя в качестве владельца¹⁸. Представляется, что объекты DAW имеют своей целью скорее эстетическую функцию, поскольку акцент, прежде всего, идет на материальность шедевра искусства.

Однако цифровое искусство использует не только электронные технологии, но и формирует определенный цифровой продукт, например, векторное изображение,

¹⁷ Музеи обожглись на NFT – в Италии приостановили производство криптокопий шедевров. (2022). *The Art Newspaper Russia*. <https://www.theartnewspaper.ru/posts/20220927-pxvc/>

¹⁸ Картины Рафаэля, Микеланджело, Леонардо да Винчи продадут в виде NFT. <https://rossaprimavera.ru/news/89544ec6>

компиляции в программе Adobe Photoshop, виртуальное пространство или NFT, и это лишь некоторые из них¹⁹.

Музеи активно используют и иные формы Digital art (англ. «цифровое искусство») в зависимости от своей концептуальной составляющей, и способы экспонирования воспроизведения музейных предметов в цифровой среде могут быть различными: от классического digital-art до NFT-объекта, подтвержденного системой блокчейн, обладающего ценностным качеством и определяющей стоимостью, который не может быть видоизменен, или, например, NFT-голограмм.

Некоторые музеи применяют мультимедийные способы показа своей коллекции или коллекции других музеев мира, т. е. воспроизведение музейных предметов в формате так называемых иммерсивных выставок художников, которые сопровождаются показом шедевров искусства на больших экранах в движущемся формате. Например, выставки «Босх. Ожившие видения», «Ван Гог. Ожившие полотна» и другие, что позволяет существенно усилить эффективность восприятия и разглядеть мельчайшие детали аналоговых произведений.

Также музеи используют иной формат показа, например видеомэппинг (англ. video – «видео» и mapping – «отражение, проецирование»), при помощи которого можно выставлять музейные предметы, которые не могут быть представлены на выставке в силу реставрации экспоната или же передачи произведения на выставку в другую музейную институцию. Так же, как в иммерсивных выставках невидимые детали картин можно увеличить в разы при помощи программного обеспечения, создающего реальную среду, с передачей изображения на проекцию. Помимо этого, музеями 3D mapping (англ. «проецирование») «активно используется для оживления экспозиций, для демонстраций видео, которые позволяют переместиться в другую эпоху»²⁰. Но здесь может зарождаться проблема отказа художественных музеев от реальных выставок в пользу виртуальных, и важно соблюдать баланс и помнить, прежде всего, о социокультурной миссии музея, направленной на вовлечение аудитории в культурную жизнь, представление музейных предметов и передачу знаний последующему поколению.

Возвращаясь к вопросу NFT, на сегодняшний день данный объект может иметь потенциал в области интеллектуальной собственности за счет свойства невзаимозаменяемости и уникальности, которые позволяют сохранять и не видоизменять информацию об авторах, провенансе произведения, приобретателях и т. д. Исследования в области NFT сильно сосредоточены на технических аспектах в области регулирования авторских прав (Nadini et al., 2021).

Существует мнение, что в юрисдикциях, где авторское право подлежит регистрации, невзаимозаменяемые токены за счет специфических особенностей, выраженных в обеспечении уникальности объектов, заключенных в цифровую форму, помогают ускорить процессы охраны и гарантировать защиту прав на интеллектуальную собственность (Bamakan et al., 2022). То есть до тех пор, пока объект не будет

¹⁹ A Short History of Digital Art: Between New Technologies & Innovative Artistic Practices. <https://magazine.artland.com/digital-art/>

²⁰ Сферы применения и стоимость видеомэппинга. Программное обеспечение POGUMAX Designer. <https://pogumax.ru/sfery-primeneniya-videomappinga-i-ego-stoimost>

официально зарегистрирован в соответствующих органах, обеспечить предохрану такого объекта в виртуальной среде по аналогии с депонированием.

На наш взгляд, как и в ситуации с депонированием, такая предохрана не может гарантировать защиту прав на результат интеллектуальной деятельности, поскольку выражается лишь в фиксации даты, а не подтверждении авторства.

На сегодняшний день отсутствие прямых запретов позволяет музеям на правах собственника совершать подобные сделки с цифровыми произведениями искусства в рамках договорных конструкций. Так, одним из первых музеев, который выпустил токен цифровой копии шедевра искусства на продажу, стала флорентийская галерея Уффици. Картина Микеланджело «Мадонна Дони» была продана в форме NFT за \$170 тысяч²¹. Это свидетельствует о том, что NFT, воплощающие музейные предметы, оцениваются достаточно высоко. Такое искусство способно удовлетворять потребность тратить и инвестировать.

На 14 февраля 2022 г. Венская галерея «Бельведер» анонсировала дроп NFT картины Густава Климта «Поцелуй», которую разбили на 10 000 токенизированных фрагментов. Покупатель стал обладателем случайного фрагмента картины с возможностью регистрации себя на сайте как его владельца²².

Произведения искусства, которые обладают особым историческим, художественным, научным или культурным значением и включены в Музейный фонд, подлежат специальному регулированию в рамках музейного законодательства. Такие предметы сами по себе не являются объектами интеллектуальной собственности, но результаты их воспроизведения могут выступать в качестве самостоятельных объектов. При этом сам NFT не является объектом интеллектуальной собственности, это техническая форма, в которой выражено цифровое произведение, в данном случае результат цифрового воспроизведения музейного предмета или производное цифровое произведение на базе оригинала произведения. NFT лишь подтверждает право на обладание уникальной версией цифрового актива.

Первая и на сегодняшний день единственная в России сделка по токенизации картин из коллекции музея проведена Государственным Эрмитажем в 2021 г. Лимитированная серия NFT-изображений пяти произведений искусства: «Уголок сада в Монжероне» Клода Моне, «Композиция VI» Василия Кандинского, «Мадонна Литта» Леонардо да Винчи, «Куст сирени» Винсента Ван Гога и «Юдифь» Джорджоне – была продана на открытом аукционе Binance²³. Это была своего рода коллекция NFT, содержащая цифровые элементы и обладающая общими чертами (Mekacher et al., 2022). При этом цена на произведение из коллекции колебалась в диапазоне, определяющем его репутацию.

Следствием проведения выставки-продажи виртуальных музейных предметов явилась невозможность игнорировать мировые события. Музей выступил

²¹ В Италии цифровую копию картины Микеланджело «Мадонна Дони» продали за \$170 тысяч. (2021, 18 мая). *Правила жизни*. <https://www.pravilamag.ru/news/culture-and-entertainment/18-05-2021/262503-v-italii-cifrovuyu-kopiyu-kartiny-mikelandzhelo-madonna-doni-prodali-za-170-tysyach/>

²² «Поцелуй» Климта в NFT и обнаженная девушка Фрейда на аукционе: новости арт-рынка (2022, 2 февраля). *Forbes*. <https://www.forbes.ru/forbeslife/454311-poceluj-klimta-v-nft-i-obnazennaa-devuska-frejda-na-aukcione-novosti-art-rynka>

²³ Partz, H. (2021, September 7). Russian State Hermitage raises \$440K via Binance NFT auction. *Cointelegraph*. <https://cointelegraph.com/news/russian-state-hermitage-raises-440k-via-binance-nft-auction>

в качестве консервативного инноватора, использующего новейшие технологии, при помощи которых расширяются цифровые возможности знакомства с Эрмитажем (Цыгулева, 2021). Однако в отличие от европейского опыта выпуска токенов в формате простых цифровых копий картин российский музей пошел по пути создания нового формата культурных проектов в виде памятного продукта²⁴.

С точки зрения права данная ситуация подпадает под действие норм музейного законодательства по использованию работ из коллекции музея, а именно нормы ст. 36 Федерального закона от 26.05.1996 № 54-ФЗ «О Музейном фонде Российской Федерации и музеях в Российской Федерации», в соответствии с которой использование музейных работ в коммерческих целях осуществляется в порядке, установленном собственником, т. е. государством, и что речь идет об оригиналах работ, которые уже являются общественным достоянием. Тогда как создание токена – это создание самостоятельного объекта интеллектуальной собственности (Брисов, Победкин, 2022).

Вместе с тем стоит отметить, что положения данной статьи распространяют свое действие на использование не оригиналов музейных предметов как таковых, а их изображений. Речь идет о передаче прав на использование в коммерческих целях воспроизведений музейных предметов и музейных коллекций, включенных в состав Музейного фонда Российской Федерации и находящихся в музеях Российской Федерации²⁵.

Норма статьи закрепляет понятие использования изображений, а потому утверждение о том, что токены создавались на основе оригиналов произведений, коммерческое использование которых никем не осуществлялось и они по-прежнему доступны в Эрмитаже, не совсем верная правовая конструкция. Воспроизведение музейных предметов было осуществлено в рамках делегирования законодателем специфических полномочий музею по воспроизведению музейных предметов, результатом которого явилось создание цифровых версий произведений искусства.

Получается, что на один материальный объект – аналоговую картину, которая находится в общественном достоянии, распространяется право собственника картины, т. е. непосредственно музея. Затем результат воспроизведения картины как квазиобъект интеллектуальной собственности (Бурдова, 2022), выраженный в форме цифрового оригинала картины, токенизированной в NFT, либо передается по лицензионному договору третьим лицам, либо отчуждается в пользу третьих лиц. В данном случае результат воспроизведения уже является автономным объектом интеллектуальной собственности, а приставка «квази» указывает на то, что такой объект не перечислен среди результатов интеллектуальной деятельности, но по своей правовой природе содержит признаки, в том числе в части предоставления правовой охраны на произведение, перешедшее в общественное достояние, при отсутствии творческого вклада музея на его создание, однако по объему и форме использования совпадающее с исключительными правами на произведение.

²⁴ Moscow Digital School про блокчейн законодательство в России и Европе, криптообменники, NFT и налогообложение (2021, 25 октября). YouTube – видеохостинг. URL: <https://www.youtube.com/watch?v=dNgBssJss1g>

²⁵ О Музейном фонде Российской Федерации и музеях в Российской Федерации. № 54-ФЗ (1996). СПС «КонсультантПлюс». https://www.consultant.ru/document/cons_doc_LAW_10496/

При этом создание невзаимозаменяемого токена не является тождественным созданию цифровой копии объекта гражданского оборота, которая также является результатом воспроизведения музейного предмета. Однако в случае с Государственным Эрмитажем конструкция была усложнена. Сделка была проведена в несколько этапов, где на первом этапе музей оцифровал оригинал картины посредством фотографии. Получилось два объекта интеллектуальной собственности: результат воспроизведения произведения искусства (квазиобъект интеллектуальной собственности) и фотография (объект авторского права), исключительные права на которую были переданы Эрмитажу по договору об отчуждении исключительных прав.

На данном этапе на распечатанную фотографию (репродукцию) была нанесена подпись директора Эрмитажа М. Б. Пиотровского, что явилось созданием служебного произведения, права на которое перешли к музею. Итоговым результатом стала цифровая картина с авторской подписью директора Эрмитажа. Промежуточные результаты были уничтожены.

Непосредственно на втором этапе данный цифровой результат был токенизирован в цифровую форму NFT, или, как его еще называют, цифровой эквивалент вещи, который является подтверждением прав на обладание соответствующим цифровым активом с определенным набором исключительных прав на произведение.

Таким образом, образовались арт-объекты, включающие в себя три файла: репродукцию с подписью директора, видеоролик, в котором М. Б. Пиотровский, сопровождая рассказом о произведении, подписывает работу и удостоверяющую криптографическую подпись²⁶.

Музейная организация создала определенную культурную концепцию, привнесла авторский вклад, поскольку не остановилась на создании простых цифровых копий картин. NFT содержит информацию оригинала картины, которая имеет ценность и существует в физической форме (Кулакова, 2022), но Эрмитаж ушел от последующих возможных претензий по отчуждению цифрового оригинала аналоговой картины, оставив один экземпляр NFT от каждого произведения искусства в собственной музейной коллекции, что послужило началу ее формирования.

Покупатели NFT-коллекции на основании лицензии получили «право наслаждения», т. е. владения уникальным цифровым объектом, демонстрации и перепродажи²⁷. И, конечно, чувство принадлежности к коллекционному и редкому экземпляру.

Тем самым, отчуждая NFT, Эрмитаж передал соответствующий цифровой криптографический сертификат, но не исключительные права на произведение, выраженное в NFT. Кроме того, музей на базе данных работ может производить и другие произведения.

Мнения в научных кругах относительно совершенной сделки сводятся в большей степени к определению правовой природы выставленных на продажу объектов, в том числе являются ли они простым воспроизведением музейного предмета или новым арт-объектом. К. А. Суворова, О. В. Жевняк делают вывод, что возникает новый, хоть и вторичный объект интеллектуальной собственности в виде NFT, и автором

²⁶ Эрмитаж продает свою коллекцию в NFT (2021, 20 августа). Vc.ru. <https://vc.ru/ipquorum/284386-ermitazh-prodaet-svoyu-kollekciyu-v-nft>

²⁷ Binance. *NFT Marketplace Terms and Conditions*. (2021). https://public.nftstatic.com/static/nft/res/aded11f38a4042fc97d8607d204e17aa.pdf?fbclid=IwAR2CvcXfkru9kKpx7Vq_FJyXp1VLzslEuv5BeXVqVt2Ws7FrO4ZVEu365oY

данной работы является сам Государственный Эрмитаж (Суворова, Жевняк, 2022). А. Кузнецова высказывает позицию создания производных произведений с нанесением авторского автографа²⁸.

На наш взгляд, учитывая тот факт, что используются результаты воспроизведения музейных предметов и на базе их создаются произведения, можно сказать также о создании именно производных произведений, где первоначальным самостоятельным квазиобъектом интеллектуальной собственности выступает простой результат воспроизведения музейного предмета.

Здесь нами предложена определенная правовая конструкция. В музее находится аналоговая картина – оригинал, тесно связанный с материальным носителем. Собственником самого предмета искусства является музей, осуществляющий оцифровку произведения, исключительные права на которое истекли и оно перешло в общественное достояние, т. е. воспроизводящий музейный предмет. Затем результат такого воспроизведения – квазиобъект интеллектуальной собственности, права на который возникли у музея, – токенизируют в NFT-формат. Появляется новый арт-объект, подпадающий под определение объекта авторского права, поскольку создается творческим трудом и выражается в объективной форме.

В дальнейшем при необходимости использования в коммерческой деятельности изображения картины приобретатель обязан запрашивать согласие музея на его дальнейшее использование согласно нормам о музейной оговорке, в соответствии с которой произведения, перешедшие в общественное достояние и находящиеся в музейном фонде, могут воспроизводиться с согласия дирекции музея, в котором такие произведения находятся.

В этой связи крайне спорной видится позиция Д. Озеркова²⁹, заведующего отделом современного искусства Эрмитажа, о том, что продажа цифрового оригинала картины привела бы к невозможности музеем, владеющим самой картиной, ее дальнейшего копирования, который забыл о специальном музейном законодательстве, устанавливающем особенности воспроизведения музейных предметов и музейных коллекций. Следуя такой логике, мировые музеи уже лишились части своей цифровой коллекции.

Также требования музейного законодательства распространяются не только на музейные предметы, но и на объекты, находящиеся на территории музея, внешний и внутренний виды здания музея. Так, между Государственным Эрмитажем и Тиллем Линдемманном (лидером группы Rammstein) был заключен лицензионный договор на использование интерьеров Эрмитажа в клипе «Любимый город». Вместе с тем исполнитель расширил объем предоставленных ему по договору прав, разместив на маркетплейсе NFT, включающие цифровые изображения интерьеров музея. Эрмитаж направил претензию о прекращении нарушений, поскольку в договоре не было оговорено условие о производстве фотосъемки предметов из собрания и интерьеров музея, их последующей токенизации в формате NFT и продаже. Позже конфликт был урегулирован, и маркетплейсу Twelve X Twelve предоставили право использования интерьеров в цифровой форме в рамках проекта NFtill на возмездной основе³⁰.

²⁸ Эрмитаж продает свою коллекцию в NFT. (2021, 20 августа). Vc.ru. <https://vc.ru/ipquorum/284386-ermitazh-prodaet-svoyu-kollekciyu-v-nft>

²⁹ О чем говорит токен. Что такое NFT от Эрмитажа? <https://spbvedomosti.ru/news/culture/o-chem-govorit-token-chto-takoe-nft-ot-ermitazha/>

³⁰ Конфликт между Эрмитажем и Линдемманном разрешился без участия артиста. (2021, сентябрь). Фонтанка.ру. <https://www.fontanka.ru/2021/09/06/70120475/>

Таким образом, помимо воспроизведения музейных предметов, в формат NFT переносят в виртуальную реальность и внутренние интерьеры музея. Представляется, что с развитием цифровизации в NFT-формат будут переведены также изображения зданий музеев, объектов, расположенных на их территории, и символики, в том числе товарные знаки музейных организаций.

Факт создания музеями NFT и формирования виртуальной музейной коллекции ведет как к позитивным, так и негативным последствиям. К позитивному опыту можно отнести возможность увеличения количества посетителей «из дома», приобщение более молодого поколения к искусству, неподдельность и уникальность экземпляров, рассмотрение картин в мельчайших подробностях, упрощение отслеживания нарушений с помощью технологий совпадений, сохранность и отсутствие амортизации объектов, экономия на реставрациях, возможность в любой момент иметь доступ.

К негативным, на наш взгляд, следует отнести уход от традиционных форм существования музея, что может негативно сказаться на старшем поколении, навязывание цифровизации, возможная потеря доступа к произведениям из-за технических сбоев, неприменимость института свободного использования цифровых произведений.

Однако со всей очевидностью можно сделать вывод о том, что рынок NFT и цифрового искусства будет развиваться, поскольку уже сейчас создаются полноценные отделы по цифровому искусству, музеи начинают формировать виртуальные коллекции, что уже говорит об отсутствии единичности проведения сделок, организуются виртуальные выставки с применением QR-кодов, передаются права на цифровые копии на площадках Google, развивается законодательство. Музеи находятся на пороге Web 3.0.

4. Результаты исследования

1. Включение музеев в процесс цифровизации.

Проведенный анализ демонстрирует, что в настоящий момент музейные организации активно включаются в процесс цифровизации посредством создания невзаимозаменяемых токенов цифровых результатов воспроизведения музейных предметов и коллекций.

1.1. Правовое регулирование NFT.

Несмотря на отсутствие в России специального правового регулирования NFT, музеи прибегают к использованию договорных конструкций, позволяющих структурировать такие сделки.

Воспроизведение музейного предмета в цифровой форме NFT не является тождественным воспроизведению музейного предмета в простом цифровом формате, поскольку содержит в себе обязательные критерии в виде уникальности экземпляра, неделимости и дефицитности конкретного токена.

1.1.1. Правовая природа воспроизведения музейного предмета в NFT.

Сам по себе NFT не является объектом интеллектуальной собственности, но результат цифрового воспроизведения музейного предмета может быть рассмотрен в рамках законодательства в сфере интеллектуальной собственности. NFT-объект, выраженный в форме сертификата уникальности цифрового объекта, по правовой природе и с целью правового регулирования сделок с ним можно отнести к «иному имуществу» объектов гражданского права.

2. Содержание правомочий правообладателя NFT.

2.1. Можно выделить основные права, которые возникают у приобретателя NFT: владения, пользования и распоряжения, что по своему содержанию также соотносится с обычными правами на имущество.

2.1.1. Владение невзаимозаменяемым токеном выражается в фактическом обладании цифровым кодом с внесением соответствующих данных в смарт-контракт. Использование объекта возможно в личных целях и посредством демонстрации, в том числе в коммерческих и некоммерческих целях, например, при организации выставки в цифровом виде. Что касается распоряжения, то правообладатель имеет право перепродать NFT единственному возможному покупателю, поскольку происходит полная передача объекта без возможности его использования другими лицами. Для перехода к правообладателю исключительных прав на объект интеллектуальной собственности, в отношении которого был выпущен NFT, необходимо заключить договор об отчуждении исключительных прав или лицензионный договор, поскольку самого по себе факта приобретения NFT недостаточно.

2.2. Учет и хранение музейных предметов в NFT-формате.

2.2.1. Музейные предметы в NFT-формате можно определить как виртуальные музейные предметы без отражения их на балансе учреждения. Учет таких объектов осуществлять в экспериментальном фонде музея с возможностью перевода в дальнейшем в основной фонд.

2.2.2. Хранение виртуальных музейных предметов видится целесообразным обеспечить на физическом электронном устройстве, которое использует генерацию случайных чисел для создания публичных и приватных ключей, хранящихся на самом устройстве без доступа в Интернет. Такой способ хранения обеспечивает безопасный доступ к виртуальной коллекции музея на блокчейн-платформе, что уже активно используется в музейной практике.

Выводы

На основании вышеизложенного можно сделать вывод, что основной спецификой использования музейных предметов в метавселенной на сегодняшний день в рамках договорных конструкций является распространение, помимо норм гражданского законодательства, императивных норм музейного законодательства.

На музейные предметы в формате NFT можно распространить такое же право собственности музея, как и на аналоговые музейные предметы. Для формирования виртуальной музейной коллекции необходимо, чтобы такие объекты были наделены свойствами музейного предмета. Тем самым целесообразно выделить в качестве самостоятельных объектов виртуальные музейные предметы, подлежащие специальному учету и хранению без отражения на балансе учреждения.

Невзаимозаменяемый токен выступает в качестве цифровой формы аналогового оригинала картины или арт-объекта, включающего воспроизведение музейного предмета в метавселенной, и подтверждает право владения уникальным цифровым активом. Музей вправе организовать продажу цифровых копий картин в NFT, передав покупателю ограниченный набор прав: владения, пользования и распоряжения.

Безусловно, регулирование объектов виртуального мира должно быть отличным от регулирования объектов реального мира. Тем самым видится необходимой разработка отдельной правовой основы для сделок с цифровыми произведениями искусства из собраний музеев в NFT.

Список литературы

- Андрейко, Е. О., Мужжавлева, Т. В. (2021). Цифровизация культуры и искусства: российский и зарубежный опыт. В книге: Н. В. Морозова и др. (ред.), *Цифровая трансформация государственного и муниципального управления: сборник материалов Всерос. науч. конф.* Чебоксары, 1 июля 2021 г. (с. 90–94). Чебоксары: ИД «Среда», 2021. <https://doi.org/10.31483/r-99129>
- Брисов, Ю. В., Победкин, А. А. (2022). Правовой режим NFT (non-fungible token) в России: как работать в отсутствие специального законодательного регулирования? *Цифровое право*, 3(1), 44–66. <https://doi.org/10.38044/2686-9136-2022-3-1-44-66>
- Бурдова, В. Д. (2022). Дуализм правовой природы музейных прав. В книге: *Труды по интеллектуальной собственности (Works on Intellectual Property)*, 41(2), 54–59. <https://doi.org/10.17323/tis.2022.14447>
- Гаврилова, Ю. А. (2021). Концепция интеграции искусственного интеллекта в правовую систему. *RUDN Journal of Law*, 25(3), 673–692. <https://doi.org/10.22363/2313-2337-2021-25-3-673-692>
- Григорьев, В. В., Нурисламова, Э. Р., Нурисламова, Н. Р. (2021). Функциональные аспекты криптовалюты. *Россия: тенденции и перспективы развития*, 16-1, 530–537.
- Долганин, А. А. (2021). Соотношение невзаимозаменяемых токенов (NFT) и интеллектуальной собственности: триумф проприетарного подхода? *Цифровое право*, 2(3), 46–54. <https://doi.org/10.38044/2686-9136-2021-2-3-46-54>
- Емельянов, Д. С., Емельянов, И. С. (2021). Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования. *Имущественные отношения в Российской Федерации*, 10(241), 71–76. <https://doi.org/10.24412/2072-4098-2021-10-71-76>
- Жуков, Д. В. (2020). Особенности защиты культурных прав в условиях развития цифровых технологий. *Журнал российского права*, 9, 44–52. <https://doi.org/10.12737/jrl.2020.105>
- Залоило, М. В., Пашенцев, Д. А. (2019). Национальный правопорядок России в условиях цифровизации. *Вестник Санкт-Петербургского университета. Право*, 10(2), 196–209. <https://doi.org/10.21638/spbu14.2019.201>
- Королева, Л. А. (2018). Цифровая эволюция искусства: социокультурный анализ в контекстах философии и культуры постмодерна. *Культура и технологии*, 3(1–2), 20–28. <https://doi.org/10.17586/2587-800X-2018-3-1-2-20-28>
- Кулакова, О. С. (2022). Цифровое искусство в контексте NFT: роль рынка и правовая неопределенность. *Цифровое право*, 3(2), 36–50. <https://doi.org/10.38044/2686-9136-2022-3-2-36-50>
- Новоселова, Л. А. (2017). «Токенизация» объектов гражданского права. *Хозяйство и право*, 12, 29–44.
- Пашенцев, Д. А. (2020). Особенности правоприменения в условиях цифровизации общественных отношений. *Вестник Санкт-Петербургского университета. Право*, 11(1), 35–49. <https://doi.org/10.21638/spbu14.2020.103>
- Рожкова, М. А. (2020). Имущественные права на новые нематериальные объекты в системе абсолютных прав. В книге: М. А. Рожкова (рук. и науч. ред.), *Право цифровой экономики – 2020 (16): ежегодник-антология* (с. 5–78). Москва: Статут.
- Савчук, В. В. (2017). Медиареальность – новая среда жизни. *Культура и технологии*, 2, 1–5. <https://doi.org/10.17586/2587-800X-2017-2-1-1-5>
- Суворова, К. А., Жевняк, О. В. (2022). NFT как объект гражданских прав. В книге: *Весенние дни науки: сборник докладов Международной конференции студентов и молодых ученых*. Екатеринбург, 21–23 апреля 2022 г. (с. 1407–1411). Екатеринбург: УрФУ, 2022.
- Цыгулева, М. В. (2021). Первый опыт реализации цифровых изображений произведений из собрания музея и передачи прав на них с использованием невзаимозаменяемых токенов. *Имущественные отношения в Российской Федерации*, 9(240), 84–95.
- Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O. et al. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Scientific Reports*, 12, 2178. <https://doi.org/10.1038/s41598-022-05920-6>
- Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, 44, 102097. <https://doi.org/10.1016/j.frl.2021.102097>
- Mekacher, A., Bracci, A., Nadini, M. et al. (2022). Heterogeneous rarity patterns drive price dynamics in NFT collections. *Scientific Reports*, 12, 13890. <https://doi.org/10.1038/s41598-022-17922-5>
- Nadini, M., Alessandretti, L., Di Giacinto, F. et al. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific Reports*, 11, 20902. <https://doi.org/10.1038/s41598-021-00053-8>
- Vasan, K., Janosov, M., & Barabási, A.-L. (2022). Quantifying NFT-driven networks in crypto art. *Scientific Reports*, 12, 2769. <https://doi.org/10.1038/s41598-022-05146-6>
- Wang, F.-Y., Qin, R., Yuan, Y., & Hu, B. (2021). “Nonfungible Tokens: Constructing Value Systems in Parallel Societies”. *IEEE Transactions on Computational Social Systems*, 8(5), 1062–1067. <https://doi.org/10.1109/TCSS.2021.3109359>

Сведения об авторе



Бурдова Вероника Дмитриевна – соискатель кафедры интеллектуальных прав, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)

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

E-mail: vdburdova@gmail.com

ORCID ID: <https://orcid.org/0000-0002-5275-3501>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1162641

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 17 октября 2022 г.

Дата одобрения после рецензирования – 23 января 2023 г.

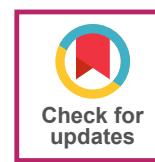
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.6>



Legal Nature of Reproducing Museum Objects in the Digital Form of NFT

Veronika D. Burdova 

Kutafin Moscow State Law University (MSAL)
Moscow, Russian Federation

Keywords

Art,
digital assets,
digital rights,
digital technologies,
intellectual property,
metaverse,
museum,
NFT,
right,
token

Abstract

Objective: by revealing the legal nature of the nonfungible token (NFT), to propose a solution for the topical issues of legal regulation of relations emerging in the sphere of online market and Internet platforms, associated with reproduction and further use in the virtual environment of tokenized digital copies of original pieces of art.

Methods: the research was based on formal-legal and comparative-legal analysis, applied together with methods of law interpretation.

Results: a conclusion is made that reproduction of a museum object in the digital form of NFT is not equal to reproduction of a museum object in the simple digital format, as it does not contain such mandatory criteria as uniqueness, indivisibility and scarcity of the specific token. An NFT object acts as a digital original of an analog original of a museum object in the digital environment and the metaverse, not as a new form of media art. Expressed in the form of a uniqueness certificate of a digital object, an NFT object, by its legal nature and for the purpose of legal regulation of deals with it, refers to "other property" among the objects of civil law, which allows the museums to apply the respective contract constructs when structuring such deals.

Scientific novelty: the author proposes a new approach to considering and improving the legal regulation, accounting and storing NFT objects as virtual museum objects, the so-called digital equivalents of an item, which possess the signs of individual-definite character and uniqueness, differing from simple digital copies, digital pieces of art, 3D mapping, etc.

© Burdova V. D., 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 research results can be used for improving legal regulation of museum activity, correcting the civil and museum legislation, in particular, for defining virtual museum objects; for implementation of law, for example, when signing deals on using and selling NFT objects, in terms of specifying the content and volume of authorities of the right holders of the nonfungible token.

For citation

Burdova, V. D. (2023). Legal Nature of Reproducing Museum Objects in the Digital Form of NFT. *Journal of Digital Technologies and Law*, 1(1), 152–174. <https://doi.org/10.21202/jdtl.2023.6>

References

- Andreyko, E. O. & Muzhzhavleva, T. V. (2021). Digitalization of culture and art: Russian and foreign experience. In N. V. Morozova et al. (Eds.). *Digital transformation of state and municipal governance: collection of works of All-Russian scientific conference*. Cheboksary, July 1, 2021 (pp. 90–94). Cheboksary: ID Sreda, 2021. (In Russ.). <https://doi.org/10.31483/r-99129>
- Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O. et al. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Scientific Reports*, 12, 2178. <https://doi.org/10.1038/s41598-022-05920-6>
- Brisov, Yu. V. & Pobedkin, A. A. (2022). Legal regime of NFT (non-fungible token) in Russia: how to work in the absence of special legislative regulation? *Tsifrovoe pravo*, 3(1), 44–66. (In Russ.). <https://doi.org/10.38044/2686-9136-2022-3-1-44-66>
- Burdova, V. D. (2022). Duality of the legal nature of museum rights. In: *Works on intellectual property*, 41(2), 54–59. (In Russ.). <https://doi.org/10.17323/tis.2022.14447>
- Dolganin, A. A. (2021). Correlation between non-fungible tokens (NFT) and intellectual property: triumph of proprietary approach? *Tsifrovoe pravo*, 2(3), 46–54. (In Russ.). <https://doi.org/10.38044/2686-9136-2021-2-3-46-54>
- Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, 44, 102097. <https://doi.org/10.1016/j.frl.2021.102097>
- Emelyanov, D. S., & Emelyanov, I. S. (2021). Non-fungible tokens (NFT) as a separate object of legal regulation. *Imushchestvennye otnosheniya v Rossiiskoi Federatsii*, 10(241), 71–76. (In Russ.). <https://doi.org/10.24412/2072-4098-2021-10-71-76>
- Gavrilova, Yu. A. (2021). Concept of integration of artificial intelligence into a legal system. *RUDN Journal of Law*, 25(3), 673–692. (In Russ.). <https://doi.org/10.22363/2313-2337-2021-25-3-673-692>
- Grigoryev, V. V., Nurislamova, E. R., & Nurislamova, N. R. (2021). Functional aspects of cryptocurrency. *Rossiya: tendentsii i perspektivy razvitiya*, 16–1, 530–537. (In Russ.).
- Koroleva, L. A. (2018). Digital evolution of art: sociocultural analysis in the contexts of postmodernism philosophy and culture. *Kultura i tekhnologii*, 3(1–2), 20–28. (In Russ.). <https://doi.org/10.17586/2587-800X-2018-3-1-2-20-28>
- Kulakova, O. S. (2022). Digital art in the context of NFT: the role of market and legal uncertainty. *Tsifrovoe pravo*, 3(2), 36–50. (In Russ.). <https://doi.org/10.38044/2686-9136-2022-3-2-36-50>
- Mekacher, A., Bracci, A., Nadini, M. et al. (2022). Heterogeneous rarity patterns drive price dynamics in NFT collections. *Scientific Reports*, 12, 13890. <https://doi.org/10.1038/s41598-022-17922-5>
- Nadini, M., Alessandretti, L., Di Giacinto, F. et al. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific Reports*, 11, 20902. <https://doi.org/10.1038/s41598-021-00053-8>
- Novoselova, L. A. (2017). “Tokenisation” of the objects of civil law. *Khozyaystvo i pravo*, 12, 29–44. (In Russ.).

- Pashentsev, D. A. (2020). Features of law enforcement under digitalization of public relations. *Vestnik Sankt-Peterburgskogo universiteta. Pravo*, 11(1), 35–49. (In Russ.). <https://doi.org/10.21638/spbu14.2020.103>
- Rozhkova, M. A. (2020). Property rights to new non-material objects in the system of absolute rights. In M. A. Rozhkova (Ed.). *Pravo tsifrovoy ekonomiki – 2020(16): yearbook-anthology* (pp. 5–78). Moscow: Statut. (In Russ.).
- Savchuk, V. V. (2017). Mediareality – a new medium of living. *Kultura i tekhnologii*, 2, 1–5. (In Russ.). <https://doi.org/10.17586/2587-800X-2017-2-1-1-5>
- Suvorova, K. A. & Zhevnyak, O. V. (2022). NFT as an object of civil rights. In: *Vesenniye dni nauki: collection of works of International conference of students and young scientists*. Yekaterinburg, April 21–23, 2022 (pp. 1407–1411). Ekaterinburg: UrFU, 2022. (In Russ.).
- Tsyguleva, M. V. (2021). First experience of marketing digital images of pieces from a museum collection and transferring the rights to them, using non-fungible tokens. *Imushchestvennyye otnosheniya v Rossiiskoi Federatsii*, 9(240), 84–95. (In Russ.).
- Vasan, K., Janosov, M., & Barabási, A.-L. (2022). Quantifying NFT-driven networks in crypto art. *Scientific Reports*, 12, 2769. <https://doi.org/10.1038/s41598-022-05146-6>
- Wang, F.-Y., Qin, R., Yuan, Y., and Hu, B. (2021). “Nonfungible Tokens: Constructing Value Systems in Parallel Societies”. *IEEE Transactions on Computational Social Systems*, 8(5), 1062–1067. <https://doi.org/10.1109/TCSS.2021.3109359>
- Zaloilo, M. V. & Pashentsev, D. A. (2019). National law order in Russia under digitalization. *Vestnik Sankt-Peterburgskogo universiteta. Pravo*, 10(2), 196–209. (In Russ.). <https://doi.org/10.21638/spbu14.2019.201>
- Zhukov, D. V. (2020). Features of protection of cultural rights under the development of digital technologies. *Zhurnal rossiyskogo prava*, 9, 44–52. (In Russ.). <https://doi.org/10.12737/jrl.2020.105>

Author information



Veronika D. Burdova – applicant of the Department of Intellectual Rights, Kutafin Moscow State Law University (MSAL)

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

E-mail: vdburdova@gmail.com

ORCID ID: <https://orcid.org/0000-0002-5275-3501>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1162641

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – October 17, 2022

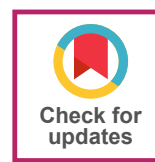
Date of approval – January 23, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 349.2:004
EDN: <https://elibrary.ru/zennzf>
DOI: <https://doi.org/10.21202/jdtl.2023.7>



Концепция труда: от традиционных социально-трудовых представлений к современным эффектам цифровой трансформации

София Рицу 

Университет Мишкольца
г. Мишкольц, Венгрия

Габор Мелипатаки 

Университет Мишкольца
г. Мишкольц, Венгрия

Дэвид Адриан Мате 

Университет Мишкольца
г. Мишкольц, Венгрия

Ключевые слова

Занятость,
концепция труда,
нетипичный труд,
социальная политика,
труд,
трудовое право,
трудовые правоотношения,
цифровизация,
цифровые платформы,
цифровые технологии

Аннотация

Цель: переосмысление сложившейся концепции труда, эволюционирующей под влиянием классических научных парадигм и радикальных цифровых и технологических трансформаций социальных отношений в условиях сложившегося концептуального многообразия и неопределенности.

Методы: ретроспективный и сравнительный правовой анализ, лежащий в основе проведенного исследования, позволил рассмотреть сложившиеся подходы к пониманию труда с учетом реалий современной ситуации в разных странах и наблюдаемых в них цифровых эффектов, приводящих к цифровизации и технологизации труда, изменениям отношений в сфере занятости, а соответственно, к изменениям трудового права и трудовым правоотношениям.

Результаты: авторы показали проблемы регулирования трудовых отношений в новых условиях и предложили их решения; выявили причинно-следственную связь между цифровизацией (в частности,

 Контактное лицо

© Рицу С., Мелипатаки Г., Мате Д. 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.

развитием цифровой экономики и технологическими новациями) и появлением нетипичных форм труда и занятости, которые в результате деятельности законодателя, регулирующего возникающие отношения в новых условиях, переводящую их из разряда нетипичных в типичные трудовые отношения, а для тех ситуаций, которые оказываются в «серой зоне» правового регулирования, – дающую такое толкование юридическим нормам, которое не потеряет свое значение в период обозримых технологических изменений; определили возрастающую значимость труда в процессе цифровизации и существенное влияние трудового права на регулирование в сфере нетипичного труда, несмотря на имеющуюся критику.

Научная новизна: рассмотрены актуальные дискуссионные вопросы, получившие новый импульс в связи с цифровым развитием общественных отношений и проявившихся цифровых эффектов, в результате которых появились новые типы и методы найма, что побуждает к пересмотру дуальной модели отношений найма, изменениям границ ранее выраженной дихотомии между работодателем и предпринимателем.

Практическая значимость: трансформация концепции труда обуславливает пересмотр традиционных правовых и основных научных подходов, ранее сложившихся в исследовании труда и занятости, на основе учета современной трансформации общественных отношений и труда, их цифровизации и технологизации.

Для цитирования

Рицу, С., Мелипатаки, Г., Мате, Д. А. (2023). Концепция труда: от традиционных социально-трудовых представлений к современным эффектам цифровой трансформации. *Journal of Digital Technologies and Law*, 1(1), 175–190. <https://doi.org/10.21202/jdtl.2023.7>

Содержание

Введение

1. Расширение концепции труда

2. Цифровые эффекты и приверженность к трудовому праву

Выводы

Введение

Дать определение концепции труда непросто, поскольку труд не имеет четких границ. Во всяком случае невозможно определить, выполняется ли какая-либо деятельность в качестве труда или нет. Однако, прежде чем мы обсудим этот вопрос, важно подчеркнуть, что мы придерживаемся подхода к труду, принятому в общественных дисциплинах.

В более ранних исследованиях рассматривались некоторые аспекты различных форм труда (Venkatesh, 1992). Труд – это целенаправленная деятельность, направленная в будущее. Его основными характеристиками являются эффективность

и специализация, которые влияют на общечеловеческие ценности. Другой важный аспект труда – социальная идентичность и доход. Мотивация индивида к труду тесно связана с потребностью в деятельности и возможностью саморегуляции. Внутрудовая деятельность обеспечивает непосредственное удовлетворение нужд и интересов человека (Quey, 1968).

Экономический подход к концепции труда является одним из самых распространенных. Согласно ему, труд – это «деятельность, за которую индивид получает финансовую компенсацию, чтобы иметь средства к существованию» (Pahl, 1988). Таким образом, одна из важнейших характеристик труда состоит в том, что труд – это юридическая сделка, приносящая доход. Это означает, что как труд может рассматриваться только такая деятельность, за которую выплачивается некая (обычно денежная) компенсация. Если бы мы провели репрезентативный опрос среди населения, то получили бы подобные ответы. Такого же толкования придерживаются и некоторые законодатели с экономическим подходом. В этом отношении можно выделить федеральное законодательство США в сфере поддержки безработных, а именно Федеральный закон 3304 о налогообложении безработных, включая комментарий к п. 7. Департамент труда США дает определение труда в руководстве, поясняющем применение этого закона (Definition of «Work» for Purposes of Section 3304(a)(7) of the Federal Unemployment Tax Act). В контексте данного закона, выполнение деятельности, за которую не выплачивается вознаграждение, не является работой. Так же определяется и концепция труда. В директиве, вышедшей в 1994 г., концепция труда интерпретируется как предоставление услуг, за которые выплачивается вознаграждение (Definition of «Work» for Purposes of Section 3304(a)(7) of the Federal Unemployment Tax Act). Эта концепция основана на экономическом подходе. Однако данная директива, опубликованная как разъяснение закона, подчеркивает тот факт, что такая интерпретация характерна для 1970-х гг. и законодатель незнаком с формами труда, ставшими типичными в период с начала до середины 1990-х гг. Законодатель указывает, что первоначальная интерпретация не охватывает предпринимателей и работников «по вызову», а также работающих по договору почасового найма. Но возникает вопрос: только ли деятельность за вознаграждение может считаться работой? В своем совместном исследовании Szép и Sík ссылаются на ряд источников, в которых обсуждаются погрешности измерений, например, работа по хозяйству не считается трудом (Szép & Sík, 2001). Такая работа регулируется налоговым, но не трудовым законодательством. Важно также отметить, что здесь объединяются несколько концепций. Следует особо выделить предпринимателей (Szekeres, 2021), так как это отдельная форма работы, сочетающая элементы деловых отношений и найма. Она отличается тем, что они зависят от других, но в то же время действуют независимо.

В исследовании R. E. Pahl концепция работы интерпретирована нечетко (Pahl, 1988). Автор, вероятно, пытался вместить множество различных понятий в один термин, объединяя волонтерство, мытье посуды и труд нейрохирурга (Laky, 1998). Рассматривая различные определения труда, мы все чаще задаемся вопросом, действительно ли следует называть трудом только ту деятельность, за которую платят деньги. Что же тогда такое ведение домашнего хозяйства? Социальное значение этой деятельности все более возрастает, но она не достаточно юридически признана. В Венгрии она признана в сфере налогового права, но не трудового. Кроме того,

можно упомянуть Закон III об общественном управлении и льготах от 1993 г.¹, раздел о пособиях по уходу за ребенком дома. Однако он затрагивает лишь часть рынка труда.

Таким образом, в рамках настоящего исследования мы рассмотрим, какие определения труда релевантны в контексте процессов цифровизации. Мы не можем использовать концепцию Дэвида Грабера (Graeber, 2019), так как обосновываем возможность правового регулирования данной сферы в заключении нашей статьи.

1. Расширение концепции труда

Изучая концепцию труда, важно рассмотреть отношения найма, направленные на работу. В рамках классических отношений найма работодатель обладает широкими правами в плане структуризации. В сущности, формальное законодательство охватывает все стороны отношений найма, и правоотношения наполняются содержанием посредством служебных инструкций. Однако эта парадигма изменилась под влиянием цифровизации. Классические квалификационные критерии не всегда сохраняют релевантность, поэтому правила, записанные в инструкциях, могут трансформироваться в процессе конкретных правоотношений: работа по классическим служебным инструкциям уже не может опираться на статичные основания, поэтому квалификационные признаки отношений найма также меняются (Sherer, 2016).

При этом очевидно, что определение работы должно включать не только работу, выполняемую в рамках отношений найма, основанных на классических служебных инструкциях. В случаях индивидуальных форм работы встает вопрос, должны ли они включаться в сферу трудового права. В исследовании István Horváth с соавторами выявлена дихотомия: с одной стороны, простая классификация необходима для систематизации; с другой – традиционная структура трудового права не применима ко всем формам труда (Horváth et al., 2021). В определенных случаях труд может также означать деятельность, которая выполняется не в рамках классических отношений найма. Концепция труда применима не только к работе, выполняемой в подчиненной позиции, но и ко всем формам работы, безотносительно к понятиям зависимости и независимости.

Исследователь Vincenti отмечал, что трудовые правоотношения входят в сферу частного права, нормы которого регулируют труд человека (как форму экономической ценности) (Vincenti, 1942). На основе этого положения в следующей главе мы подробнее рассмотрим содержание предпринимательской деятельности, а также зависимые и независимые формы труда и покажем, что их также можно классифицировать в рамках правоотношений найма. При этом концепция труда охватывает не только отношения найма и самозанятости (на основе деловых и посреднических соглашений). В настоящее время широкое распространение получили некоторые формы коллективной работы. Работа за оклад по-прежнему занимает важное место, однако нужно понимать, что труд может включать элементы, не предусматривающие компенсацию за их выполнение. Развитие общественной экономики и технологические

¹ Act III of 1993 on Social Governance and Social Benefits. https://ec.europa.eu/migrant-integration/library-document/act-iii-1993-social-governance-and-social-benefits_en

изменения привели к появлению ряда новых форм занятости, которые дополнили или заменили традиционные формы².

Дать определение концепции труда непросто, поскольку он не имеет четких границ (Brief, 1990). Выше мы коснулись экономической точки зрения, согласно которой труд – это любая деятельность, за которую выплачивается вознаграждение. Однако такой подход значительно сужает определение труда, так как не учитывает виды работ, которые человек выполняет без вознаграждения или даже в качестве волонтерства. Такой вид работы рассматривается в основном только тогда, когда она не выполняется, потому что ведение домашнего хозяйства, волонтерская работа играют важную роль в улучшении жизненных условий, наряду с доходами и участием в рынке труда. Трудоспособное население часто одновременно несет нагрузку по уходу за детьми и пожилыми, что может повлиять на решения в области занятости (Mann & Chang, 2015). Так, в исследовании Röder с соавторами анализировались стратегии выхода на работу матерей после родов. Было обнаружено, что в странах Евросоюза женщины после декретного отпуска все чаще не возвращаются на оплачиваемую работу, а остаются вести домашнее хозяйство и ухаживать за детьми (Röder et al., 2018). Несомненно, работа по дому выполняется не только женщинами; однако исследование на основе многовариантного анализа и двух показателей текущего состояния здоровья показало, что корреляция между ведением домашнего хозяйства и уровнем здоровья относительно низка, тогда как корреляция между выходом на оплачиваемую работу и уровнем заболеваемости гораздо выше для обоих полов; ряд показателей для определенных аспектов трудовой деятельности также показывают, что результаты не зависят от пола (Hunt & Annandale, 2008).

В прошедшие десятилетия, особенно в течение последних двадцати лет, наблюдалась трансформация концепции труда (Tyutyuryukov & Guseva, 2021; Bamel et al., 2022; Oberländer & Bipp, 2022; Richter, 2020). Труд может рассматриваться как источник средств к существованию, как реализация карьерных целей или в самом счастливом случае как реализация склонности человека. Отталкиваясь от последнего, мы можем также затронуть концепцию эмоциональной работы. Эмоциональная работа определяется как эмоциональное регулирование, необходимое для того, чтобы работники демонстрировали организационно-желаемые эмоции. Это понятие все больше привлекает внимание, так как оно релевантно в сфере услуг, где социальное взаимодействие с покупателями, клиентами или пациентами является важной частью работы (Zapf & Holz, 2006).

В настоящее время все более значимой частью работы становится наполнение ее индивидуальным содержанием (Rácz, 2021). В последние десятилетия основными характеристиками трудовых отношений стали неоднородность и индивидуализация. Этот тренд усиливается за счет появления нетипичных форм труда, подчеркивающих самореализацию и развитие работников (Török, 2014). В таком аспекте труд приобретает еще большую значимость, учитывая, что цифровизация только способствует этому процессу. В будущем мы можем предсказать дальнейшее расширение концепции труда и дифференциацию трудовых отношений.

Все вышесказанное подтверждает, что определение труда может включать множество его форм, не ограничиваясь определением задач, выполняемых в рамках

² OECD Employment Outlook. (2019). <https://www.oecd.org/employment-outlook/2019/>

классических отношений найма. Концептуальное определение труда не может не быть широким; границы его размыты. Кроме того, оно должно ориентироваться на будущее, т. е. описывать не только те правоотношения найма, которые существуют в данный момент. При этом несомненно, что, изучая определенные проблемы интерпретации труда, нельзя игнорировать необходимость гарантий для тех, кто выполняет работу.

Очевидно, что трудовые отношения и иные правоотношения, направленные на работу по найму, должны адаптироваться к изменениям в обществе, происходящим в результате цифрового развития.

2. Цифровые эффекты и приверженность к трудовому праву

Развивая далее тезисы, представленные во Введении, мы хотим отметить, что концепция труда становится спорной даже в отношении тех видов деятельности, в ходе которых человек получает вознаграждение и обеспечивает себя средствами к существованию; во всяком случае она спорна с правовой точки зрения. Это относится к правовой классификации правоотношений лиц, выполняющих работу, а именно классификации предпринимателей и зависимых работников. Дуальная модель отношений найма подразумевает дихотомию между работодателем и предпринимателем (Jakab, 2018). Эта проблема уже вызвала острую дискуссию среди специалистов, которая недавно получила новый импульс с появлением новых типов и методов найма в результате цифровых эффектов (Prugberger, 2018). Значительную долю в этом процессе занимают формы работы через платформы, которые мы рассматриваем в данной статье как собирательную категорию. Особенность работы через платформы состоит в том, что она во многом основана на крайне гибких, нетипичных правоотношениях. Эти правоотношения охватывают в первую очередь смешанные гражданско-правовые отношения в рамках гражданского права, с элементами договора найма, посреднического договора, делового соглашения и договора переуступки. Другая характеристика официальных правоотношений состоит в том, что сторона договора, по сути, лишь предоставляет исполнителю рынок для выполнения работы, за которую он получает определенное вознаграждение. Пример работы через платформы – деятельность доставщиков товаров. Они регистрируются через приложение, заключая при этом контракт с различными параметрами. На основе этого контракта курьер получает доступ к постоянно обновляемой базе данных, в которой непрерывно появляется информация о том, какие услуги может оказать конкретный доставщик. Обычно курьер не берет на себя обязанности оказывать услуги (Rácz, 2021); в большинстве случаев не определяется ни минимальное количество заданий, ни количество часов; курьер сам решает, когда и сколько заданий он выполнит. Сторона, заключающая договор, в первую очередь стремится обеспечить непрерывное выполнение заданий путем выплаты вознаграждений. Курьер осуществляет деятельность своими собственными средствами как частное лицо или как индивидуальный предприниматель, но в любом случае задание выполняется для кого-то другого и в большинстве случаев индивидуально. Этот пример показывает, что смешанный контракт привел к появлению гибридного решения. Это существенно влияет не только на концепцию труда, но и на интерпретацию понятия зависимого труда.

Как подчеркивает Tamás Prugberger, самым существенным элементом как договоров об оказании услуг, так и договоров найма является то, что тот, кто оказывает услугу, должен быть доступен человеку, заказывающему услугу, как работник должен быть доступен работодателю, в течение всего периода, установленного контрактом; а также в течение всего этого периода он должен регулярно выполнять услугу или работу, оговоренную в контракте (Prugberger, 2020). Обязанность быть доступным действительно создает положение доминирования между сторонами, однако, по нашему мнению, зависимость не ограничивается этим элементом. Все вышесказанное подтверждается конкретными теориями, лежащими в основе трудового права, и следствиями из них.

Основой отношений найма является независимый и зависимый труд. Изначально зависимость определялась как чисто экономическая, затем возникла теория личной зависимости. Последняя была основана на том, что работники вкладывают свою личность в выполняемую деятельность и между сторонами возникают особые зависимые отношения.

Позднее эти теории уступили место рассуждениям о том, что критерий разграничения в отношениях найма лежит в области объекта услуги. В случае отношений найма услуга не конкретизирована; более того, работодатель наделен правом давать инструкции. Таким образом, мы можем разграничить отношения найма и иные (гражданские) правоотношения в первую очередь на основе того факта, что работодатель пользуется широким односторонним правом определять деятельность работника и предоставление услуги (Rácz, 2021). Однако это полностью опровергается при работе через платформы, поскольку сторона, владеющая платформой, отказывается от права на заключение одностороннего контракта с лицом, выполняющим работу в определенных случаях и определенным образом. Платформа не дает инструкций, она лишь предоставляет возможность выполнять работу. Сторона, владеющая платформой, не выставляет требований по выполнению работы, а предмет услуги определяется контрактом и в некоторых отношениях четко описан; поэтому, в соответствии с последней описанной теорией, сторона, владеющая платформой, теоретически не находится в доминирующем положении (Lee, 2022). Такая позиция стороны, владеющей платформой, обычно подчеркивается прописанной в контракте ролью посредника; другими словами, они заявляют, что только соединяют спрос и предложение, но не стремятся влиять на структуру занятости (Rácz, 2021).

Приверженность можно видеть и в других аспектах. С определенной точки зрения можно говорить также об экономической зависимости, поскольку работа через платформы обычно выполняется социальными группами, находящимися в некоторой степени на периферии рынка труда. Такой тип занятости присущ в основном молодым людям, студентам или, к примеру, матерям в декрете как дополнительный заработок. Эта модель является благословением и проклятием для уязвимых сегментов рынка труда. Основываясь на одном из исследований, посвященных проблемам социального обеспечения женщин, можно предположить, что такая модель будет особенно привлекательна для женщин, стремящихся найти баланс между заработком и семейными обязанностями. Исследователь Gerber рассматривал вопросы о том, женщины или мужчины ощущают большую неопределенность, работая через платформы, и отличаются ли их риски. На материале Германии между женщинами и мужчинами обнаружились большие различия в этих вопросах; это свидетельствует о высокой степени дуальности рынка труда и прекаризации по гендерному

признаку, а также о сохранении традиционного разделения домашних обязанностей (Gerber, 2022).

Отношения доминирования проявляются также в том, что сторона, владеющая платформой, сохраняет право контроля, хотя и в обновленной форме. Платформа собирает огромное количество данных, влияющих на работу, замеряет активность, скорость выполнения, уровень удовлетворенности клиентов (Orlikowski & Scott, 2021; Terhoeven et al., 2022; Yao et al., 2022). Действительно, даже в случае использования делового соглашения клиент имеет право в некоторой степени давать инструкции и контролировать, но эти права ограничены. По нашему мнению, ситуация доминирования и зависимости между стороной, владеющей платформой, и работником может существовать в первую очередь (но не только) по причине широких полномочий в сфере контроля.

В свете вышесказанного, с юридической точки зрения до сих пор, к сожалению, не решен вопрос, нужно ли создавать концепцию труда, учитывающую только нерегулярный труд. Создание такой концепции очень помогло бы правоприменительной деятельности. Вместе с тем создание такой всеобъемлющей концепции в существующих реалиях не представляется возможным. Кроме того, важно подчеркнуть, что изменяющиеся условия и развитие цифровых технологий требуют осмысления, без которого невозможно решить все возникающие проблемы концептуализации и разграничения понятий.

Выводы

Из вышеизложенного также следует, что концепция труда является одновременно статичной и динамичной. Причина этого в том, что ее значение и объем входящих в нее видов деятельности непрерывно изменяются и расширяются. Наблюдается как снижение значимости труда, так и изменение труда как такового. С одной стороны, значение других факторов производства, помимо труда, т. е. капитала и знаний, возросло по сравнению с XIX в. С другой – снизилось формирующее и социализирующее влияние совместного труда: эпоха классического рабочего движения осталась позади, а с ней ушло и то время, когда опыт, интересы, конфликты и союзы сферы труда существенно влияли на политику. Одной из причин такого развития являются фундаментальные изменения в формах труда, в ходе которых акцент сместился с ручного труда на нефизический труд, с индустриального общества на общество услуг, что произошло под влиянием революции в сфере коммуникации и глобализации (Terhoeven et al., 2022). Согласно тезису Murphy и Oesh, развитие технологий должно привести к выхолащиванию структуры занятости, а далее – к универсальной схеме поляризации во всех технологически развитых странах (Murphy & Oesch, 2018). Эти авторы указывают на то, что изменения в структуре занятости определяются трудовыми институтами и предложением на рынке труда, особенно факторами образования и иммиграции, поэтому поляризация является единственно возможным сценарием в сфере занятости. В своем исследовании на материале Ирландии и Швейцарии, используя статистические данные и разносторонний анализ рабочей силы, они доказали наличие долгосрочных (за период в почти 40 лет) изменений в структуре занятости (Murphy & Oesch, 2018).

Исследуя цифровизацию труда, специалисты по общественным наукам обнаружили новые группы работников, возникших на почве цифрового капитализма.

Появились такие категории, как фрилансеры, внештатные исполнители, производящие потребители. Таким образом, цифровизация влияет на существующие группы работников; например, многие из них заменяются в процессе автоматизации, но возникают и новые профессиональные группы (Dorschel, 2022).

В заключение отметим, что труд может рассматриваться как любая деятельность, имеющая целью реализацию или сохранение какой-либо личной или межличностной, цивилизационной, культурной, правовой, политической или экономической ценности. Очевидная цель труда в экономике – создание товаров и услуг, имеющих экономическую ценность. Эти товары и услуги должны обеспечивать комфорт, безопасность, защиту, предсказуемость, в конечном итоге – приятную жизнь или в крайнем случае выживаемость. Однако в процессе такого труда могут быть реализованы не только экономические, но и внеэкономические ценности, в первую очередь личные и межличностные. Это произойдет при условии, что труд даст человеку возможность проявить творчество. Многофакторные исследования, посвященные отношению работников к своему труду, проводились на репрезентативных выборках в Бельгии, Германии, Японии и США в 1982–1983 и 1989–1992 гг. Их результаты подтвердили, что одним из значимых векторов такого отношения является вектор «нагрузка/контроль – общественный вклад». Работники, определявшие свой труд в терминах «нагрузка/контроль» и/или «принуждение», подчеркивали свои издержки в процессе труда. Те же, кто рассматривал работу в основном как отношения ответственности и обмена, отмечали взаимную выгоду между работником и организацией или обществом в целом. Респонденты, определявшие труд как вклад в общественное благосостояние, подчеркивали социальные выгоды работы (Ruiz-Quintanilla & England, 1996). Следует также отметить, что такая ситуация характерна в определенной степени для всех видов человеческой деятельности, хотя, несомненно, в меньшей степени в экономической деятельности, чем, например, в науке или культуре (Rimler, 1999).

Вопрос в том, насколько всеобъемлюща эта концепция. Можем ли мы включить в нее новые технологические решения и обеспечить как минимум такую же степень защиты в рамках трудового права, как труду в классическом понимании? Ответа на первый вопрос пока нет. Возможно, придется пересмотреть некоторые аспекты этой концепции. Другой вопрос – насколько верно законодатель понимает концепцию труда. Способен ли он дать интерпретацию, которая через год или два не станет бессмысленной из-за технологического прогресса? Судя по современному состоянию, законодательство сильно отстает. Если посмотреть хотя бы на законодательство Венгрии, как в нем смешаны понятия домашнего офиса и удаленной работы, то придется признать, что законодатель не понимает концепции труда в современном мире, а возможно, и не хочет этого понимать. Результаты цифровизации не признаются, защита занятых в этой сфере не обеспечивается. До сих пор используются концепции XX в., современные проблемы трактуются с тех позиций. Если законодатель не понимает различий между домашним офисом и удаленной работой, то что говорить о таких еще более сложных реалиях, как работа через платформу или использование коллаборативных роботов, которые лежат в основе Индустрии 5.0 (Benotsmane et al., 2020). Проблемой станет не только применение концепции труда, но и решение проблем рынка труда и социально-правовых вопросов. Тем не менее наш подход к этой ситуации в целом полон надежды. Мы надеемся, что ситуация изменится и что политики также осознают необходимость перемен.

Számjegyzék

- Bamel, U., Kumar, S., Lim, W. M., Bamel, N., & Meyer, N. (2022). Managing the dark side of digitalization in the future of work: A fuzzy TISM approach. *Journal of Innovation & Knowledge*, 7(4), 100275. <https://doi.org/10.1016/j.jik.2022.100275>
- Benotmane, R., Dudás, L., & Kovács, G. (2020). Simulation and trajectory optimization of collaborating robots by application of solidworks and matlab software in industry 4.0. *Academic Journal of Manufacturing Engineering*, 18(4), 191–197.
- Brief, A. P.-N. (1990). Work and meaning: definitions and interpretations. In A. P.-N. Brief, *Meanings of occupational work: A collection of essays*. Lexington, MA: Lexington Books.
- Definition of "Work" for Purposes of Section 3304(a)(7) of the Federal Unemployment Tax Act. (n.d.). https://oui.doleta.gov/dmstree/uipl/uipl92/uipl_1892.htm#:~:text=In%20General,for%20which%20remuneration%20is%20payable
- Dorschel, R. (2022). Reconsidering digital labour: bringing tech workers into the debate. *New Technology, Work and Employment*, 37(2), 288–307. <https://doi.org/10.1111/ntwe.12225>
- Gerber, C. (2022). Gender and precarity in platform work: Old inequalities in the new world of work. *New Technologies, Work and Employment*, 37(2), 206–230. <https://doi.org/10.1111/ntwe.12233>
- Graeber, D. (2019). *Bullshit works*. Simon & Schuster.
- Horváth, I., Pérez del Prado, D., Petrovics, Z., & Sitzia, A. (2021). The Role of Digitisation in Employment and Its New Challenges for Labour Law Regulation: The Hungarian, Italian and Spanish Solutions, Comparison, and Criticism. *ELTE Law Journal*, 2, 101–132. <https://doi.org/10.54148/eltelj.2021.2.101>
- Hunt, K. & Annandale, E. (2008). Just the job? Is the relationship between health and domestic and paid work gender-specific? *Sociology of Health & Illness*, 15(5), 632–664. <https://doi.org/10.1111/1467-9566.ep11434424>
- Jakab, N. (2018). Systematic thinking on employee status. *Lex et Scientia*, 25(2), 56–68.
- Laky, T. (1998). Változó foglalkozás a munka változó világában. *Közgazdasági Szemle*, 45(2), 123–136.
- Lee, B.-Y. (2022). Neither Employee nor Contractor: A Case Study of Employment Relations between Riders and Platform-Based Food-Delivery Firms in Taiwan. *Work, Employment and Society*, 095001702211031. <https://doi.org/10.1177/09500170221103147>
- Mann, M., & Chang, C. (2015). Work-Family Issues. In *The Encyclopedia of Adulthood and Aging* (pp. 1–5). <https://doi.org/10.1002/9781118521373.wbeaa197>
- Murphy, E. C., & Oesch, D. (2018). Is Employment Polarisation Inevitable? Occupational Change in Ireland and Switzerland, 1970–2010. *Work, Employment and Society*, 32(6), 1099–1117. <https://doi.org/10.1177/0950017017738944>
- Oberländer, M., & Bipp, T. (2022). Do digital competencies and social support boost work engagement during the COVID-19 pandemic? *Computers in Human Behavior*, 130, 107172. <https://doi.org/10.1016/j.chb.2021.107172>
- Orlikowski, W. J., & Scott, S. V. (2021). Liminal innovation in practice: Understanding the reconfiguration of digital work in crisis. *Information and Organization*, 31(1), 100336. <https://doi.org/10.1016/j.infoandorg.2021.100336>
- Pahl, R. E. (1988). *On Work: Historical, Comparative and Theoretical Approaches*. New York: Basil Blackwell.
- Prugberger, T. (2018). A jogkövetkezményeket érintő problémák a munkaszerződés egyes hibatípusainál. *Debreceni Jogi Műhely*, 15(3–4), 19–26. <https://doi.org/10.24169/djm/2018/3-4/3>
- Prugberger, T. (2020). Az atipikus szolgálati/munkaszerződések jogdogmatikai és rendszerezésbeli kérdései, különös hangsúllyal a munkaerőpiac legújabb igényeire. *Miskolci Jogi Szemle*, 2, 44–66.
- Quey, R. (1968). Toward a Definition of Work. *The Personnel and Guidance Journal*, 47(3), 223–227. <https://doi.org/10.1002/j.2164-4918.1968.tb02920.x>
- Rácz, I. (2021). Platform munkavégzés Magyarországon Munkajogi és egyéb jogági dilemmák. *Magyar Munkajog E-folyóirat*, 1, 1–15.
- Rahrovani, Y. (2020). Platform drifting: When work digitalization hijacks its spirit. *The Journal of Strategic Information Systems*, 29(2), 101615. <https://doi.org/10.1016/j.jsis.2020.101615>
- Richter, A. (2020). Locked-down digital work. *International Journal of Information Management*, 55, 102157. <https://doi.org/10.1016/j.ijinfomgt.2020.102157>
- Rimler, J. (1999). A munka jövője. *Közgazdasági Szemle*, 9, 772–788.

- Röder, A., Ward, M., & Frese, C.-A. (2018). From Labour Migrant to Stay-at-Home Mother? Childcare and Return to Work among Migrant Mothers from the EU Accession Countries in Ireland. *Work, Employment & Society*, 32(5), 850–867. <https://doi.org/10.1177/0950017017713953>
- Ruiz-Quintanilla, S., & England, G. (1996). How working is defined: Structure and stability, *Journal of Organizational Behaviour*, 17, 515–540. <http://www.jstor.org/stable/3000375>
- Sherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353–400. <https://doi.org/10.2139/ssrn.2609777>
- Szekeres, B. (2021). *Munkajogoninnen – munkaviszonytúl*. Miskolc: Bíbor Kiadó.
- Szép, K., & Sík, E. (2001). A háztartási termelés pénzértéke. *Statisztikai Szemle*, 7, 596–612.
- Terhoeven, J., Tegtmeier, P., & Wischniewski, S. (2022). Human-centred work design in times of digital change – work conditions, level of digitization and recent trends for object-related tasks. *Procedia CIRP*, 107, 302–307. <https://doi.org/10.1016/j.procir.2022.04.049>
- Török, E. (2014). *Munka és társadalom – A munka jelentésváltozásai a bér munkán innen és túl*. Budapest: L'Harmattan Kiadó.
- Tyutyuryukov, V., & Guseva, N. (2021). From remote work to digital nomads: tax issues and tax opportunities of digital lifestyle. *IFAC-PapersOnLine*, 54(13), 188–193. <https://doi.org/10.1016/j.ifacol.2021.10.443>
- Venkatesh, A. V. (1992). An Emerging Distributed Work Arrangement: An Investigation of Computer-Based Supplemental Work at Home. *Management Science*, 38(12), 1687–1706. <https://doi.org/10.1287/mnsc.38.12.1687>
- Vincenti, G. (1942). *A munka magánjogi szabályai*. Budapest: Grill Károly Könyvkiadó.
- Yao, Q. M., Baker, L. T., & Lohrke, F. T. (2022). Building and sustaining trust in remote work by platform-dependent entrepreneurs on digital labor platforms: Toward an integrative framework. *Journal of Business Research*, 149, 327–339. <https://doi.org/10.1016/j.jbusres.2022.05.046>
- Zapf, D., & Holz, M. (2006). On the positive and negative effects of emotion work in organizations. *European Journal of Work and Organizational Psychology* Volum, 1, 1–28. <https://doi.org/10.1080/13594320500412199>

Сведения об авторах



София Рицу – аспирант кафедры аграрного и трудового права, Университет Мишкольца

Адрес: Университетский городок, г. Мишколец, Венгрия

E-mail: jogriczu@uni-miskolc.hu

ORCID ID: <https://orcid.org/0000-0002-4024-5833>



Габор Мелипатаки – доцент, профессор кафедры аграрного и трудового права, Университет Мишкольца

Адрес: Университетский городок, г. Мишколец, Венгрия

E-mail: jogmega@uni-miskolc.hu

ORCID ID: <https://orcid.org/0000-0002-0359-6538>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/226288>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57220559340>

Google Scholar ID: https://scholar.google.ru/citations?user=ivnh_csAAAAJ



Дэвид Адриан Мате – аспирант кафедры аграрного и трудового права, Университет Мишкольца

Адрес: Университетский городок, г. Мишколец, Венгрия

E-mail: jogmate@dot.com

ORCID ID: <https://orcid.org/0000-0001-7995-6707>

Вклад авторов

Авторы внесли равный вклад в создание статьи, а именно:

Введение – Габор Мелипатаки, София Рицу; разработка концепции работы – София Рицу, Габор Мелипатаки; «Цифровые эффекты и приверженность к трудовому праву» – Дэвид Адриан Мате, Габор Мелипатаки; Выводы – Габор Мелипатаки, Дэвид Адриан Мате, София Рицу.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Финансирование:

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 12 ноября 2022 г.

Дата одобрения после рецензирования – 18 января 2023 г.

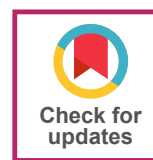
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.7>



Concepts of Work: from Traditional Social-Labor Ideas to Modern Effects of Digital Transformation

Zsofia Riczu  

University of Miskolc
Miskolc, Hungary

Gabor Melypataki 

University of Miskolc
Miskolc, Hungary

David Adrian Mate 

University of Miskolc
Miskolc, Hungary

Keywords

Atypical work,
concept of work,
definition of work,
digitization,
importance of work,
social legal challenges,
social policy

Abstract

Objective: technology and digitalization play a converse role in these two fields of study of criminal sciences. On the one hand, they are used by agencies of criminal justice system in order to control, manage and prevent crime and criminals. On the other hand, criminals enjoy technology in carrying out their plans to commit crime. Thus, from the criminal sciences' perspective, technology may be used or misused, and this is an interesting topic, and at the same time, an important research area for criminologists.

Methods: the present article seeks to provide a descriptive-analytical discussion about digitalization of criminology and criminal justice in the light of modern technologies, internet and cyberspace. It introduces new areas and sub-disciplines including administrative criminology based upon actuarial justice and risk management/assessment theory, cyber criminology and cyber victimology, as two sub-disciplines of the new century, and algorithmic or computational criminology, as one of the latest area in criminal sciences, which all are influenced by digitalization and technology.

Results: authors concluded that due to the digitalization atypical work emerges but legislator defines the scope of work regulated by law and that makes atypical work relationship becomes a typical work relationship.

© Riczu Zs., Melypataki G., Mate D. 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.

At the same time some areas fall into the gray zone. To fix that legislator should provide an interpretation that will not become empty in a year or two due to technological changes.

Scientific novelty: the applicability of technology and digitalization in criminology and criminal justice has widely increased and developed, specifically since the beginning of the third millennium.

Practical significance: digitalization and Technology has become increasingly important to criminology and criminal justice at both the theory and practice within the sphere of social and criminal sciences. The nature and types of crime and criminals, and also the methods and mechanisms of control and preventing them in the light of requirements of criminal policy and criminal justice are highly dependent upon technology and digitalization.

For citation

Riczu, Zs., Melypataki, G., Mate, D. A. (2023). Concepts of Work: from Traditional Social-Labor Ideas to Modern Effects of Digital Transformation. *Journal of Digital Technologies and Law*, 1(1), 175–190. <https://doi.org/10.21202/jdtl.2023.7>

References

- Bamel, U., Kumar, S., Lim, W. M., Bamel, N., & Meyer, N. (2022). Managing the dark side of digitalization in the future of work: A fuzzy TISM approach. *Journal of Innovation & Knowledge*, 7(4), 100275. <https://doi.org/10.1016/j.jik.2022.100275>
- Benotsmane, R., Dudás, L., & Kovács, G. (2020). Simulation and trajectory optimization of collaborating robots by application of solidworks and matlab software in industry 4.0. *Academic Journal of Manufacturing Engineering*, 18(4), 191–197.
- Brief, A. P.-N. (1990). Work and meaning: definitions and interpretations. In A. P.-N. Brief, *Meanings of occupational work: A collection of essays*. Lexington, MA: Lexington Books.
- Definition of “Work” for Purposes of Section 3304(a)(7) of the Federal Unemployment Tax Act. (n.d.). https://oui.doleta.gov/dmstree/uipl/uipl92/uipl_1892.htm#:~:text=In%20General,for%20which%20remuneration%20is%20payable
- Dorschel, R. (2022). Reconsidering digital labour: bringing tech workers into the debate. *New Technology, Work and Employment*, 37(2), 288–307. <https://doi.org/10.1111/ntwe.12225>
- Gerber, C. (2022). Gender and precarity in platform work: Old inequalities in the new world of work. *New Technologies, Work and Employment*, 37(2), 206–230. <https://doi.org/10.1111/ntwe.12233>
- Graeber, D. (2019). *Bullshit works*. Simon & Schuster.
- Horváth, I., Pérez del Prado, D., Petrovics, Z., & Sitzia, A. (2021). The Role of Digitisation in Employment and Its New Challenges for Labour Law Regulation: The Hungarian, Italian and Spanish Solutions, Comparison, and Criticism. *ELTE Law Journal*, 2, 101–132. <https://doi.org/10.54148/eltelj.2021.2.101>
- Hunt, K. & Annandale, E. (2008). Just the job? Is the relationship between health and domestic and paid work gender-specific? *Sociology of Health & Illness*, 15(5), 632–664. <https://doi.org/10.1111/1467-9566.ep11434424>
- Jakab, N. (2018). Systematic thinking on employee status. *Lex et Scientia*, 25(2), 56–68.
- Laky, T. (1998). *Változó fogalmak a munka változó világában*. *Közgazdasági Szemle*, 45(2), 123–136.
- Lee, B.-Y. (2022). Neither Employee nor Contractor: A Case Study of Employment Relations between Riders and Platform-Based Food-Delivery Firms in Taiwan. *Work, Employment and Society*, 095001702211031. <https://doi.org/10.1177/09500170221103147>
- Mann, M., & Chang, C. (2015). Work-Family Issues. In *The Encyclopedia of Adulthood and Aging* (pp. 1–5). <https://doi.org/10.1002/9781118521373.wbeaa197>

- Murphy, E. C., & Oesch, D. (2018). Is Employment Polarisation Inevitable? Occupational Change in Ireland and Switzerland, 1970–2010. *Work, Employment and Society*, 32(6), 1099–1117. <https://doi.org/10.1177/0950017017738944>
- Oberländer, M., & Bipp, T. (2022). Do digital competencies and social support boost work engagement during the COVID-19 pandemic? *Computers in Human Behavior*, 130, 107172. <https://doi.org/10.1016/j.chb.2021.107172>
- Orlikowski, W. J., & Scott, S. V. (2021). Liminal innovation in practice: Understanding the reconfiguration of digital work in crisis. *Information and Organization*, 31(1), 100336. <https://doi.org/10.1016/j.infoandorg.2021.100336>
- Pahl, R. E. (1988). *On Work: Historical, Comparative and Theoretical Approaches*. New York: Basil Blackwell.
- Prugberger, T. (2018). A jogkövetkezményeket érintő problémák a munkaszerződés egyes hibatípusainál. *Debreceni Jogi Műhely*, 15(3–4), 19–26. <https://doi.org/10.24169/djm/2018/3-4/3>
- Prugberger, T. (2020). Az atipikus szolgálati/munkaszerződések jogdogmatikai és rendszerezésbeli kérdései, különös hangsúllyal a munkaerőpiac legújabb igényeire. *Miskolci Jogi Szemle*, 2, 44–66.
- Quey, R. (1968). Toward a Definition of Work. *The Personnel and Guidance Journal*, 47(3), 223–227. <https://doi.org/10.1002/j.2164-4918.1968.tb02920.x>
- Rácz, I. (2021). Platform munkavégzés Magyarországon Munkajogi és egyéb jogági dilemmák. *Magyar Munkajog E-folyóirat*, 1, 1–15.
- Rahrovani, Y. (2020). Platform drifting: When work digitalization hijacks its spirit. *The Journal of Strategic Information Systems*, 29(2), 101615. <https://doi.org/10.1016/j.jsis.2020.101615>
- Richter, A. (2020). Locked-down digital work. *International Journal of Information Management*, 55, 102157. <https://doi.org/10.1016/j.ijinfomgt.2020.102157>
- Rimler, J. (1999). A munka jövője. *Közgazdasági Szemle*, 9, 772–788.
- Röder, A., Ward, M., & Frese, C.-A. (2018). From Labour Migrant to Stay-at-Home Mother? Childcare and Return to Work among Migrant Mothers from the EU Accession Countries in Ireland. *Work, Employment & Society*, 32(5), 850–867. <https://doi.org/10.1177/0950017017713953>
- Ruiz-Quintanilla, S., & England, G. (1996). How working is defined: Structure and stability. *Journal of Organizational Behaviour*, 17, 515–540. <http://www.jstor.org/stable/3000375>
- Sherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353–400. <https://doi.org/10.2139/ssrn.2609777>
- Szekeres, B. (2021). *Munkajogoninnen – munkaviszonytól*. Miskolc: Bíbor Kiadó.
- Szép, K., & Sík, E. (2001). A háztartási termelés pénzértéke. *Statistikai Szemle*, 7, 596–612.
- Terhoeven, J., Tegmeier, P., & Wischniewski, S. (2022). Human-centred work design in times of digital change – work conditions, level of digitization and recent trends for object-related tasks. *Procedia CIRP*, 107, 302–307. <https://doi.org/10.1016/j.procir.2022.04.049>
- Török, E. (2014). *Munka és társadalom – A munka jelentésváltozásai a bér munkán innen és túl*. Budapest: L'Harmattan Kiadó.
- Tyutyuryukov, V., & Guseva, N. (2021). From remote work to digital nomads: tax issues and tax opportunities of digital lifestyle. *IFAC-PapersOnLine*, 54(13), 188–193. <https://doi.org/10.1016/j.ifacol.2021.10.443>
- Venkatesh, A. V. (1992). An Emerging Distributed Work Arrangement: An Investigation of Computer-Based Supplemental Work at Home. *Management Science*, 38(12), 1687–1706. <https://doi.org/10.1287/mnsc.38.12.1687>
- Vincenti, G. (1942). *A munka magánjogi szabályai*. Budapest: Grill Károly Könyvkiadó.
- Yao, Q. M., Baker, L. T., & Lohrke, F. T. (2022). Building and sustaining trust in remote work by platform-dependent entrepreneurs on digital labor platforms: Toward an integrative framework. *Journal of Business Research*, 149, 327–339. <https://doi.org/10.1016/j.jbusres.2022.05.046>
- Zapf, D., & Holz, M. (2006). On the positive and negative effects of emotion work in organizations. *European Journal of Work and Organizational Psychology* Volum, 1, 1–28. <https://doi.org/10.1080/13594320500412199>

Authors information



Zsolia Riczu – PhD candidate, University of Miskolc, Faculty of Law, Agricultural and Labour Law Department

Address: Miskolc-Egyetemváros, Miskolc, Hungary

E-mail: jogriczu@uni-miskolc.hu

ORCID ID: <https://orcid.org/0000-0002-4024-5833>



Gabor Melypataki – Assistant professor, University of Miskolc, Faculty of Law, Agricultural and Labour Law Department

Address: Miskolc-Egyetemváros, Miskolc, Hungary

E-mail: jogmega@uni-miskolc.hu

ORCID ID: <https://orcid.org/0000-0002-0359-6538>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/226288>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57220559340>

Google Scholar ID: https://scholar.google.ru/citations?user=ivnh_csAAAAJ



David Adrian Mate – PhD candidate, University of Miskolc, Faculty of Law, Agricultural and Labour Law Department

Address: Miskolc-Egyetemváros, Miskolc, Hungary

E-mail: jogmate@dot.com

ORCID ID: <https://orcid.org/0000-0001-7995-6707>

Authors' contributions

The authors participated equally in the preparation of the study as follows: Introduction – Gabor Melypataki, Zsolia Riczu; Expansion of the concept of work – Zsolia Riczu, Gabor Melypataki; Digital effects and labor law addiction – David Adrian Mate, Gabor Melypataki; Conclusions – Gabor Melypataki, David Adrian Mate, Zsolia Riczu.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – November 12, 2022

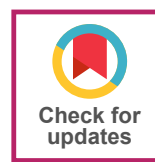
Date of approval – January 18, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научный обзор
УДК 346.62:004
EDN: <https://elibrary.ru/rcvuae>
DOI: <https://doi.org/10.21202/jdtl.2023.8>



Правовое регулирование отношений в сфере краудфандинга в Республике Беларусь

Андрей Витальевич Василевский 

Национальный центр законодательства и правовых исследований Республики Беларусь
г. Минск, Республика Беларусь

Ключевые слова

Договор,
законодательство,
краудинвестинг,
краудлендинг,
краудревординг,
краудфандинг,
право,
регулирование,
онлайн-финансирование,
цифровые технологии

Аннотация

Цель: изучение теоретико-правовых основ краудфандинга и разработка научно обоснованных предложений по совершенствованию законодательства Республики Беларусь в данной сфере.

Методы: методологическую основу исследования составляет система принципов, приемов и способов изучения общих закономерностей возникновения, становления и развития социально-правовых явлений. При выполнении исследования используются общие и частные методы научного познания: анализ, синтез, сравнительно-правовой, логический, системный, формально-юридический, диалектический и другие.

Результаты: проанализирована история появления и становления краудфандинга. Выявлены социально-экономические и технико-технологические факторы, способствующие популяризации краудфандинга среди пользователей сети Интернет. Рассмотрены происхождение понятия «краудфандинг» и наполнение его определенным смыслом. Обозначены разновидности краудфандинга в зависимости от цели вложения денежных средств лицами, осуществляющими финансирование. Установлен основной субъектный состав правоотношений при краудфандинге, состоящий из следующих лиц: соискатель финансирования; лицо, осуществляющее финансирование; оператор сервиса онлайн-финансирования. Представлен общий алгоритм правоотношений между основными субъектами краудфандинга. Охарактеризованы положительные и отрицательные аспекты краудфандинга. Обзорно проанализировано законодательство зарубежных государств на предмет правового регулирования краудфандинга. На основе проведенного анализа обозначены общие тренды развития законодательства в данной сфере. Рассмотрены программные и нормативные правовые акты по развитию краудфандинга в Республике Беларусь. Названы возможные договорные модели оформления правоотношений сторон. Определены технические и правовые требования к функционалу сервиса онлайн-финансирования.

© Василевский А. В., 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.

Предложен минимально необходимый комплекс мер по предупреждению рисков и угроз, связанных с привлечением и предоставлением денежных средств посредством сервиса онлайн-финансирования. На основании присущих оператору функций определены отдельные требования к содержанию правил сервиса онлайн-финансирования.

Научная новизна: комплексно исследованы понятие, правовая природа и особенности правового регулирования краудфандинга. Выявлены факторы, влияющие на формирование правовых норм, регулирующих привлечение и предоставление денежных средств с помощью сервисов онлайн-финансирования. Выработаны авторские предложения по совершенствованию законодательства Республики Беларусь в рассматриваемой сфере общественных отношений.

Практическая значимость: результаты научного исследования имеют значение для развития исследований в области гражданского, хозяйственного, информационного права. Полученные результаты могут применяться в процессе преподавания курса гражданского, хозяйственного, информационного права, использоваться субъектами права законодательной инициативы при разработке и внесении соответствующих законопроектов, а также выступать предметом дальнейших научных исследований по данной проблематике.

Для цитирования

Василевский, А. В. (2023). Правовое регулирование отношений в сфере краудфандинга в Республике Беларусь. *Journal of Digital Technologies and Law*, 1(1), 163–206. <https://doi.org/10.21202/jdtl.2023.8>

Содержание

Введение

1. Общие положения о краудфандинге
 - 1.1. История становления, понятие и признаки краудфандинга
 - 1.2. Виды краудфандинга
2. Правоотношения при краудфандинге
 - 2.1. Стороны
 - 2.2. Динамика общественных отношений сторон
3. Положительные и отрицательные аспекты краудфандинга
4. Правовое регулирование краудфандинга
 - 4.1. Опыт нормативного правового регулирования краудфандинга в зарубежных странах
 - 4.2. Опыт и перспективы нормативного правового регулирования краудфандинга в Республике Беларусь

Выводы

Список литературы

Введение

Вопросы доступа к финансам не теряют своей актуальности для физических лиц, стартапов, малого и среднего предпринимательства. Затруднения в привлечении необходимого объема финансирования особо остро ощущаются в высокорискованной инновационной сфере.

Долгие годы доминирующее положение в распределении финансовых потоков занимают банки. Как правило, данные кредитно-финансовые организации неохотно предоставляют крупные суммы заемных средств начинающим предпринимателям, поскольку опасаются невозврата средств. Такие опасения, по сложившейся практике, обусловлены тем, что энтузиасты, начинающие свое дело, берутся за реализацию весьма рискованных инициатив, зачастую не имея опыта предпринимательской деятельности, что нередко приводит к их экономической несостоятельности и банкротству созданных ими коммерческих юридических лиц (Armour & Enriques, 2018).

Бизнес-ангелы, венчурные фонды и другие небанковские кредитно-финансовые организации или спонсоры также оказывают финансовую помощь предпринимателям. Размер такой помощи варьируется и в ряде случаев сопоставим с размером заемных денежных средств, предоставляемых банками. Бизнес-ангелы чаще всего выделяют сравнительно небольшое количество средств для реализации понравившегося им проекта. Венчурные фонды, напротив, предоставляют значительные суммы средств, поскольку нацелены на более крупные проекты в конкретных секторах экономики. Такие фонды заинтересованы в высокой доходности за высокий риск вложения средств в частные инициативы, поэтому, как и банки, предъявляют ряд квалификационных требований к проектам и предпринимателям.

В целом наблюдаются тенденции по сокращению финансовых потоков и ужесточению квалификационных, экономических, организационных требований к участникам гражданского оборота при предоставлении им денежных средств. Складывающийся тренд обуславливается ведущимися санкционными экономическими войнами, экономической нестабильностью мировых рынков, вызванной распространением эпидемии и применением строгих карантинных мер, снижением темпов роста, а порой и вовсе кризисом отдельных отраслей экономики, сопровождающимся падением котировок сырьевых ресурсов на биржах и др.

В связи с изложенным альтернативные источники финансирования играют все более значимую роль в гражданском обороте, способствуя доступу к необходимому объему финансирования.

С развитием и распространением информационно-коммуникационных технологий изменилась среда коммуникации между людьми. Популярным способом финансирования стало предоставление средств через интернет-платформы. Появились специальные сайты и приложения в глобальной компьютерной сети Интернет, посредством которых физические или юридические лица, нуждающиеся в некой сумме денежных средств, имеют возможность обратиться за помощью не к традиционным кредитно-финансовым организациям, а к другим неравнодушным лицам. Такой способ финансовой коммуникации между лицами в сети Интернет широко известен под словесным обозначением «краудфандинг».

Простота, доступность и удобство привлечения и предоставления денежных средств с помощью финансовых онлайн-услуг стимулируют активное развитие и рост глобального рынка таких транзакций. В государствах принимаются нормативные

правовые акты, направленные на регулирование общественных отношений по отдельным видам краудфандинга. Необходимость принятия специального законодательства в данной сфере, по мнению экспертов, обосновывается тем, что отсутствие надлежащего правового регулирования краудфандинга «затрудняет разрешение возможных споров между участниками, создает предпосылки для ущемления прав и законных интересов потребителей таких финансовых услуг, осуществления незаконной предпринимательской деятельности, может способствовать появлению финансовых пирамид, случаев финансирования незаконной деятельности и т. д.» (Степура, 2021; Селява, 2021).

В СМИ достаточно много публикаций о том, что краудфандинг является инновационным механизмом финансирования (Парукова, 2020). Вместе с тем данный способ привлечения и предоставления денежных средств не настолько новый, каким его пытаются представить отдельные исследователи. Концепция сбора средств со всех заинтересованных лиц, положенная в основу краудфандинга, насчитывает не одно столетие (Каменков, 2022). Инновационность данному процессу придают используемые на современном этапе человеческого развития технологии, которые оказывают влияние на способ осуществления коммуникации между людьми. Принимая во внимание изложенное, в настоящем исследовании уместно вести речь не о новом механизме финансирования, а о новой среде либо новом способе коммуникации при осуществлении коллективного финансирования.

1. Общие положения о краудфандинге

1.1. История становления, понятие и признаки краудфандинга

Несмотря на относительно недавнее появление исследуемого способа коммуникации, «точную дату его применения для осуществления коллективного финансирования установить весьма затруднительно. Условно за нее можно принять 1997 г. Этот год примечателен тем, что поклонники британской рок-группы Marillion без какого-либо участия самой группы организовали и провели в Сети интернет-кампанию по сбору средств для финансирования музыкального тура исполнителей по всей территории США»¹.

Со временем идея привлечения и предоставления денежных средств при помощи специализированных сервисов онлайн-финансирования (сайтов и приложений) в сети Интернет нашла свое распространение. В 2001 г. ArtistShare стал первым сервисом в США, позволяющим поклонникам музыки финансово поддерживать творческие начинания исполнителей². В киноиндустрии краудфандинг впервые стал применяться с 2002 г., с запуском сайта FilmVenture.com³.

¹ Crowdfunding for enterprise (an examination of the crowdfunding landscape in Europe. (2016). <https://www.crucialcrowdfunding.com/wp-content/uploads/2017/05/CROWDFUNDING-FOR-ENTERPRISE-an-Examination-of-the-Crowdfunding-Landscape-in-Europe.pdf>

² ArtistShare. <https://www.artistshare.com/about>

³ FilmVenture. <https://web.archive.org/web/20021105143430/http://www.filmventure.com/fv/> (С апреля 2016 г. данный сайт не функционирует.)

На начало 2000-х гг. количество сервисов онлайн-финансирования насчитывало единицы. Положение дел изменилось к 2010 г. По оценкам «Всемирного банка, таких сервисов стало уже несколько сотен, причем большая их часть была сконцентрирована в США. Так, по состоянию на 2013 г. в США было представлено 344 сервиса онлайн-финансирования, в Великобритании – 87, во Франции – 53, Канаде и Нидерландах – по 34, Испании – 27, Германии – 26, Бразилии – 17, Италии – 15, Австралии – 12, Индии – 10, России и ЮАР – по 4 сервиса»⁴ (Василевский, 2020а).

Заметим, что на ранних этапах своего развития процесс привлечения и предоставления денежных средств посредством сервисов онлайн-финансирования не имел специального наименования, термин «краудфандинг» вошел в обиход рядового пользователя сети Интернет значительно позже.

В целях изучения правового регулирования общественных отношений в сфере краудфандинга необходимо обратиться к этимологии данного понятия, а также изучить наполнение его определенным смыслом в соответствующей области применения – сети Интернет, из которой термин был заимствован экономикой и юриспруденцией.

Применяемый неологизм является транслитерацией на русский язык английского слова crowdfunding. Термин crowdfunding образован от двух слов: crowd – «толпа» и funding – «финансирование», что в дословном переводе на русский язык обозначает «народное финансирование». В последнее время под краудфандингом все чаще понимают онлайн-финансирование.

Авторство названного термина принадлежит Майклу Салливану (англ. Michael Sullivan). В 2006 г. в сети Интернет им был запущен сервис Fundavlog, основной целью которого, по замыслу создателя, была помощь в финансировании проектов видеоблогеров, в создании таких материалов, как новые веб-шоу, документальные фильмы и пр.⁵ Проект Fundavlog вобрал в себя достижения ранее запущенного М. Салливаном сайта vlogdir.com, специализировавшегося на видеоблогах, а также содержал ряд дополнительных функций, в числе которых для настоящего исследования представляет интерес возможность при нажатии соответствующей кнопки на сайте профинансировать то либо иное понравившееся пользователю видео. Сумма взносов была ранжирована и указана на кнопках сайта, среди которых основная – 1 цент за клик. Проект Fundavlog был интересен общественности, однако не нашел своего последующего продолжения и развития.

В интервью «Das Crowdfunding Magazin» М. Салливан отметил, что на первых этапах разработки Fundavlog он пытался найти новый термин, который мог бы более полно отразить общественные процессы по софинансированию проектов, технические механизмы которых были предложены как на созданном им, так и в ряде других функционирующих на то время сервисов⁶. В своем блоге

⁴ Crowdfunding's Potential for the Developing World. <https://documents1.worldbank.org/curated/en/409841468327411701/pdf/840000WP0Box380crowdfunding0study00.pdf>

⁵ Справочно следует отметить, что на то время проекты по созданию видеохостингов активно прорабатывались многими разработчиками программного обеспечения, например, популярный ныне видеохостинг YouTube был основан в 2005 г.

⁶ Crowdfunding-Wortschöpfer Michael Sullivan im Interview. (2015, Oktober 28). <https://www.crowdfunding.de/magazin/crowdfunding-wortschoepfer-michael-sullivan-im-interview/>

о сервисе Fundavlog он назвал способ коммуникации лиц при осуществлении финансирования посредством программно-технических средств сервиса в сети Интернет термином «crowdfunding». Как заверяет сам автор, выбор данного термина был для него очевиден, поскольку в то время в обиходе популярными были понятия «crowd» и «crowdsourcing»⁷.

Термин «краудсорсинг» впервые был предложен в 2006 г. в статье «The Rise of Crowdsourcing» ежемесячного журнала «Wired» американским журналистом Джеффом Хауи (англ. Jeff Howe)⁸. По мнению Н. В. Михалевой, автор статьи вложил в данное понятие следующий смысл: «...для решения какой-либо проблемы на добровольных началах при помощи информационно-коммуникационных технологий привлекается неопределенное количество лиц, способных принять участие в ее решении» (Михалева, 2019).

После опубликования статьи Д. Хауи стал вплотную заниматься темой краудсорсинга, наблюдая и описывая это явление в своем блоге crowdsourcing.com. В последующем эти наблюдения были положены в основу монографии «Краудсорсинг: как сила толпы определяет будущее бизнеса» (англ. «Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business»), вышедшей в свет в 2008 г. В указанной работе посредством исторического метода исследования автор описал природу краудсорсинга. Истоки данного явления он видит в образовании «сообществ любителей» и связывает его развитие с появлением особого направления информационных технологий – открытого программного обеспечения, благодаря которому «любители» получили законный доступ к исходному коду программ и, более того, могли вносить в него правки, принимая тем самым участие в доработке открытого программного продукта. Краудфандинг в названной монографии упоминается лишь несколько раз в противопоставление краудсорсингу. Принципиальная разница между названными социальными процессами коммуникации заключается в том, что краудфандинг понимается как коллективное финансирование проекта, а не работа группы лиц над решением проблемы. Иными словами, данный способ реализации проекта предполагает не активное участие большинства, а их пассивное участие посредством предоставления финансирования. Общим для названных процессов, по мнению Д. Хауи, является то, что как краудсорсингу, так и краудфандингу присущ социальный интеграционный импульс, который позволяет уменьшить количество иерархических звеньев между людьми в решении проблемы или реализации проекта.

В поисковой системе Google первые запросы слова «crowdfunding» были сделаны пользователями только в 2007 г., причем до конца 2011 г. популярность запросов, по оценкам Google Trends, не превышала 10 баллов из 100 возможных⁹. В русскоязычном сегменте поисковой системы Google первое обращение к понятию «краудфандинг» датируется декабрем 2010 г. При этом динамика запросов русскоязычной

⁷ Fundavlog. <https://web.archive.org/web/20070224191008/http://fundavlog.com/community/index.php?op=ViewArticle&articleId=9&blogId=1>

⁸ The Rise of Crowdsourcing. (2006). <https://www.wired.com/2006/06/crowds/>

⁹ Google Trends. <https://trends.google.ru/trends/explore?date=all&q=rowdfunding>

версии термина примерно сопоставима с общими тенденциями поиска слова «crowdfunding»¹⁰.

Распространение в обиходе пользователей сети Интернет термина «crowdfunding» исследователи связывают с функционированием сервиса онлайн-финансирования Kickstarter¹¹. Согласно данным Google Trends, динамика истории запросов сервиса онлайн-финансирования Kickstarter схожа с поиском слова «crowdfunding»¹². С момента запуска (28 апреля 2009 г.) до времени проведения настоящего исследования (октябрь 2022 г.) названный сервис является одним из самых популярных сервисов онлайн-финансирования в мире. Посредством Kickstarter 21 млн человек приняли участие в финансировании, 6,3 млрд долл. США было собрано и 228 078 проектов успешно профинансировано¹³. С помощью Kickstarter финансируются разнообразные проекты в 15 категориях: игры, кино и видео, дизайн, технологические проекты, музыка, издательство, кулинария, искусство, мода, комиксы, театр, фото, танцы, ремесла, журналистика.

По имеющимся на октябрь 2022 г. статистическим данным, на сервисе Kickstarter наибольшее количество успешно профинансированных проектов относится к категориям «музыка» – 33 713 проектов, «кино и видео» – 30 964, «игры» – 32 781. По сумме вложенных средств лидируют проекты из категории «игры» – 2,53 млрд долл. США.

Популяризации краудфандинга в целом способствовала совокупность факторов, среди которых основными являются нижеследующие.

В первую очередь это экономический кризис 2007–2008 гг. В этот период традиционные финансовые институты в лице банков и небанковских кредитно-финансовых организаций приняли меры по минимизации риска невозврата средств. Значительно уменьшилось финансирование стартапов, малого и среднего предпринимательства¹⁴. Ужесточились квалификационные требования к участникам гражданского оборота при предоставлении им заемных средств на запрашиваемые цели¹⁵. Кроме этого, повысились процентные ставки по кредитам и займам.

Экономическая нестабильность привела к росту числа граждан среднего и пожилого возраста, вовлеченных в предпринимательскую деятельность. Основной целью в организации такого вида самозанятости стало сохранение существующего до кризиса уровня доходов. По мнению экспертов, успех предпринимательской деятельности указанной социально-демографической группы связан с тем, что люди старшей возрастной категории обладают более широкими общественными связями.

¹⁰ Google Trends. <https://trends.google.ru/trends/explore?q=краудфандинг>. Занимательным фактом является то, что среди стран, представляющих русскоязычный сегмент сети Интернет, максимально частое обращение к поиску понятия «краудфандинг» наблюдается в Беларуси.

¹¹ A social history of crowdfunding. (2011). <https://socialmediaweek.org/blog/2011/12/a-social-history-of-crowdfunding/>

¹² Google Trends. <https://trends.google.ru/trends/explore?date=all&q=kickstarter>

¹³ Kickstarter. <https://www.kickstarter.com/about?ref=global-footer>

¹⁴ Banking on each other (Peer-to-peer lending to business: Evidence from Funding Circle). https://media.nesta.org.uk/documents/banking_on_each_other.pdf

¹⁵ The Rise of Future Finance: The UK Alternative Finance Benchmarking Report. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/the-rise-of-future-finance/>

Указанное способствует в поиске финансирования от большего количества друзей и знакомых¹⁶ (Cai et al., 2021).

Развитию краудфандинга также способствовали существующие в мире социальные барьеры. Доступ к финансовым ресурсам в ряде стран ограничивается по признаку пола, расы или другим некоммерческим факторам.

Согласно зарубежным исследованиям, инвесторы (спонсоры) предпочитают вкладывать средства в проекты, инициаторы (соискатели финансирования) которых соответствуют им по полу, расе и социально-экономическому статусу (Duan et al., 2020). Соискатели финансирования, не относящиеся к данной социально-демографической группе, в большинстве случаев оказываются вне рынка венчурного и ангельского финансирования.

Совокупность обозначенных экономических, организационно-процедурных, социальных обременений и барьеров, связанных с получением денежных средств от традиционных институтов, стимулировало соискателей финансирования к поиску альтернативных источников привлечения денежных средств. При анализе возможных вариантов наиболее простой и результативный – сбор денежных средств со всех лиц, тем или иным образом заинтересованных в реализации проекта. Такой способ привлечения средств не является новым, неоднократно применялся на практике и подтвердил свою экономическую эффективность.

С прогрессивным развитием и обширным распространением информационно-коммуникационных технологий «масштабы, скорость и доступность социальных контактов вышли на качественно новый уровень, стало возможным в режиме реального времени взаимодействие с большим числом заинтересованных лиц вне зависимости от их географического местонахождения. Наряду с этим у рядовых пользователей банковских услуг появилась возможность удаленного и оперативного осуществления финансовых транзакций. Наличие такого технического потенциала способствовало оптимизации издержек на распространение информации о проекте и организации сбора денежных средств посредством сервисов онлайн-финансирования» (Василевский, 2020а).

Весомый вклад в информационное освещение проектов вносят интернет-средства массовой коммуникации (такие как YouTube, TikTok, «ВКонтакте», «Одноклассники», Twitter*, Viber, Telegram и другие видеохостинги, социальные сети, мессенджеры и пр.). Каждый из потенциальных инвесторов (спонсоров) обладает доступом к таким источникам информации через смартфон, компьютер, ноутбук. Эти гаджеты и доступ в сеть Интернет стали неотъемлемой частью социальной жизни человека. За внимание пользователя к проекту в сети Интернет разворачивается конкурентная борьба (выпускается качественный и популярный («хайповый») материал («контент»), набираются подписчики, ставятся лайки и пр.) (Wang et al., 2020; Wolfe et al., 2021; Bi et al., 2017). Интернет-СМИ способствуют своего рода трансформации социального капитала в финансовый и позволяют обойти стороной «бюрократическую», «переборчивую в финансировании проектов» цепь традиционных посредников.

Предложенное словесное обозначение «краудфандинг» (народное финансирование) всецело отражает сущность происходящих на первых этапах становления

¹⁶ Gabison, Garry A. (2015). *Understanding Crowdfunding and its Regulations*. <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC92482/lbna26992enn.pdf>

анализируемого способа коммуникации процессов по привлечению и предоставлению денежных средств посредством специализированных сервисов онлайн-финансирования в сети Интернет. В этот период времени в преобладающем большинстве случаев финансирование привлекалось на реализацию каких-либо творческих, благотворительных инициатив (к примеру, запись альбома; организация концерта; помощь людям, оказавшимся в трудной жизненной ситуации, и пр.). В экономике такая модель финансирования известна как модель кредитования между физическими лицами (одноранговая модель) (англ. peer-to-peer lending, сокр. обозначение – P2P).

Вместе с тем следует принимать во внимание, что приведенное терминологическое обозначение общественных процессов по привлечению и предоставлению денежных средств посредством сервисов онлайн-финансирования не является единственно возможным. Например, Кембриджский центр альтернативных финансов (англ. Cambridge Centre for Alternative Finance), а также ряд других институтов и экономистов оперируют более общим понятием – «(интерактивные) альтернативные финансы» (англ. (online) alternative finance). Применение данного обозначения логически обусловлено тем, что рассматриваемый способ осуществления финансирования противопоставляется традиционным способам (к примеру, таким, как получение кредитов, займов, грантов и пр.). Наряду с этим в зарубежном законодательстве для целей правового регулирования применяются и иные правовые категории, к примеру «инвестиции, привлеченные посредством инвестиционных платформ» и др.

С усложнением и расширением диапазона используемых на сервисах онлайн-финансирования финансовых инструментов трансформировался и контекст понимания термина «краудфандинг». В частности, состоявшимся фактом следует признать значимое участие в краудфандинге квалифицированных инвесторов, а также набирающую оборот межкорпоративную схему финансирования (англ. business to business, сокр. обозначение – B2B), применение которой на данный момент вызывает во многих национальных правовых порядках ряд теоретико-правовых вопросов, требующих нормативного разрешения.

Сегодня понятие «краудфандинг» носит зонтичное (общее) значение для различного рода бизнес-моделей коллективного финансирования в сети Интернет. Несмотря на многообразие таких бизнес-моделей, им присущи некоторые общие черты, позволяющие отнести их к краудфандингу. А. Голикова, проанализировав подходы отечественных и зарубежных экономистов, выделяет следующие основные признаки краудфандинга:

«1) сбор денежных средств осуществляется посредством сервиса онлайн-финансирования в сети Интернет и специального посредника – организации, деятельность которой связана с предоставлением услуг сервиса онлайн-финансирования (оператор сервиса онлайн-финансирования);

2) оператор сервиса онлайн-финансирования не относится к категории банков или иных традиционных финансовых учреждений;

3) оператор сервиса онлайн-финансирования не вкладывает собственные средства в поддержание какого-либо краудпроекта, размещенного на его сервисе онлайн-финансирования;

4) система взносов ранжирована и доступна каждому пользователю;

5) финансирование одного краудпроекта осуществляется за счет перечислений от большого количества участников» (Голикова, 2019).

На основании сказанного можно сделать вывод о том, что под краудфандингом следует понимать способ привлечения и предоставления денежных средств в сети Интернет для финансирования проектов. Такое финансирование чаще всего осуществляется небольшими суммами денежных средств от множества заинтересованных участников гражданского оборота. При этом оператор сервиса онлайн-финансирования, как правило, не относится к традиционным финансовым институтам в лице банков и небанковских кредитно-финансовых организаций.

1.2. Виды краудфандинга

В большинстве научно-популярных публикаций термин «краудфандинг» представляет собой собирательную категорию четырех основных бизнес-моделей коллективного финансирования: благотворительный краудфандинг, краудревординг (также известен в публикациях под наименованием «наградной краудфандинг»), краудлендинг и краудинвестинг. В то же время данный подход не является общепризнанным. В частности, во многих публикациях краудлендинг не рассматривается как компонент краудфандинга (Ткачев, Баталко, 2018; Lihn, 2019).

В юридической и экономической литературе приводятся многочисленные основания для классификации краудфандинга. основополагающей для целей правового регулирования повсеместно признается классификация в зависимости от цели вложения денежных средств. По данному основанию различают коммерческие и некоммерческие виды краудфандинга (Василевский, 2020b; Shneor et al., 2023).

Коммерческий краудфандинг основан на вложении лицами денежных средств в целях получения прибыли (доходов) или достижения иного значимого результата, связанного с осуществлением предпринимательской деятельности. В литературе коммерческий краудфандинг причисляют к одному из способов инвестирования (Усеня, 2019).

К коммерческим видам краудфандинга относят:

- краудинвестинг (англ. equity-based crowdfunding, crowdfinvesting, investment-based crowdfunding) – форма онлайн-финансирования хозяйственных обществ малого и среднего предпринимательства посредством приобретения инвесторами эмиссионных ценных бумаг этих обществ. Инвесторы, принимая участие в данном виде коммерческого краудфандинга, получают дивиденды по приобретенным эмиссионным ценным бумагам и разделяют с соискателем финансирования риски предпринимательской деятельности в части потенциальной потери вложенных денежных средств. Заметим, что в целях ускоренного развития бизнеса соискателя финансирования в правоприменении распространена практика, в соответствии с которой инвесторам не выплачиваются дивиденды либо их размер незначителен. В связи с этим большинство инвесторов в долгосрочной перспективе рассчитывают на капитализацию хозяйственного общества соискателя финансирования и последующую перепродажу на фондовой бирже по более высокой стоимости по сравнению с понесенными затратами принадлежащих им эмиссионных ценных бумаг финансируемого хозяйственного общества. Для инвесторов краудинвестинг отличается повышенной степенью риска, поскольку получение прибыли и ее размер слабо прогнозируемы и зависят от множества неконтролируемых им факторов (Lukkarinen, 2020);

– краудлендинг (англ. lending-based crowdfunding, credit-based crowdfunding, loan-based crowdfunding, crowdlending) – форма онлайн-финансирования физических и (или) юридических лиц посредством предоставления инвесторами краткосрочных коммерческих займов (Усеня, 2020). В отличие от краудинвестинга прибыль инвесторов при данном виде краудфандинга прогнозируема и формируется за счет уплаты соискателями инвестиций по договорам займа процентов, размер которых согласован сторонами или установлен на сервисе онлайн-финансирования.

Некоммерческий краудфандинг основан на вложении денежных средств для социальных, личных, бытовых, семейных и иных целей, прямо не связанных с извлечением прибыли (дохода).

Выделяют следующие виды некоммерческого краудфандинга:

– краудревординг (англ. crowdrewording) – форма онлайн-финансирования производителей товаров или лиц, оказывающих услуги, посредством предоставления потребителями денежных средств взамен на вознаграждение в виде рекламы, продукта или услуги, финансирование которых осуществляется (Zhao & Ryu, 2020);

– благотворительный краудфандинг (англ. donation crowdfunding), фандрайзинг (англ. fundraising) – форма онлайн-финансирования, при которой спонсоры безвозмездно предоставляют денежные средства на реализацию социально значимого проекта.

В целях формирования представлений об объеме каждого из представленных выше видов краудфандинга на рис. 1 приведены соответствующие статистические данные рынка альтернативного финансирования в Европе (без учета Великобритании) за 2020 г.

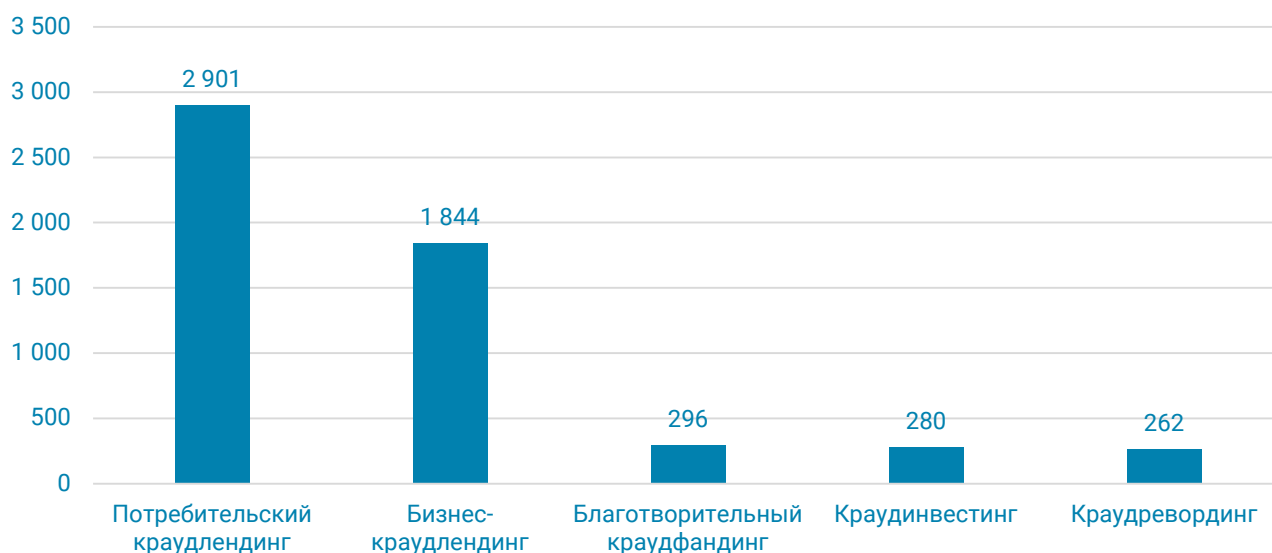


Рисунок 1. Общий объем рынка альтернативного финансирования в Европе (без учета Великобритании) в 2020 г. по видам краудфандинга (млн долл. США)

Источник: *Total value of the alternative finance market in Europe (excluding the UK) in 2020.* (2022).

<https://www.statista.com/statistics/412394/europe-alternative-finance-transaction-value-market-segment/>

Тенденции последних пяти лет на рынке альтернативного финансирования в Европе (без учета Великобритании) по видам краудфандинга продемонстрированы на рис. 2.

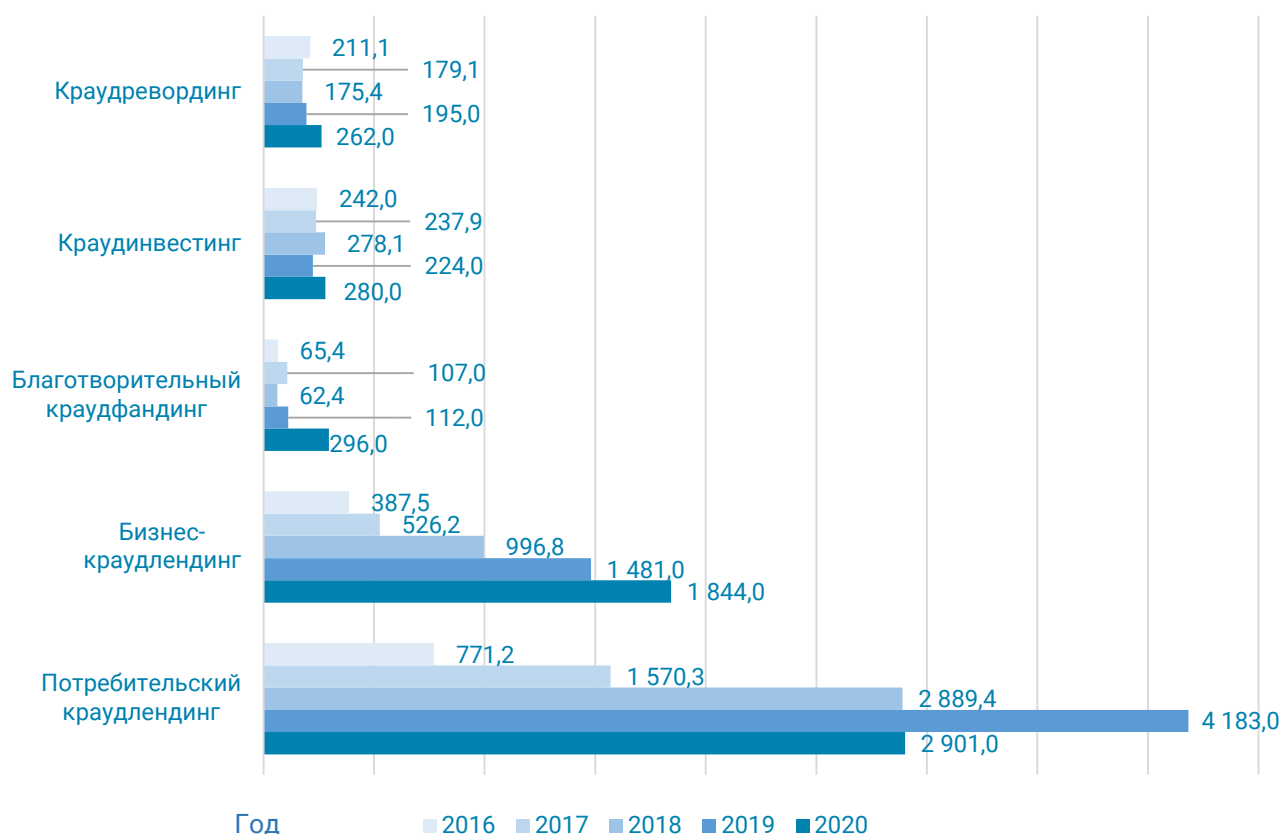


Рисунок 2. Общий объем рынка альтернативного финансирования в Европе (без учета Великобритании) за период 2016–2020 гг. по видам краудфандинга (млн долл. США)

Источник: *Peer-to-peer consumer and business lending transaction value in Europe (excluding the UK) from 2014 to 2020. (2022).* <https://www.statista.com/statistics/412400/europe-alternative-finance-transaction-value-p2p-lending/>; *Equity-based crowdfunding transaction value in Europe (excluding the UK) from 2013 to 2020. (2022).* <https://www.statista.com/statistics/412460/europe-alternative-finance-transaction-value-equity-crowdfunding/>; *Donation-based crowdfunding transaction value in Europe (excluding the UK) from 2015 to 2020. (2022).* <https://www.statista.com/statistics/412463/europe-alternative-finance-transaction-value-donation-crowdfunding/>

Представленные статистические данные отчетливо свидетельствуют, что по объему привлекаемых денежных средств доминирующее положение на рынке альтернативного финансирования в Европе занимает краудлендинг, далее со значительным разрывом следуют другие виды краудфандинга. В целом аналогичные тренды характерны для всего рынка альтернативного финансирования в мире.

2. Правоотношения при краудфандинге

2.1. Стороны

Общественные отношения по привлечению и предоставлению денежных средств с использованием сервисов онлайн-финансирования вне зависимости от их вида возникают, изменяются и прекращаются между тремя основными и необходимыми участниками.

1. Соискатель финансирования, фандрайзер (англ. fundraisers) или инициатор (создатель) проекта (англ. projectscreators) – физическое или юридическое лицо (как правило, человек, нуждающийся в помощи; начинающий предприниматель

(«стартапер»); субъект малого или среднего бизнеса), заинтересованное в привлечении денежных средств на реализацию какой-либо цели.

2. Лицо, осуществляющее финансирование (англ. funders) – физическое и (или) юридическое лицо, предоставляющее на возмездной или безвозмездной основе денежные средства соискателю финансирования на реализацию какого-либо проекта. В зависимости от вида краудфандинга они именуется:

- даритель, спонсор, благотворитель или жертвователь (англ. donors) – при благотворительном краудфандинге;
- потенциальный покупатель (англ. prebuyers), спонсор или бэкер (англ. backers) – при краудревординге;
- заимодавец (англ. lenders) – при краудлендинге;
- инвестор (англ. investors) – при краудинвестинге.

Подчеркнем, что в благотворительном краудфандинге лица, осуществляющие финансирование, не являются инвесторами, так как они не вкладывают денежные средства в актив в надежде на то, что его стоимость со временем увеличится на рынке.

3. Оператор сервиса онлайн-финансирования – юридическое лицо, оказывающее соискателям финансирования и лицам, осуществляющим финансирование, соответственно услуги по содействию в привлечении или предоставлении денежных средств.

Круг лиц, участвующих в общественных отношениях краудфандинга, не ограничивается представленными выше субъектами. Так, например, на стороне соискателя финансирования могут выступать также агенты или организаторы конкурса по привлечению денежных средств; в некоммерческом краудфандинге наряду с оператором сервиса онлайн-финансирования, как правило, участвуют лица, способствующие привлечению средств на безвозмездной основе (волонтеры) и др.

2.2. Динамика общественных отношений сторон

Общий алгоритм развития действий и правоотношений сторон при краудфандинге выглядит следующим образом:

а) соискатель финансирования в сети Интернет изучает правила сервисов онлайн-финансирования, репутацию сервисов среди пользователей, отзывы пользователей о функционировании сервисов и о деятельности операторов и др. На основании полученных сведений соискатель финансирования выбирает подходящий под преследуемые цели или реализуемый проект сервис онлайн-финансирования, проходит на нем регистрацию и заполняет заявку на привлечение денежных средств, на основе которой сервисом генерируется предложение по привлечению денежных средств. В зависимости от вида краудфандинга и конкретного сервиса онлайн-финансирования отличаются поля, подлежащие заполнению в заявке. С учетом общей для соискателей финансирования во всех видах краудфандинга цели, заключающейся в привлечении денежных средств, такого рода заявки в большинстве случаев содержат следующие широко распространенные поля для заполнения сведений:

- максимальный объем (общая сумма) привлекаемых денежных средств;
- минимальный объем денежных средств заинтересованного в финансировании лица, достижение которого является необходимым условием для заключения договора по предоставлению денежных средств;
- срок привлечения денежных средств;
- цель привлечения денежных средств либо информация о проекте, на реализацию которого привлекаются денежные средства, и др.

Кроме того, в правилах сервиса онлайн-финансирования может быть предусмотрено, что соискатель обязан прикрепить к заявке необходимые скан-копии подтверждающих документов;

б) оператор сервиса онлайн-финансирования на основании информации, полученной из регистрационной формы и заявки на привлечение денежных средств, осуществляет предварительную оценку соискателя финансирования и предложенного им проекта (при наличии). Оценка проводится оператором сервиса онлайн-финансирования в соответствии с самостоятельно определенными критериями и методиками, подлежащими равным образом применению ко всем соискателям, с учетом особенностей преследуемых ими целей или реализуемых проектов. По итогам проведенной оценки оператор принимает решение об одобрении заявки соискателя финансирования и размещении на сервисе онлайн-финансирования предложения по привлечению денежных средств либо об отклонении такой заявки с мотивированным обоснованием причин. Оператор обязан уведомить соискателя о принятом решении посредством сервиса онлайн-финансирования. Срок уведомления устанавливается в правилах сервиса онлайн-финансирования и исчисляется с момента направления соискателем финансирования заявки на привлечение денежных средств;

в) пользователи сети Интернет, среди которых лица, заинтересованные в осуществлении финансирования, изучив имеющиеся на сервисе онлайн-финансирования активные предложения по привлечению денежных средств, принимают решение о финансировании заинтересовавшего их проекта (Boudreau et al., 2021). В целях получения дополнительной информации о соискателе финансирования и о его предложении, а также для заключения договора по предоставлению денежных средств (далее – договор финансирования) пользователи проходят регистрацию на сервисе онлайн-финансирования;

г) посредством сервиса онлайн-финансирования лицо, желающее профинансировать заинтересовавшее его предложение, заключает с соответствующим соискателем финансирования на возмездной либо безвозмездной основе, в зависимости от вида краудфандинга, договор финансирования. Во исполнение заключенного договора заинтересованное в осуществлении финансирования лицо перечисляет установленную в предложении либо согласованную сторонами сумму денежных средств на счет соискателя финансирования;

д) информацию обо всех фактах, относящихся к исполнению или прекращению договора финансирования, заключенного посредством сервиса онлайн-финансирования, стороны обязаны фиксировать на этом сервисе.

Правоотношения сторон краудфандинга для наглядности продемонстрированы в виде условной схемы на рис. 3.

Как можем заметить из представленных выше алгоритма и схемы, оператор сервиса онлайн-финансирования имеет ключевое значение в организации краудфандинга. Оператор, во-первых, осуществляет администрирование сервиса онлайн-финансирования, без которого краудфандинг как явление не существует, во-вторых, оказывает посреднические услуги по привлечению и содействию в предоставлении денежных средств, т. е. участвует в соединении спроса и предложений, и, наконец, в-третьих, обеспечивает функционирование сервиса онлайн-финансирования для заключения, исполнения и прекращения договорных правоотношений между соискателем финансирования и лицом, осуществляющим финансирование.

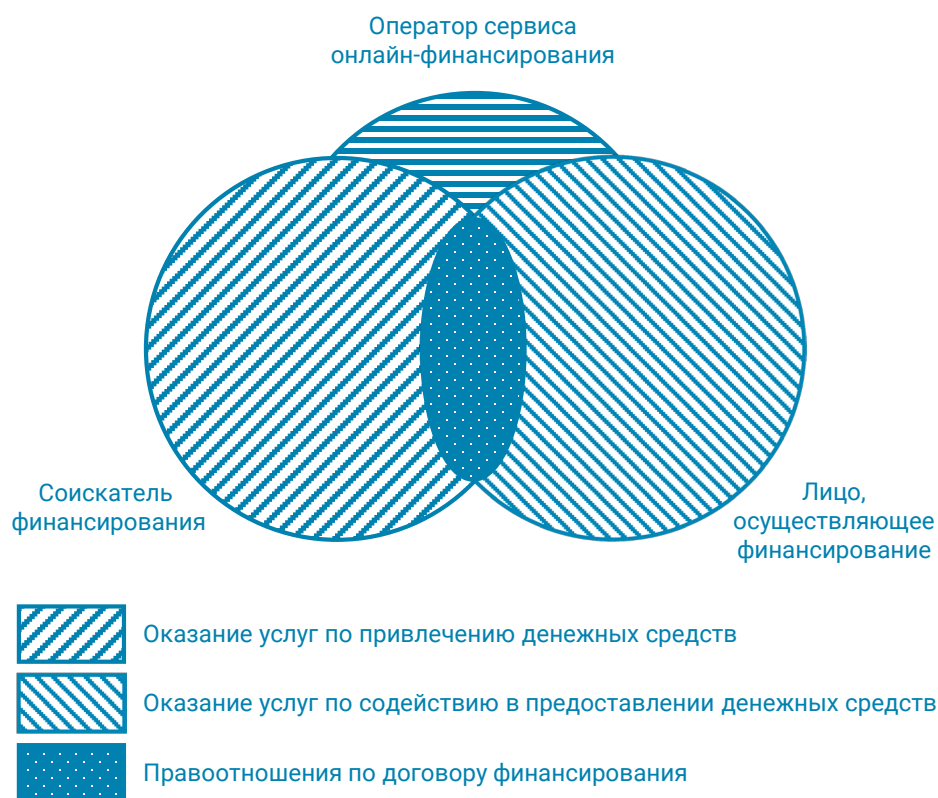


Рисунок 3. Правоотношения лица, осуществляющего финансирование, соискателя финансирования и оператора сервиса онлайн-финансирования при краудфандинге¹⁷

Источник: составлено автором.

Сервис онлайн-финансирования представляет собой техническо-программное решение, «специализированный интернет-ресурс, на котором размещаются крауд-проекты» (Горовая, 2016), или «веб-сайт, посвященный сбору денежных средств посредством краудфандинга» (Gedda et al., 2016)¹⁸. Сервис выступает своего рода посреднической площадкой (инструментом) для взаимодействия лиц, заинтересованных в привлечении денежных средств для достижения какой-либо цели, и лиц, готовых профинансировать достижение этой цели (Вишнякова, 2018). Сервис онлайн-финансирования является постоянным элементом экосистемы краудфан-

¹⁷ На рис. 3 круги условно обозначают субъектов краудфандинга. В целях индивидуализации субъектов круги подписаны и изображены с использованием различных способов оформления: круг «оператор сервиса онлайн-финансирования» заштрихован горизонтальными линиями; круг «соискатель финансирования» заштрихован косыми линиями с наклоном вправо; круг «лицо, осуществляющее финансирование» заштрихован косыми линиями с наклоном влево. Область пересечения кругов демонстрирует правоотношения сторон при краудфандинге: пересечение круга «оператор сервиса онлайн-финансирования» с кругом «соискатель финансирования» или кругом «лицо, осуществляющее финансирование», соответственно обозначает правоотношения оказания услуг по привлечению или содействию в предоставлении денежных средств; пересечение всех трех кругов – правоотношения по заключению, исполнению и прекращению договора финансирования посредством сервиса онлайн-финансирования.

¹⁸ В Республике Беларусь функционируют различные сервисы онлайн-финансирования как для коммерческого, так и некоммерческого краудфандинга. Например, Maesens.by осуществлял свою деятельность с 2011 по 2018 г.; <https://www.talaka.org> запущен в 2013 г.; <https://dev.investo.by> запущен в 2015 г.; <https://unihelp.by> запущен в 2016 г. и др.

динга, что придает его участникам чувство уверенности в безопасности реализуемых правоотношений. Информационное наполнение сервиса онлайн-финансирования о проекте способствует активному привлечению денежных средств. На платформе зачастую указывается информация о сумме уже собранных средств и о количестве лиц, принявших участие в финансировании. Потенциальные инвесторы (спонсоры) склонны вкладывать свои денежные средства в проект, пользующийся поддержкой множества лиц. Срабатывает социально-психологический эффект «мудрости толпы», согласно которому люди учитывают результаты коллективного мышления при принятии собственного решения (Mollick & Nanda, 2016). Немаловажное значение при этом имеет и модель сбора средств, которая применяется на сервисе онлайн-финансирования. Большинство сервисов используют модель «все или ничего», при которой денежные средства, собранные на реализацию проекта, предоставляются соискателю финансирования только в том случае, если достигнуто пороговое значение заявленной при регистрации проекта необходимой суммы. По такой модели оператор сервиса онлайн-финансирования аккумулирует собираемые денежные средства сперва на своих счетах. При недостижении в установленный срок пороговой суммы денежных средств, необходимой на финансирование проекта, оператор сервиса возвращает денежные средства лицам, их предоставившим.

Деятельность операторов сервисов онлайн-финансирования различается в зависимости от страны, с учетом применяемого законодательства. Некоторые операторы проводят предварительную оценку проектов, другие просто собирают заявителей и заинтересованные стороны, а некоторые, наоборот, выступают в качестве единственного акционера финансируемого проекта (Щетинина, 2016).

Операторы сервиса онлайн-финансирования заинтересованы в том, чтобы их сервис имел безупречную репутацию и не ассоциировался у пользователей сети Интернет с мошенническими или некачественными (безуспешными) проектами. Связано это с конкурентной борьбой между операторами за внимание потенциальных соискателей финансирования и инвесторов (спонсоров) к предлагаемому ими сервису.

Во многих случаях, если соискателю финансирования удастся привлечь денежные средства, оператор услуги по сбору средств взимает плату за свою деятельность, которая варьируется в зависимости от территориального (географического) расположения оператора, уровня конкуренции и используемой бизнес-модели краудфандинга.

3. Положительные и отрицательные аспекты краудфандинга

Привлечение и предоставление денежных средств посредством сервисов онлайн-финансирования характеризуются широким спектром положительных аспектов, в числе которых можно выделить следующие.

Восполняется дефицит финансирования проекта без сложных квалификационных требований к соискателю финансирования. Соискатели финансирования могут настроить бизнес-модель краудфандинга, исходя из особенностей реализуемого ими проекта, а также организационного и финансового положения. Иными словами, соискатели финансирования, применяющие краудфандинг, имеют больше «рычагов» контроля и настройки финансирования, нежели при получении средств от традиционных финансовых институтов.

Трансграничность финансовых потоков. Проект финансируют люди и организации со всего мира, при этом их количество не ограничено. Трансграничность

позволяет соискателям финансирования в случае успешного сбора денежных средств выходить на новые рынки.

В экономический оборот «привлекаются ресурсы граждан, которые по отдельности не являются достаточными для ведения хоть сколько-нибудь полезной деятельности, но в совокупности образуют весьма значительные суммы, которые можно было бы пустить на развитие рынка в различных отраслях, что особенно актуально в условиях экономической нестабильности» (Клинов, 2018).

Соискатели финансирования сохраняют контроль над проектом, что позволяет им дорабатывать и улучшать его в период сбора денежных средств, учитывая критические замечания общественности.

Соискатели финансирования могут проанализировать конъюнктуру рынка на предмет востребованности предлагаемого ими продукта. Кроме того, при успешном сборе денежных средств соискатели финансирования получают гарантированных потребителей выпускаемой продукции из числа лиц, профинансировавших проект.

В рамках сбора денежных средств происходит своего рода социальное страхование. Данный аспект особо актуален для высокорискованных инновационных проектов. Краудфандинг позволяет привлекать незначительные суммы средств от большого количества лиц, каждое из которых разделяет предпринимательский риск в части возможной потери внесенного им вклада, не рискуя при этом большим состоянием.

Зачастую краудфандинг дополняет традиционные источники финансирования. Вместе с тем в ряде случаев он также значительно облегчает доступ к ним. Банкам, небанковским кредитно-финансовым организациям и сообществам проще оценить потенциал идеи, возможные риски и заинтересованность соискателя финансирования в успехе проекта, если проект уже находится на стадии реализации. В большинстве случаев при последующем привлечении денежных средств традиционные финансовые институты принимают положительное решение о предоставлении финансирования в развитие такого проекта. Заинтересованность потенциальных инвесторов в финансировании перспективных инновационных проектов, находящихся на стадии реализации, растет в геометрической прогрессии. Одним из ярких примеров такой практики является инновационный проект по созданию шлема (очков) виртуальной реальности Oculus Rift. Сбор средств на реализацию данного проекта был запущен 1 августа 2012 г. на платформе Kickstarter, соискателями финансирования для сбора была заявлена сумма денежных средств в размере 250 тыс. долл. США. Всего за месяц от 9 522 лиц было собрано 2,4 млн долл. США¹⁹. Спустя несколько лет, 25 марта 2014 г., компания Oculus VR (являющаяся разработчиком указанного проекта) была приобретена Facebook^{**} за 2 млрд долл. США²⁰. Менее чем за два года капитализация компании – разработчика проекта выросла более чем в 20 раз, причем началу данного процесса способствовал краудфандинг.

Таким образом, заинтересованность соискателей финансирования в краудфандинге очевидна. В свою очередь потенциальные инвесторы (спонсоры) и потребители

¹⁹ Oculus Rift: Step Into the Game. (2016). <https://www.kickstarter.com/projects/1523379957/oculus-rift-step-into-the-game>

²⁰ Facebook Buying Oculus Virtual-Reality Company for \$2 Billion. <https://time.com/37842/facebook-oculus-rift/>

заинтересованы в краудфандинге, поскольку получают доступ к новым продуктам, прежде чем те станут широко коммерциализированы.

В то же время краудфандинг не лишен недостатков.

Мошенничество представляет наибольшую угрозу. Традиционные репутационные и правоприменительные методы и средства не всегда эффективны. Соискатели финансирования не являются постоянными субъектами экосистемы краудфандинга. Поэтому в ряде случаев они не дорожат безупречностью своей деловой репутации (Karpoff, 2021). Лица, предоставляющие денежные средства, в свою очередь не обладают достаточной заинтересованностью в предъявлении иска о мошенничестве или нарушении договора финансирования со стороны недобросовестного соискателя финансирования. Связано это с тем, что основной идеей краудфандинга является сбор небольших сумм со многих лиц вместо крупных вложений с ограниченного числа субъектов. Незначительный размер потери внесенного вклада не стимулирует отдельное лицо к участию в дорогостоящем, затянутом во времени судебном разбирательстве. В связи с этим лица, предоставляющие денежные средства в краудфандинге, наиболее подвержены рискам мошенничества.

В противодействии мошенничеству активную роль играют операторы сервисов онлайн-финансирования, которые проводят комплексную проверку проекта и применяют ряд превентивных мер оценки его качества (Ferreira et al., 2022). Например, зачастую для этих целей используется модель финансирования «все или ничего» и др. Значительный вклад в противодействие мошенничеству вносят также лица, предоставляющие денежные средства, исходя из имеющихся у каждого знаний и аналитических способностей, срабатывает отмеченный выше эффект «мудрости толпы». Кроме того, лица, предоставляющие денежные средства, могут нивелировать обозначенные выше риски путем ограничения и диверсификации финансовых потоков. Иными словами, вкладывать небольшие средства в различные проекты.

Наряду с намеренным мошенничеством существуют риски непреднамеренного провала проекта. Неудача может постигнуть проект в силу различных причин, например, некомпетентности и самонадеянности соискателей финансирования, экономической неэффективности проекта, технических просчетов, неблагоприятного изменения внешних факторов (экономический, сырьевой, производственный кризис; обстоятельства непреодолимой силы (форс-мажор)) и пр.

Отсутствие развитого фондового рынка не способствует продвижению бизнес-моделей краудфандинга, в основу которых положена собственность на уставной фонд финансируемого хозяйственного общества. Инвесторы в таких бизнес-моделях зачастую рассчитывают на получение прибыли, посредством последующей реализации части ранее приобретенного в рамках краудфандинга уставного фонда. Если фондовый рынок недостаточно развит, то инвесторы лишены такой возможности получения прибыли и, соответственно, не заинтересованы в осуществлении инвестиций таким образом.

Что касается налогообложения, то во многих странах распространенной практикой является предоставление налоговых льгот субъектам налогообложения при финансировании ими некоммерческих организаций. Такие же налоговые льготы хотели бы иметь и спонсоры, осуществляющие финансирование некоммерческих проектов посредством краудфандинга. Однако, поскольку операторы сервиса онлайн-финансирования, аккумулирующие денежные средства, во многих случаях являются коммерческими организациями, спонсоры формально-юридически не обладают правами на такие льготы. Кроме того, в ряде стран налоговые льготы варьируются в зависимости от того, за счет каких средств (прибыли, основного капитала либо заемных)

предприятие финансирует свои исследования и разработки. Такие расхождения налоговых режимов оказывают влияние на спрос финансирования, предпочтения инвесторов (спонсоров), соискателей финансирования в способе привлечения, предоставления денежных средств и, соответственно, на то, как развивается краудфандинг.

В ряде стран правовому регулированию краудфандинга уделяется недостаточное внимание, что создает дополнительные риски гарантий и безопасности общественных отношений. Наряду с регулятивной функцией нормы права также выполняют и просветительную (информационную) функцию для участников гражданского оборота.

Краудфандинг подходит «не для всех», ввиду того что для успешного привлечения средств на реализацию проекта от соискателей финансирования, как правило, требуется инновационный подход, маркетинговые навыки, информационная грамотность, креативность и пр. В случае если соискатели финансирования в недостаточной степени владеют вышеназванными компетенциями, они могут воспользоваться консалтинговыми услугами специалистов по продвижению проектов в сети Интернет. Такие услуги в том числе могут оказывать операторы сервисов онлайн-финансирования.

В довершение всего существуют риски в сфере интеллектуальной собственности. Соискателям финансирования в целях успешного привлечения денежных средств необходимо раскрывать значительный объем информации о проекте. В случае отсутствия соответствующих правоохранных документов интеллектуальной собственности представленную информацию могут присвоить себе недобросовестные участники гражданского оборота (Ерш, 2021).

4. Правовое регулирование краудфандинга

С учетом обозначенных выше положительных и отрицательных аспектов краудфандинга перед регулирующими органами государств мира возникает ряд вопросов, требующих нормативного разрешения (Sanderson et al., 2022). Среди таких вопросов можно выделить следующие основные. Кто вправе осуществлять деятельность оператора сервиса онлайн-финансирования? Какие квалификационные требования следует предъявлять к операторам сервисов онлайн-финансирования? Какие модели краудфандинга вправе применяться? Кто вправе предоставлять денежные средства посредством сервисов онлайн-финансирования? Какой размер денежных средств вправе предоставлять одно лицо в целом? Кто вправе принимать денежные средства? Какую сумму денежных средств соискатели финансирования вправе привлекать для реализации проекта? Как часто они вправе это делать?

Генеральный вектор развития правового регулирования общественных отношений, складывающихся при краудфандинге, намечен в международных актах об электронной коммерции. Положения данных актов носят рекомендательный характер для участников делового оборота и государств. Принимаются такие акты различными международными организациями, в числе которых наиболее влиятельны Организация Объединенных Наций (далее – ООН)²¹, Всемирная торговая организация

²¹ ООН. Типовой закон об электронной торговле Комиссии Организации Объединенных Наций по праву международной торговли. https://www.un.org/ru/documents/decl_conv/conventions/commerce.shtml

(далее – ВТО)²², Организация по экономическому сотрудничеству и развитию (далее – ОЭСР)²³ и др. В понимании «электронной коммерции» сегодня не наблюдается единства. Превалирует подход ВТО и ОЭСР, согласно которому «электронную коммерцию» рассматривают как совокупность отношений по заключению сделок с помощью предназначенных специально для этого средств. Таковыми выступают как сами информационно-телекоммуникационные сети, в частности сеть Интернет, так и иные средства, например, специализированные сайты, мобильные приложения. При этом из понятия электронной коммерции исключаются сделки, заключенные посредством телефонного звонка, телекса, факса, а также обычной электронной почты (Савельев, 2016).

4.1. Опыт нормативного правового регулирования краудфандинга в зарубежных странах

В большинстве государств правовое регулирование краудфандинга дифференцировано в зависимости от применяемой бизнес-модели. Некоммерческий краудфандинг зачастую упорядочен в положениях общегражданского законодательства, в то время как коммерческие бизнес-модели краудфандинга имеют обособленное нормативное регулирование.

В числе первых специальных правовых актов, регулирующих правоотношения лиц по коммерческому привлечению и предоставлению денежных средств посредством сервисов онлайн-финансирования, следует отметить Закон США 2012 г. «О бизнес-стартапах» (англ. Jumpstart Our Business Startups Act, сокр. JOBS Act)²⁴. В преамбуле к названному закону отмечено, что представленные в нем положения призваны увеличить количество рабочих мест в Америке и обеспечить экономический рост за счет улучшения доступа к публичным (общественным) рынкам капитала для начинающих, развивающихся предприятий. Раздел III JOBS Act неофициально известен как «Закон о краудфандинге» (англ. Crowdfund Act). Правовые положения названного раздела на момент принятия весьма прогрессивны. Закрепляется возможность субъектов хозяйствования использовать бизнес-модели краудфандинга, основанные на обращении ценных бумаг. Притом что финансовый рынок США долгие годы до этого был более чем консервативен и зарегулирован. Несмотря на принятие акта, его практическая реализация участниками гражданского оборота стала возможной значительно позже. В 2015 г. Комиссией по ценным бумагам и биржам США (англ. The United States Securities and Exchange Commission, сокр. – SEC) принимается соответствующий нормативный акт, развивающий положения раздела III JOBS Act. Акт вступил в силу 16 мая 2016 г.²⁵, после чего субъекты хозяйствования

²² WTO. *E-Commerce in Developing Countries: Opportunities and Challenges for Small and Medium-Sized Business*. https://www.wto.org/english/res_e/booksp_e/ecom_brochure_e.pdf

²³ OECD. *OECD Glossary of Statistical Terms. Electronic Commerce*. <https://stats.oecd.org/glossary/detail.asp?ID=4721>

²⁴ *Jumpstart Our Business Startups Act*. <https://www.govinfo.gov/content/pkg/BILLS-112hr3606enr/pdf/BILLS-112hr3606enr.pdf>

²⁵ *Regulation Crowdfunding*. (2016). <https://www.sec.gov/rules/final/2015/33-9974.pdf>

США смогли в полной мере легально применять финансовые бизнес-модели краудфандинга (La Viña & Black, 2018).

Представленное правовое регулирование вызвало резонанс в мировой деловой общественности. Интерес к этой теме прежде всего обусловлен первенством США в нормативном регулировании рассматриваемой сферы общественных отношений, а также статусом США как одной из ведущих экономик, определяющей в числе прочих равных стран вектор развития мировых рынков.

В последующем специальное нормативное регулирование краудфандинга было принято и в других государствах. Например, в Итальянской Республике в 2012 г. была принята новая редакция Декрета «О дальнейших неотложных мерах экономического развития Италии» (итал. Decreto-legge «Ulteriori misure urgenti per la crescita del Paese») ²⁶, придавшая нормативному правовому акту статус закона ²⁷, содержащего среди прочих норм положения о краудфандинге для инновационных предприятий; во Французской Республике в 2014 г. – Декрет «О краудфандинге» (фр. Ordonnance relative au financement participatif) ²⁸; в Австрийской Республике в 2015 г. – Федеральный закон «Об альтернативных формах финансирования» (нем. Bundesgesetz über alternative Finanzierungsformen (Alternativfinanzierungsgesetz – AltFG)) ²⁹; в Федеративной Республике Германия в 2015 г. – Федеральный закон «О защите “малых” инвесторов» (нем. Kleinanlegerschutzgesetz) ³⁰ (Odorović & Wenzlaff, 2020); в Российской Федерации в 2019 г. – Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» ³¹ и др. ³²

В силу стремления государств – членов ЕАЭС к гармонизации гражданского законодательства особый интерес для Республики Беларусь представляет опыт нормативного регулирования рассматриваемых общественных отношений в Российской Федерации.

В России 1 января 2020 г. вступил в силу Федеральный закон от 2 августа 2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ

²⁶ Decreto-legge 18 ottobre 2012, № 179 «Ulteriori misure urgenti per la crescita del Paese». <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012-10-18;179!vig=>

²⁷ Executive Summary of the new Italian legislation on innovative startups. https://www.mise.gov.it/images/stories/documenti/Executive_Summary_Italy_Startup_Act_02_05_2016.pdf

²⁸ Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029008408/>

²⁹ Bundesgesetz über alternative Finanzierungsformen (Alternativfinanzierungsgesetz – AltFG). <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009241>

³⁰ Kleinanlegerschutzgesetz. https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/18_Legislaturperiode/2015-07-10-Kleinanlegerschutzgesetz/0-Gesetz.html

³¹ О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации. № 259-ФЗ. (2019). https://www.consultant.ru/document/cons_doc_LAW_330652/

³² Правовые акты приведены для обозначения основ начального (первичного) правового регулирования отношений в сфере краудфандинга в отдельных государствах мира. К настоящему времени объем правового регулирования рассматриваемой сферы общественных отношений в правовом порядке данных стран значительно шире нормативного содержания обозначенных выше актов.

и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон № 259). Во время рассмотрения вышеуказанного федерального закона в Государственной Думе³³ акт имел иное название – «Об альтернативных способах привлечения инвестиций (краудфандинге)». Как предполагается, «причиной к изменению названия послужило то, что указанный закон призван регулировать не весь краудфандинг в целом, а только коммерческий...»³⁴ В пользу данной версии свидетельствуют положения п. 5 ч. 1 ст. 2 и ст. 5 Закона № 259, из которых следует, что нормативно урегулирован сбор средств на цели, связанные с осуществлением соискателями финансирования прежде всего предпринимательской деятельности. В свою очередь, некоммерческий краудфандинг находится вне сферы правового регулирования данного нормативного правового акта.

В положениях Закона № 259 предлагаются следующие основные группы правовых актов, призванных регулировать отношения сторон при краудфандинге.

1. Правила инвестиционной платформы – организационный акт оператора инвестиционной платформы, определяющий основные условия ее работы: правила авторизации, требования к инвесторам и реципиентам и т. д. (ст. 4 Закона № 259).

2. Договоры об оказании услуг, заключаемые между оператором инвестиционной платформы с одной стороны и инвесторами или соискателями инвестиций с другой. Посредством заключения указанных договоров соответственно обеспечивается доступ соискателей инвестиций и инвесторов к участию в краудфандинге (ст. 3 Закона № 259).

3. Договор, заключаемый между инвестором и соискателем инвестиций. Эта часть отношений сторон краудфандинга является наиболее дискуссионной, поскольку ряд договорных схем полностью не укладывается в классические модели договоров, урегулированные законодательством, прежде всего Гражданским кодексом Российской Федерации.

В ст. 5 Закона № 259 указаны способы инвестирования с использованием инвестиционной платформы: 1) предоставление займов; 2) приобретение эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы, за исключением эмиссионных ценных бумаг кредитных организаций, некредитных финансовых организаций, а также структурных облигаций и предназначенных для квалифицированных инвесторов ценных бумаг; 3) приобретение утилитарных цифровых прав.

В целях формирования представлений о возможных векторах развития законодательства Республики Беларусь, направленного на упорядочивание рассматриваемой сферы общественных отношений, лаконично представим основные нормативные требования, предъявляемые к участникам экосистемы краудфандинга.

В законодательстве зарубежных государств наметились следующие тенденции по установлению квалификационных требований к лицам, претендующим осуществлять деятельность оператора сервиса онлайн-финансирования:

- регистрация в качестве юридического лица;
- положительная деловая репутация учредителей (участников) и представителей органов управления юридического лица;

³³ О привлечении инвестиций с использованием инвестиционных платформ: проект федерального закона Российской Федерации, № 419090-7. (2018). <https://sozd.duma.gov.ru/bill/419090-7>

³⁴ Краудфандинг: понятие, правовое регулирование и договорные конструкции: на основе материала В. Э. Поляковой. <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=117866#uDYA3KTqUGIETuLs>

– наличие специального разрешения на осуществление деятельности оператора сервиса онлайн-финансирования. Во многих юрисдикциях совершение административных процедур по выдаче соответствующих разрешений входит в компетенцию министерства финансов либо национального банка государства. Заметим, что данное требование в превалирующем большинстве государств является обязательным в отношении операторов, применяющих краудинвестинг. Связано это со спецификой правового режима обороноспособности ценных бумаг. При этом получение соответствующего разрешения (лицензии), как правило, происходит по упрощенной процедуре в сравнении с общим разрешительным (лицензионным) порядком;

– принятие организационно-технических мер по сбору и проверке данных о соискателях финансирования и предлагаемых к финансированию проектов (при наличии);

– принятие превентивных мер по противодействию мошенничеству, в числе которых предоставление лицам, планирующим осуществлять финансирование, всесторонней, разрешенной в соответствии с законодательством информации о соискателе финансирования и его проекте, на который осуществляется сбор средств;

– применение мер по противодействию легализации средств, добытых преступным путем, и финансированию террористических организаций и др.

В качестве примера установления квалификационных требований к операторам сервисов онлайн-финансирования как к ключевым субъектам экосистемы краудфандинга приведем опыт нормотворческой деятельности Французской Республики. Выбор данного правового порядка основан на том, что законодательство Франции – одно из немногих, в котором представлено регулирование деятельности операторов сервисов онлайн-финансирования, применяющих как коммерческие, так и некоммерческие виды краудфандинга (Sannajust et al., 2014). В национальном сегменте правоотношений краудфандинга Франции соответственно различают два правовых статуса оператора сервиса онлайн-финансирования: CIP – «советник краудфандинговых инвестиций» (фр. conseil en investissement participatif), который вправе оказывать посреднические услуги по коммерческим видам краудфандинга, и IFP – «инвестиционный посредник в краудфандинге» (фр. intermédiaire en financement participatif), имеющий право оказывать посреднические услуги по некоммерческим видам краудфандинга. Выбор операторами правового статуса зависит от спектра финансовых и консультационных услуг, которые они готовы предложить соискателям финансирования и лицам, осуществляющим финансирование.

CIP – оператор сервиса онлайн-финансирования должен соответствовать следующим требованиям:

– являться юридическим лицом, созданным во Франции;

– быть зарегистрированным в системе ORIAS (база данных посредников в осуществлении банковских операций и платежных услуг);

– предоставлять гарантии своей деятельности;

– быть членом аккредитованного представительства Autorité des Marchés Financiers, сокр. AMF³⁵ (если оператор сервиса онлайн-финансирования не является членом AMF, то в отношении его осуществляются специальные процедуры контроля)³⁶;

³⁵ Autorité des Marchés Financiers – государственный орган, регулирующий рынок ценных бумаг во Франции.

³⁶ General regulation of the Autorité Des Marchés Financiers. <https://reglement-general.amf-france.org/eli/fr/aai/amf/rg/20161218/en.pdf>

- застраховать свою деятельность (минимальная гарантированная сумма по страховому полису должна составлять 400 тыс. евро за каждый страховой случай возмещения ущерба и 800 тыс. евро ежегодно);
- соблюдать нормативные предписания Валютно-финансового кодекса Франции (фр. Code monétaire et financier, сокр. CMF)³⁷ и Положения о AMF;
- обеспечивать защиту интересов пользователей, предоставлять всестороннюю информацию для оценки рисков при осуществлении финансирования;
- на стадии регистрации в системе ORIAS предъявляются и другие институциональные требования.

Для приобретения статуса IFP-оператор сервиса онлайн-финансирования должен:

- являться юридическим лицом. По сравнению с требованиями к CIP, не обязательно созданным во Франции (допускается деятельность иностранных представительств);
- быть зарегистрированным в системе ORIAS;
- застраховать свою деятельность (минимальная гарантированная сумма по страховому полису должна составлять 250 тыс. евро за каждый страховой случай возмещения ущерба и 500 тыс. евро ежегодно, а в отношении операторов сервисов онлайн-финансирования, ориентированных исключительно на благотворительность, – 100 тыс. и 200 тыс. евро соответственно);
- соблюдать нормативные предписания Валютно-финансового кодекса Франции (фр. CMF).

В случае если IFP-операторы сервисов онлайн-финансирования оказывают услуги по переводу средств между соискателем финансирования и лицом, осуществляющим финансирование, тем самым выступая своего рода платежными учреждениями, также необходимо иметь разрешение ACPR и лицензию платежного учреждения (фр. Prestataire de Services de Paiement), получаемую в упрощенном порядке. Для получения названной лицензии размер уставного капитала оператора сервиса онлайн-финансирования должен составлять не менее 40 тыс. евро.

Таким образом, следует констатировать, что во Франции закреплён широкий спектр квалификационных и институциональных требований, предъявляемых к операторам сервисов онлайн-финансирования. Наличие таких нормативных цензов способствует повышению качества оказываемых операторами услуг и является своего рода гарантией надлежащей защиты интересов сторон правоотношений краудфандинга.

В отношении соискателей финансирования наиболее распространены нормативные предписания, устанавливающие:

- лимиты по объёму привлекаемых денежных средств в течение 12-месячного периода, либо календарного года;
- институциональные требования (организационно-правовая форма, вид осуществляемой деятельности; размер уставного фонда и др.).

К примеру, в США общая сумма финансирования, привлечённая посредством краудфандинга для реализации проекта, не должна превышать 1,07 млн долл. США, во Франции – 1 млн евро, в России – 1 млрд рублей и т. д. В Италии инициировать

³⁷ Code monétaire et financier. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072026/2019-05-24/

сбор средств на реализацию проекта вправе только инновационные организации. В России по данному аспекту правовое регулирование исходит от обратного, в законодательстве определены критерии субъектов, которым не допускается привлекать денежные средства через сервисы онлайн-финансирования. В законодательстве государств мира к соискателям финансирования могут предъявляться и иные нормативные требования.

В отдельных правовых актах специальные квалификационные требования предъявляются также к лицам, осуществляющим финансирование. Например, в Италии для осуществления сбора средств на инновационный проект через сервисы онлайн-финансирования необходимо, чтобы не менее 5 % денежных средств поступило от профессиональных инвесторов. Данное требование основывается на возможности всесторонней оценки рисков того либо иного проекта профессиональными инвесторами и тем самым превентивной защиты от возможных имущественных потерь неквалифицированных участников гражданского оборота, желающих принять участие в финансировании³⁸. В США нормативно ограничен объем вкладываемых лицами денежных средств по всем регулируемым бизнес-моделям краудфандинга в течение 12-месячного периода. Так, если годовой доход и имеющиеся чистые активы лица в стоимостной оценке менее 107 тыс. долл. США, то лимит осуществления финансирования составляет 2 200 долл. США, или 5 % от наименьшей суммы годового дохода и имеющихся чистых активов. Если годовой доход и имеющиеся чистые активы лица равны или превышают 107 тыс. долл. США, то лимит соответственно равен 10 %. При этом в течение 12-месячного периода общая сумма ценных бумаг, приобретенных лицом через сервисы онлайн-финансирования, не должна превышать 107 тыс. долл. США, вне зависимости от годового дохода и имеющихся чистых активов³⁹. В России физические лица имеют право инвестировать через инвестиционные платформы денежные средства в сумме не более 600 тыс. рублей в течение одного календарного года.

4.2. Опыт и перспективы нормативного правового регулирования краудфандинга в Республике Беларусь

В Республике Беларусь институту краудфандинга уделяется пристальное внимание. В программных правовых актах по различным сферам и направлениям социально-экономического развития республики обозначены состояние и векторы дальнейшего развития краудфандинга в краткосрочной и среднесрочной перспективе:

– в Концепции информационной безопасности Республики Беларусь при характеристике гуманитарного аспекта текущего состояния информационной сферы констатируется широкое применение практики краудфандинга⁴⁰;

³⁸ Review of Crowdfunding Regulation. https://eurocrowd.org/wp-content/uploads/2022/02/ECN_Review_of_Crowdfunding_Regulation_2017.pdf

³⁹ Spotlight on Jumpstart Our Business Startups (JOBS) Act. <https://www.sec.gov/spotlight/jobs-act.shtml>

⁴⁰ О Концепции информационной безопасности Республики Беларусь. № 1. (2019). <https://pravo.by/document/?guid=3871&p0=P219s0001>

- в Государственной программе инновационного развития Республики Беларусь на 2016–2020 гг. предусмотрено развитие интернет-платформ (краудфандинга) в качестве инструмента взаимодействия потребителей и производителей товаров и услуг, инвесторов и соискателей инвестиций⁴¹;
- в Республиканской программе мероприятий по проведению в Республике Беларусь 2018–2020 гг. под знаком Года малой родины предусмотрена разработка проекта Указа Президента Республики Беларусь «О деятельности финансовых интернет-площадок» в целях расширения доступа физических и юридических лиц к финансовым ресурсам посредством интернет-площадок бизнес-финансирования⁴²;
- в Стратегии развития цифрового банкинга в Республике Беларусь на 2016–2020 гг. отдельным направлением цифровой трансформации рынка финансовых услуг определено создание организаций, предоставляющих альтернативные финансовые услуги, в том числе занимающихся разработкой инновационных программно-технических решений⁴³;
- в Стратегии развития финансового рынка Республики Беларусь до 2020 г.⁴⁴, а также в Стратегии развития малого и среднего предпринимательства «Беларусь – страна успешного предпринимательства» на период до 2030 г. предусмотрено формирование институциональных условий для развития системы небанковского финансирования⁴⁵;
- в Основных направлениях денежно-кредитной политики Республики Беларусь на 2021 г. запланировано расширение доступа физических и юридических лиц к заемным средствам через сервисы онлайн-заимствования⁴⁶;
- в Программе социально-экономического развития Республики Беларусь на 2021–2025 гг. предусмотрено: в сфере жилищно-коммунального хозяйства внедрение сервисов краудфандинга и краудинвестинга в цифровые платформы умных регионов, предоставляющих жителям возможность выбора вариантов благоустройства их придомовых участков; в финансовом секторе – расширение доступа физических и юридических лиц к заемным средствам через сервисы онлайн-заимствования⁴⁷;
- в Программе деятельности Правительства Республики Беларусь на период до 2025 г. предусмотрено правовое обеспечение института краудфандинга

⁴¹ О Государственной программе инновационного развития Республики Беларусь на 2016–2020 годы. № 31. (2017). <https://pravo.by/document/?guid=12551&p0=P31700031>

⁴² Постановление Совета Министров Республики Беларусь № 547 от 18 июля 2018 г. <https://pravo.by/document/?guid=12551&p0=C21800547&p1=1>

⁴³ Постановление Правления Национального банка Республики Беларусь № 108 от 2 марта 2016 г. <https://www.nbrb.by/legislation/documents/pp108.pdf>

⁴⁴ Постановление Совета Министров Республики Беларусь, Национального банка Республики Беларусь № 229/6 от 28 марта 2017 г. <https://pravo.by/document/?guid=3871&p0=C21700229>

⁴⁵ Постановление Совета Министров Республики Беларусь № 743 от 17 октября 2018 г. <https://pravo.by/document/?guid=3871&p0=C21800743>

⁴⁶ Об утверждении Основных направлений денежно-кредитной политики Республики Беларусь на 2021 год: Указ Президента Республики Беларусь от 22 декабря 2020 г. № 481. <https://pravo.by/document/?guid=12551&p0=P32000481&p1=1>

⁴⁷ Об утверждении Программы социально-экономического развития Республики Беларусь на 2021–2025 годы: Указ Президента Республики Беларусь от 29 июля 2021 г. № 292. <https://pravo.by/document/?guid=3871&p0=P32100292>

в целях облегчения доступа субъектов малого и среднего предпринимательства к финансированию⁴⁸;

– в Государственной программе «Малое и среднее предпринимательство» на 2021–2025 гг. предусмотрено устранение пробелов в правовом регулировании деятельности сервисов онлайн-заимствования посредством принятия проекта Указа Президента Республики Беларусь «О сервисах онлайн-заимствования»⁴⁹.

Запланированные в приведенных программных правовых актах мероприятия и меры постепенно успешно реализуются. В частности, 25 мая 2021 г. принят Указ Президента Республики Беларусь № 196 «О сервисах онлайн-заимствования и лизинговой деятельности»⁵⁰. В названном законодательном акте предусмотрено нормативное регулирование краудлендинга (Войтова и др., 2022). Урегулированы отношения, связанные с деятельностью оператора сервиса онлайн-заимствования, а также с заключением и исполнением посредством такого сервиса договора займа и договора в обеспечение исполнения обязательств.

Остальные виды краудфандинга в Республике Беларусь пока не имеют специального регулирования, что во многом сдерживает их развитие. Лица, планирующие осуществлять деятельность по оказанию услуг сервиса онлайн-финансирования в таких видах краудфандинга, вынуждены руководствоваться общими положениями административного и гражданского законодательства, которые подлежат применению прямо либо по аналогии. Между тем специфика краудфандинга, проявляющаяся в основанном на факторе риска значительном объеме оборота денежных средств, а также вовлеченности посредством сети Интернет в процессы финансирования многочисленного и зачастую непрофессионального круга лиц, требует установления специального правового режима оказания услуг сервисов онлайн-финансирования (Парукова, 2020).

В свете общеевропейских тенденций, продемонстрированных на рис. 1 и 2, а также внутренней динамики белорусского общества по оказанию коллективной безвозмездной финансовой взаимопомощи в ближайшее время перспективным направлением дальнейшего развития краудфандинга в Республике Беларусь видится создание условий для деятельности операторов сервисов онлайн-благотворительности (Кучко, Левицкая, 2018).

На основании норм действующего гражданского законодательства Республики Беларусь наиболее подходящей договорной моделью, с помощью которой оператор сервиса онлайн-финансирования с одной стороны и соискатель финансирования или лицо, планирующее осуществлять финансирование, с другой могут урегулировать правоотношения между собой, является договор об оказании услуг (ст. 733 Гражданского кодекса Республики Беларусь – ГК Беларуси)⁵¹. В содержании такого договора возможно предусмотреть права и обязанности сторон при размещении информации

⁴⁸ Постановление Совета Министров Республики Беларусь № 758 от 24 декабря 2020 г. <https://pravo.by/document/?guid=12551&p0=C22000758&p1=1>

⁴⁹ Постановление Совета Министров Республики Беларусь № 56 от 29 января 2021 г. <https://pravo.by/document/?guid=3871&p0=C22100056>

⁵⁰ О сервисах онлайн-заимствования и лизинговой деятельности. № 196. (2021). <https://pravo.by/document/?guid=12551&p0=P32100196&p1=1>

⁵¹ Гражданский кодекс Республики Беларусь: в ред. Закона Республики Беларусь от 18 июля 2022 г. № 195-З. <https://pravo.by/document/?guid=3871&p0=hk9800218>

соискателя финансирования о проекте на сервисе онлайн-финансирования оператора, а также порядок посреднических услуг оператора в содействии привлечению или предоставлению денежных средств.

Отношения между соискателем финансирования и лицом, предоставляющим денежные средства, оформляются посредством различных договоров. Выбор определенного договора зависит от конкретной бизнес-модели краудфандинга.

При благотворительном краудфандинге чаще всего заключаются договоры дарения (ст. 543 ГК Беларуси), пожертвования (ст. 553 ГК Беларуси), договор предоставления безвозмездной (спонсорской) помощи (п. 5 Указа Президента Республики Беларусь от 1 июля 2005 г. № 300 «О предоставлении и использовании безвозмездной (спонсорской) помощи»)⁵² и др.

При краудревординге применяются договоры купли-продажи с предварительной оплатой (ст. 457 ГК Беларусь) и др. При этом, как обращает внимание О. И. Бандык, «если краудфандинг предусматривает условие о том, что товар будет передан донору (инвестору), независимо от размера его платежа и конечной стоимости самого товара, то применить ст. 457 ГК невозможно» (Бандык, 2019). Кроме того, для целей краудревординга возможно также заключение договора конвертированного займа и опционного договора (соответственно подп. 5.1 и 5.2 п. 5 Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики»)⁵³. В силу проводимого правового эксперимента, сфера нормативного регулирования данных договоров ограничена по субъектному составу резидентами Парка высоких технологий и третьими лицами, вступающими с ними в соответствующие договорные отношения. В проекте Закона Республики Беларусь «Об изменении кодексов»⁵⁴ указанные экспериментальные договорные модели взаимоотношения сторон планируется включить в содержание ГК Беларуси, дополнив его статьями 770-1 «Конвертируемый заем» и 399-2 «Опционный договор». Сфера действия правового регулирования названных статей будет распространяться на неограниченный круг участников гражданского оборота⁵⁵.

Правоотношения соискателей финансирования и инвесторов при краудинвестинге, на основании действующего гражданского законодательства Республики Беларусь, возможно оформить при помощи договора купли-продажи доли (акций) уставного фонда хозяйственного общества. Проанализировав данный договор на предмет практической реализации, Е. В. Усеня отмечает, что такая схема взаимоотношения сторон «является теоретически возможной, однако неудобной с практической точки зрения ввиду необходимости соблюдения ряда требований законодательства» (Усеня, 2019).

⁵² О предоставлении и использовании безвозмездной (спонсорской) помощи. № 300 (2005). <https://pravo.by/document/?guid=3961&p0=P30500300>

⁵³ О развитии цифровой экономики. № 8. (2017). <https://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1>

⁵⁴ Об изменении кодексов: проект закона Республики Беларусь. <https://house.gov.by/ru/zakony-ru/view/ob-izmenenii-kodeksov-1114/>

⁵⁵ Профессионально об актуальном: проект закона Республики Беларусь «Об изменении кодексов»: основные изменения в подраздел 2 раздела III Гражданского кодекса. <https://www.pravo.by/novosti/novosti-pravo-by/2019/mart/32692/>

На практике затруднения при документальном оформлении указанной договорной модели взаимоотношения сторон возникнут по следующим причинам:

- нормативно ограничено число участников хозяйственного общества (за исключением ОАО), их количество не может быть более 50 (ч. 5 ст. 66, ч. 1 ст. 91, ч. 1 ст. 112, ст. 113 Закона Республики Беларусь от 9 декабря 1992 г. № 2020-XII «О хозяйственных обществах»)⁵⁶;

- при оформлении каждой сделки купли-продажи доли (акций) в уставном фонде соискателя финансирования необходимо соблюсти все корпоративные процедуры (предоставить преимущественное право участникам общества и самому обществу провести общее собрание и т. д.);

- при принятии нового инвестора в ООО и ОДО необходимо производить государственную регистрацию изменений в устав и др.

Схожие формализованные корпоративные процедуры прослеживаются в законодательствах многих государств. Проведение таких процедур обосновывается регуляторами в первую очередь общим стремлением обезопасить гражданский оборот от мошеннических схем недобросовестных участников.

Становление краудинвестинга в национальных правовых порядках государств затруднено также и тем, что привлечение соискателями финансирования на соответствующем сервисе онлайн-финансирования (не являющемся биржей) денежных средств взамен предоставления доли (акций) в уставном фонде хозяйственного общества по сути означает публичное предложение части доли (акций) уставного фонда (первичное публичное размещение – initial public offering, сокр. IPO) (Furnari, 2021). В законодательных актах большинства государств (в том числе и Республики Беларусь), регулирующих порядок обращения ценных бумаг, а также деятельность бирж, установлено, что для публичного предложения части уставного фонда необходимо, чтобы предложение было осуществлено на бирже и хозяйственное общество соответствовало ряду критериев (в части финансовой отчетности, раскрытия информации, объемов эмиссии и др.). Тем временем на данном этапе экономического развития соискателями финансирования посредством краудфандинга, как правило, выступают стартапы, малый и средний бизнес. Выполнение императивных требований специального законодательства для большинства из названных субъектов хозяйствования становится весьма затруднительным либо вовсе невозможным. Более того, сервисы онлайн-финансирования не являются биржами. В связи с этим краудинвестинг во многих государствах формально-юридически не запрещен, однако на практике не осуществим (Yasar, 2021). Формально-юридически разрешить указанную ситуацию возможно посредством установления специального упрощенного правового режима обращения ценных бумаг при краудинвестинге. Практика закрепления такого правового регулирования широко распространена в зарубежных правовых порядках.

В Республике Беларусь целесообразно принять отдельные законодательные акты по каждому из видов краудфандинга (Усеня, 2018). Предметом правового регулирования станут общественные отношения, связанные с осуществлением операторами сервисов онлайн-финансирования деятельности по организации соответствующего вида краудфандинга. Принимая во внимание, что краудлендинг уже урегулирован Указом Президента, с учетом требований п. 4 ст. 33 Закона Республики

⁵⁶ О хозяйственных обществах. № 2020-XII. (1992). <https://pravo.by/document/?guid=3871&p0=v19202020>

Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах»⁵⁷, общественные отношения по остальным видам краудфандинга также следует регламентировать в Указах Президента Республики Беларусь.

В содержании проектов указов Президента следует предусмотреть:

- наличие у оператора сервиса онлайн-финансирования правового статуса юридического лица, зарегистрированного в Республике Беларусь;
- требования к деловой репутации, предъявляемые к учредителям (участникам), собственнику имущества, бенефициарным и иным владельцам оператора сервиса онлайн-финансирования;
- требования к деловой репутации и квалификации руководителя, его заместителя, ответственного за выполнение правил внутреннего контроля в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения и ответственного должностного лица в указанной сфере оператора сервиса онлайн-финансирования.

Юридическое лицо приобретает право осуществлять деятельность оператора сервиса онлайн-финансирования по конкретному виду краудфандинга со дня его включения государственным органом в соответствующий реестр. В Республике Беларусь компетенциями по формированию и ведению реестра по видам краудфандинга возможно наделить Национальный банк, Министерство экономики, Министерство финансов, Комитет государственного контроля.

В целях формирования и ведения реестра операторов сервисов онлайн-финансирования по видам краудфандинга советуемый государственный орган следует наделить полномочиями по установлению:

- порядка включения юридических лиц в реестр и внесения изменений в реестр (в том числе формы и содержания заявления о включении в реестр, перечня прилагаемых к нему документов, формы свидетельства о включении в реестр, оснований отказа в принятии заявления о включении в реестр (внесении изменений в реестр) и отказа во включении в реестр);
- порядка исключения оператора сервиса онлайн-финансирования из реестра (в том числе оснований исключения из реестра, отказа в принятии заявления об исключении из реестра и отказа в исключении из реестра).

Оператору сервиса онлайн-финансирования надлежит добросовестно оказывать услуги по организации краудфандинга, что означает оказание услуг в соответствии с экономическими интересами и намерениями соискателя финансирования и лица, осуществляющего финансирование. В целях обеспечения выполнения указанной обязанности в законодательных актах предусматриваются ограничения прав оператора сервиса онлайн-финансирования. К примеру, при краудлендинге оператор сервиса онлайн-заимствования не может быть стороной по договору займа, договору в обеспечение исполнения обязательств, заключаемым посредством этого сервиса онлайн-заимствования, а также не вправе привлекать на свои банковские счета и аккумулировать денежные средства клиентов для их последующего направления заемщикам, иным образом участвовать в движении денежных средств при осуществлении расчетов по договорам займа.

⁵⁷ О нормативных правовых актах. № 130-З. (2018). <https://pravo.by/document/?guid=3871&p0=H11800130>

Оператор сервиса онлайн-финансирования оказывает услуги по организации краудфандинга на основании отдельно заключаемых с участниками администрируемого им сервиса договоров. С соискателем финансирования заключается договор об оказании услуг по привлечению денежных средств, а с лицом, заинтересованным в осуществлении финансирования, – договор об оказании услуг по содействию в предоставлении денежных средств. Согласно условиям названных договоров, участники краудфандинга получают доступ к сервису онлайн-финансирования. Заинтересованное в осуществлении финансирования лицо также получает доступ к полной и достоверной информации: об условиях, предлагаемых к заключению посредством сервиса онлайн-финансирования договоров финансирования; о результатах проведенной оператором сервиса онлайн-финансирования оценки, соискателей финансирования и предложенных к финансированию проектов (при наличии).

Заключая соответствующий договор об оказании услуг, оператор сервиса онлайн-финансирования обязан установить конкретное физическое или юридическое лицо, с которым вступает в договорные правоотношения. Наряду с этим оператору надлежит получить от лица подтверждение, что оно ознакомилось и согласно с правилами сервиса онлайн-финансирования.

Договоры об оказании услуг по привлечению и содействию в предоставлении денежных средств являются договорами присоединения. Условия договоров определяются оператором в правилах сервиса онлайн-финансирования. Одним из обязательных условий договора об оказании услуг по содействию в предоставлении денежных средств является указание на то, что лицо, заинтересованное в осуществлении финансирования, осознает и принимает высокие риски, связанные с предоставлением денежных средств посредством сервиса онлайн-финансирования.

При необходимости изменения условий договора об оказании услуг оператор сервиса онлайн-финансирования должен направить участникам такого сервиса соответствующее предложение способом, обеспечивающим их персональное информирование. К примеру, путем оповещения в личном кабинете участника на сервисе онлайн-финансирования. Молчание не следует признавать волеизъявлением стороны по договору, за исключением случаев, предусмотренных законодательными актами.

Односторонние действия оператора по изменению условий договора об оказании услуг, а равно отказ от исполнения такого договора допускаются лишь в случаях, прямо предусмотренных правилами сервисов онлайн-финансирования или законодательными актами.

С помощью технологий и технических средств сервиса онлайн-финансирования соискатели финансирования и лица, заинтересованные в осуществлении финансирования, имеют возможность заключать между собой договоры финансирования, соответствующие применяемому виду краудфандинга (к примеру, договор купли-продажи эмиссионных ценных бумаг, договор коммерческого займа, договор купли-продажи или оказания услуг с предварительной оплатой, договор пожертвования или безвозмездной (спонсорской) помощи и т. д.) (Парукова, 2020).

На сервисе онлайн-финансирования надлежит использовать программное обеспечение, фиксирующее действия участников в отношении заключения, исполнения и расторжения договоров финансирования и оказания услуг.

Посредством сервиса онлайн-финансирования формируется и ведется реестр заключенных с использованием такого сервиса договоров. В реестр договоров

включаются сведения, позволяющие установить стороны договоров, существенные условия договоров и даты их заключения. Сведения о каждом заключенном договоре оператором сервиса онлайн-финансирования следует хранить до дня его прекращения, а также после его прекращения в течение установленного законодательством срока.

В период всего срока хранения сведений о договорах на сервисе онлайн-финансирования должны обеспечиваться: сохранность и достоверность таких сведений, а также возможность для сторон договора получения текста договора.

Оператор сервиса онлайн-финансирования по требованию участника в течение предусмотренного в законодательном акте срока с даты обращения обязан выдать документ о заключении договора посредством сервиса онлайн-финансирования, соответствующий установленным в законодательстве требованиям, а также иные необходимые участнику документы, связанные с заключением (исполнением) такого договора.

Как известно, привлечение и предоставление денежных средств посредством сервисов онлайн-финансирования сопряжено с множеством рисков и угроз, в числе которых мошенничество, сбор средств на запрещенные, деструктивные цели и т. д. (Папаскуя, 2021). Обозначенные риски и угрозы должны быть подконтрольны как государственным органам (в первую очередь Национальному банку, Комитету государственного контроля и др.), выступающим гарантами безопасности и общественного согласия в данной сфере, так и непосредственно оператору сервиса онлайн-финансирования. В связи с этим регуляторам необходимо разработать эффективную систему мер по выявлению и предупреждению таких рисков и угроз. В то же время подлежащие установлению меры не должны «сковывать» или ущемлять активность участников краудфандинга, которая в большинстве случаев основана на факторе естественного (добросовестного) экономического риска.

На основе анализа опыта зарубежных государств отметим наиболее распространенные меры по выявлению и предупреждению рисков и угроз, связанных с привлечением и предоставлением денежных средств посредством сервисов онлайн-финансирования:

- идентификация и аутентификация участников сервиса онлайн-финансирования, определение порядка допуска к информационным ресурсам сервиса онлайн-финансирования;

- установление требований к содержанию предложения о привлечении денежных средств;

- установление требований к участникам сервиса онлайн-финансирования (к примеру, возраст физических лиц, экономическое положение, требования к руководителю (исполняющему органу) юридического лица, частота и размер привлечения и предоставления денежных средств и т. д.);

- определение перечня договоров, которые могут заключать соискатель финансирования и лицо, осуществляющее финансирование с использованием информационных технологий и технических средств сервиса онлайн-финансирования, а также порядка заключения, изменения и расторжения таких договоров;

- определение состава информации, раскрываемой оператором сервиса онлайн-финансирования, а также порядка и сроков раскрытия такой информации и др.

В реализации приведенных мер оператору сервиса онлайн-финансирования отводится определяющая роль. Поскольку в правоотношениях по организации

краудфандинга оператор наиболее тесно взаимодействует как с соискателями финансирования, так и с лицами, осуществляющими финансирование. Конкретные процедуры реализации мер по выявлению и предупреждению рисков и угроз операторам надлежит определять в правилах сервиса онлайн-финансирования.

В рамках обозначенной деятельности оператор, прежде чем разместить в публичном доступе на сервисе онлайн-финансирования предложение по привлечению денежных средств, должен получить и проанализировать информацию о соискателе финансирования и о предполагаемом к финансированию проекте (при наличии).

В этих целях оператор сервиса онлайн-финансирования запрашивает у соискателя финансирования следующую информацию:

а) при регистрации на сервисе онлайн-финансирования:

- имя, дату и место рождения, адрес места жительства физического лица или индивидуального предпринимателя; наименование, место нахождения и адрес юридического лица;

- сведения о структуре и персональном составе органов управления юридического лица;

- основные виды деятельности; продукты или услуги, предлагаемые соискателем финансирования;

- годовую бухгалтерскую (финансовую) отчетность индивидуального предпринимателя или юридического лица за последний заверченный отчетный год;

б) при заполнении заявки на привлечение денежных средств:

- информацию, позволяющую составить общие представления о целях привлечения денежных средств;

- информацию об обстоятельствах, которые могут оказать влияние на достижение вышеназванных целей;

- сведения об основных рисках, связанных с привлечением денежных средств;

- срок действия предложения о привлечении денежных средств;

- минимальный объем вкладываемых отдельным заинтересованным в осуществлении финансирования лицом денежных средств;

- максимальный объем денежных средств, по достижению которого действие предложения о привлечении денежных средств прекращается;

- сведения о фактах (событиях, действиях), которые могут оказать существенное влияние на исполнение соискателем финансирования обязательств перед заинтересованными в финансировании лицами.

Наряду с этим соискатель финансирования при заполнении регистрационной формы подтверждает, что:

а) применительно к соискателям финансирования – юридическим лицам:

- не имеет задолженности по платежам в бюджет и (или) государственные целевые бюджетные и (или) внебюджетные фонды;

- не находится на стадии ликвидации или реорганизации юридического лица;

б) применительно к соискателям финансирования – физическим и юридическим лицам:

- не признан судом экономически несостоятельным (банкротом), не находится на любом этапе рассмотрения дела об экономической несостоятельности (банкротстве);

- не причастен к осуществлению, финансированию или иному пособничеству в осуществлении террористической, экстремистской деятельности, распространении

оружия массового поражения либо легализации доходов, полученных преступным путем;

в) применительно к соискателям финансирования – физическим лицам:

– не имеет непогашенной или неснятой судимости за преступления против собственности и порядка осуществления экономической деятельности.

Указанную выше информацию соискатель финансирования предоставляет оператору сервиса онлайн-финансирования в стандартной форме, установленной правилами сервиса онлайн-финансирования.

Оператор сервиса онлайн-финансирования, в соответствии с самостоятельно определяемыми критериями и методикой, осуществляет оценку соискателя финансирования, а также предлагаемого к финансированию проекта (при наличии).

При положительной оценке оператор обязан разместить на сервисе онлайн-финансирования в предусмотренные в законодательном акте сроки предложение по привлечению денежных средств, содержащее информацию о соискателе финансирования и о предлагаемом к финансированию проекте (при наличии) в объеме, установленном законодательным актом. Информация размещается на сервисе онлайн-финансирования в стандартной форме, разработанной оператором, для возможности сравнения лицами, заинтересованными в осуществлении финансирования, условий предложений по привлечению денежных средств между собой.

Оператор сервиса онлайн-финансирования вправе осуществлять деятельность по организации краудфандинга при условии публичного раскрытия на сервисе онлайн-финансирования правил данного сервиса. На основании присущих оператору функций в правилах сервиса онлайн-финансирования обычно содержатся:

- условия договора об оказании услуг по привлечению денежных средств и договора об оказании услуг по содействию в предоставлении денежных средств;
- порядок присоединения к договорам об оказании услуг, включая порядок установления лиц при заключении таких договоров;
- требования к участникам сервиса онлайн-финансирования;
- виды краудфандинга, реализуемые с помощью сервиса онлайн-финансирования;
- требования к содержанию предложения о привлечении денежных средств;
- размер вознаграждения оператора сервиса онлайн-финансирования или порядок его определения либо указание на отсутствие вознаграждения;
- состав информации, раскрываемой оператором сервиса онлайн-финансирования, а также порядок и сроки раскрытия такой информации и иные сведения в соответствии с требованиями, установленными законодательными актами.

Выводы

Резюмируя вышеизложенное, подчеркнем основные выводы.

1. Краудфандинг – способ привлечения и предоставления денежных средств от широкого круга лиц в сети Интернет для реализации какой-либо коммерческой или некоммерческой цели.

Несмотря на то, что понятие «краудфандинг» относительно недавно появилось в обиходе пользователей сети Интернет, концепция сбора средств от всех заинтересованных в реализации проекта лиц, положенная в его основу, известна довольно-таки давно. От устоявшихся в законодательстве и правоприменении способов

коллективного финансирования краудфандинг отличается прежде всего использованием специализированных сервисов онлайн-финансирования в глобальной компьютерной сети Интернет.

При краудфандинге не изменяется суть классических правоотношений по привлечению и предоставлению денежных средств. Вместе с тем правоотношения возникают, изменяются и прекращаются в режиме удаленного доступа сторон в специально созданной для этого цифровой среде (сервисе онлайн-финансирования). В связи с применением специальной среды рассматриваемые правоотношения сторон опосредуются участием третьей стороны – организации, деятельность которой связана с предоставлением услуг сервиса онлайн-финансирования.

Краудфандинг представляет собой собирательную категорию различных бизнес-моделей коллективного финансирования. Общепринятой признается классификация краудфандинга в зависимости от возможности получения лицами, осуществляющими финансирование, дохода от вложения средств. По данному критерию соответственно выделяют коммерческие и некоммерческие виды краудфандинга.

2. Субъектный состав правоотношений краудфандинга представлен следующими основными участниками: соискателем (реципиентом) финансирования; лицом, осуществляющим финансирование; оператором сервиса онлайн-финансирования. Оператор сервиса онлайн-финансирования, как правило, не относится к традиционным финансовым институтам, таким как банки и небанковские кредитно-финансовые организации. Между названными участниками экосистемы краудфандинга возникает как минимум три группы правоотношений: отношения между оператором сервиса онлайн-финансирования и соискателем (реципиентом) финансирования; отношения между оператором сервиса онлайн-финансирования и лицом, планирующим осуществлять финансирование; отношения между соискателем финансирования и лицом, осуществляющим финансирование.

3. В законодательстве зарубежных государств наметились следующие тенденции правового регулирования общественных отношений краудфандинга:

а) регулирование коммерческих и некоммерческих видов краудфандинга в различных нормативных правовых актах. Правовое регулирование бизнес-моделей некоммерческого краудфандинга, как правило, представлено в положениях общегосударственного законодательства. В свою очередь, бизнес-модели коммерческого краудфандинга зачастую имеют специальное нормативное регулирование в отдельных законодательных актах. Такая практика обусловлена спецификой регулируемых общественных отношений бизнес-моделей коммерческого краудфандинга, в основе которых заложено извлечение прибыли (дохода) или иного результата, связанного с осуществлением предпринимательской деятельности;

б) контроль за деятельностью операторов сервисов онлайн-финансирования со стороны государства посредством выдачи соответствующих разрешений (лицензий);

в) предъявление в нормативных правовых актах квалификационных и институциональных требований к операторам сервисов онлайн-финансирования, соискателям финансирования и лицам, осуществляющим финансирование;

г) ограничение частоты и объема привлекаемых соискателем финансирования денежных средств в определенный период времени, который, как правило, равен 12 месяцам;

д) ограничение частоты и объема вкладываемых лицом, осуществляющим финансирование, денежных средств в установленный период времени.

4. В Республике Беларусь осуществляется планомерное развитие краудфандинга. В программных правовых актах в краткосрочной и среднесрочной перспективе определены актуальные векторы дальнейшего становления данной сферы общественных отношений.

Широкое распространение в Республике Беларусь краудинвестинга, благотворительного краудфандинга и краудревординга сдерживает отсутствие специального нормативного регулирования данных видов краудфандинга. В связи с этим целесообразно разработать проекты указов Президента Республики Беларусь, регулирующих общественные отношения, связанные с привлечением и предоставлением денежных средств посредством сервисов онлайн-финансирования по соответствующим видам краудфандинга, а также устанавливающих правовые основы деятельности операторов таких сервисов.

Принятие специальных законодательных актов в обозначенной сфере будет способствовать диверсификации источников и инструментов финансовой поддержки физических лиц, субъектов малого и среднего предпринимательства, обеспечению национальной безопасности, снижению криминогенных рисков, упорядочиванию общественных отношений по привлечению и предоставлению денежных средств посредством сервисов онлайн-финансирования, повышению качества оказываемых операторами сервисов онлайн-финансирования услуг и является своего рода гарантией надлежащей защиты прав и интересов соискателей финансирования и лиц, осуществляющих финансирование.

5. В ближайшее время перспективным направлением дальнейшего развития краудфандинга в Республике Беларусь видится создание условий для деятельности операторов сервисов онлайн-благотворительности. В связи с этим актуальна и востребована разработка проекта Указа Президента Республики Беларусь «Об утверждении положения о деятельности сервисов онлайн-благотворительности». В проекте названного законодательного акта следует предусмотреть: требования к оператору и участникам сервиса онлайн-благотворительности; требования к сервису онлайн-благотворительности; порядок заключения и исполнения договоров пожертвования и безвозмездной (спонсорской) помощи посредством сервиса онлайн-благотворительности; меры по защите благотворителей (жертвователей, спонсоров); порядок осуществления расчетов между сторонами.

* Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

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

Список литературы

- Бандык, О. И. (2019). Краудфандинг: понятие и перспективы применения. *Юридический мир*, 6, 49.
- Василевский, А. В. (2020а). Краудфандинг: инновационное инвестирование. В книге: *XIV Машеровские чтения : материалы Междунар. науч.-практ. конф. студентов, аспирантов и молодых ученых, Витебск, 21 октября 2020 г.* (с. 430–432). Витебск: ВГУ имени П. М. Машерова.
- Василевский, А. В. (2020b). Правовое регулирование отношений в сфере краудфандинга. В книге: О. А. Бакиновская (ред.), *Актуальные проблемы правового обеспечения развития цифровой экономики в Республике Беларусь* (с. 147–173). Минск: Колорград.

- Вишнякова, М. В. (2018). Условия развития социального предпринимательства в Республике Беларусь. *Весті БДПУ. Серія 2. Гісторыя. Філасофія. Паліталогія. Сацыялогія. Эканоміка. Культуралогія*, 3(97), 93–98. <https://elibrary.ru/zabtwx>
- Войтова, О., Герасимчик, Ю., Шилина, Л. (2022). Направления развития небанковской деятельности на финансовом рынке Республики. *Банковский вестник*, 4(705), 23–35. <https://elibrary.ru/kthljw>
- Голикова, А. С. (2019). Ключевые аспекты функционирования краудфандинга. *Банкаўскі веснік*, 9(674), 33–43. <https://elibrary.ru/avjhiq>
- Горовая, В. В., Мурачковский, Ф. В. (ред.) (2016). *Практическое пособие по краудфандингу*. Москва: Глобал Нетворкс.
- Ерш, Е. А. (2021). Альтернативные источники венчурного финансирования в условиях цифровой трансформации. *Цифровая трансформация*, 4, 34–40. <https://elibrary.ru/hzexyo>
- Каменков, В. С. (2022). Краудфандинг: содержание, правовое регулирование, сферы применения. *Сацыяльна-эканамічныя і прававыя даследаванні*, 2(68), 12–17. <https://elibrary.ru/bvtvir>
- Клинов, А. О. (2018). Правовое регулирование краудфандинга в России и за рубежом. *Закон*, 2, 90–105. <https://elibrary.ru/yvtake>
- Кучко, Е. Е., Левицкая, И. В. (2018). Практики в области социального предпринимательства: опыт Беларуси. В сборнике: *Бизнес. Инновации. Экономика* (с. 95–103). Минск: Белорусский государственный университет, Институт бизнеса. <https://elibrary.ru/xtepcj>
- Михалева, Н. В. (2019). Проблема правового регулирования краудфандинга в Российской Федерации. *Вестник Международного юридического института*, 1(68), 24–30. <https://elibrary.ru/rtfgqw>
- Папаскуа, Г. Т. (2021). Краудфандинг: понятие, виды и риски. *Актуальные проблемы российского права*, 16(7), 77–85. EDN: <https://elibrary.ru/ioyzkd>. DOI: <https://doi.org/10.17803/1994-1471.2021.128.7.077-085>
- Парукова, Е. В. (2020). Правовое регулирование краудфандинга как инвестиционной деятельности в Республике Беларусь. *Вестник Сургутского государственного университета*, 2(28), 68–74. EDN: <https://elibrary.ru/knhdsz>. DOI: <https://doi.org/10.34822/2312-3419-2020-2-68-74>
- Савельев, А. И. (2016). *Электронная коммерция в России и за рубежом: правовое регулирование* (2-е изд., перераб. и доп.). Москва: Статут.
- Селява, Г. (2021). Сервисы онлайн-заимствования как альтернативный механизм финансирования. *Банкаўскі веснік*, 7(696), 17–20. <https://elibrary.ru/cmuatl>
- Степура, И. А. (2021). Краудлендинг: механизм функционирования и законодательное регулирование сервисов онлайн-заимствования. *Право.by*, 5(73), 89–94. <https://elibrary.ru/sannoh>
- Ткачев, А., Баталко, В. (2018). Возможности и риски краудфандинга и P2P-займов. *Банкаўскі веснік*, 5(658), 37–44. <https://elibrary.ru/zazbfr>
- Усеня, Е. В. (2018). Правовые основы безвозмездного краудфандинга в Республике Беларусь. *Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение*, 8(3), 23–28. <https://elibrary.ru/xqvxyz>
- Усеня, Е. В. (2019). Правовые условия для развития краудфандинга в Республике Беларусь. *Право.by*, 4, 40–45. <https://elibrary.ru/yzeybc>
- Усеня, Е. В. (2020). Краудлендинг: понятие и перспективы развития в Республике Беларусь. *Право.by*, 3(65), 40–44. <https://elibrary.ru/vppowz>
- Щетинина, Е. А. (2016). Акционерный краудфандинг как альтернативная модель финансирования бизнеса на раннем этапе развития и стартапов. *Международные подходы. Экономический вектор*, 1(4), 22–27. <https://elibrary.ru/vpnrsf>
- Armour, J., & Enriques, L. (2018). The Promise and Perils of Crowdfunding: Between Corporate Finance and Consumer Contracts. *The Modern Law Review*, 81(1), 51–84. <https://doi.org/10.1111/1468-2230.12316>
- Bi, S., Liu, Z., & Usman, K. (2017). The influence of online information on investing decisions of reward-based crowdfunding. *Journal of Business Research*, 71, 10–18. <https://doi.org/10.1016/j.jbusres.2016.10.001>
- Boudreau, K. J., Jeppesen, L. B., Reichstein, T., & Rullani, F. (2021). Crowdfunding as Donations to Entrepreneurial Firms. *Research Policy*, 50(7). <https://doi.org/10.1016/j.respol.2021.104264>
- Cai, W., Polzin, F., & Stam, E. (2021). Crowdfunding and social capital: A systematic review using a dynamic perspective. *Technological Forecasting and Social Change*, 162(120412). <https://doi.org/10.1016/j.techfore.2020.120412>
- Duan, Y., Hsieh, T.-S., Wang, R. R., & Wang, Z. (2020). Entrepreneurs' facial trustworthiness, gender, and crowdfunding success. *Journal of Corporate Finance*, 64(101693). <https://doi.org/10.1016/j.jcorpfin.2020.101693>

- Ferreira, V., Papaoikonomou, E., & Terceño, A. (2022). Unpeel the layers of trust! A comparative analysis of crowdfunding platforms and what they do to generate trust. *Business Horizons*, 65(1), 7–19. <https://doi.org/10.1016/j.bushor.2021.08.004>
- Furnari, S. L. (2021). Trough Equity Crowdfunding Evolution and Involution: Initial Coin Offering and Initial Exchange Offering. *Lex Russica*, 1, 101–117. EDN: <https://elibrary.ru/tbrdxt>. DOI: <https://doi.org/10.17803/1729-5920.2021.170.1.101-117>
- Gedda, D., Nilsson, B., Săthén, Z., & Søylen, K. S. (2016). Crowdfunding: finding the optimal platform for funders and entrepreneurs. *Technology Innovation Management Review*, 6(3), 31–40. <https://doi.org/10.22215/timreview/973>
- Karpoff, J. M. (2021). The future of financial fraud. *Journal of Corporate Finance*, 66(101694). <https://doi.org/10.1016/j.jcorpfin.2020.101694>
- La Viña, L. Y. De, & Black, S. L. (2018). US Equity Crowdfunding: A Review of Current Legislation and A Conceptual Model of the Implications for Equity Funding. *The Journal of Entrepreneurship*, 27(1), 83–110. <https://doi.org/10.1177/0971355717738600>
- Lihn, D. H. (2019). Impacts of Founder on The Success of Crowdfunding in Vietnam. *Journal of Economics and Business*, 2(2), 356–362. <https://doi.org/10.31014/aior.1992.02.02.92>
- Lukkarinen, A. (2020). Equity Crowdfunding: Principles and Investor Behaviour. In *Advances in Crowdfunding: Research and Practice* (pp. 93–118). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-46309-0_5
- Mollick, E., & Nanda, R. (2016). Wisdom or Madness? Comparing Crowds with Expert Evaluation in Funding the Arts. *Management Science*, 62(6), 1533–1553. <https://doi.org/10.1287/mnsc.2015.2207>
- Odorović, A., & Wenzlaff, K. (2020). The joint production of confidence – self-regulation in European crowdfunding markets. *Baltic Journal of Management*, 15(2), 303–331. <https://doi.org/10.1108/BJM-04-2019-0119>
- Sanderson, L., Wright McNaughton, G., & Yashiro, N. (2022, 13 October). Does faster internet increase exports? Evidence from New Zealand. In *OECD Economics Department Working Papers*, 1730. <https://doi.org/10.1787/18151973>
- Sannajust, A., Roux, F., & Chaibi, A. (2014). Crowdfunding In France: A New Revolution? *Journal of Applied Business Research (JABR)*, 30(6), 1919–1928. <https://doi.org/10.1016/j.respol.2021.104264>
- Shneor, R., Zhao, L., & Fabian Michael Goedecke, J. (2023). On relationship types, their strength, and reward crowdfunding backer behavior. *Journal of Business Research*, 154(113294). <https://doi.org/10.1016/j.jbusres.2022.08.058>
- Wang, W., Chen, W., Zhu, K., & Wang, H. (2020). Emphasizing the entrepreneur or the idea? The impact of text content emphasis on investment decisions in crowdfunding. *Decision Support Systems*, 136(113341). <https://doi.org/10.1016/j.dss.2020.113341>
- Wolfe, M. T., Patel, P. C., & Manikas, A. S. (2021). Shock and awe: Loudness and unpredictability in Twitter messages and crowdfunding campaign success. *Journal of Innovation & Knowledge*, 6(4), 246–256. <https://doi.org/10.1016/j.jik.2021.06.002>
- Yasar, B. (2021). The new investment landscape: Equity crowdfunding. *Central Bank Review*, 21(1), 1–16. <https://doi.org/10.1016/j.cbrev.2021.01.001>
- Zhao, L., & Ryu, S. (2020). Reward-Based Crowdfunding Research and Practice. In *Advances in Crowdfunding: Research and Practice* (pp. 119–143). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-46309-0_6

Сведения об авторе



Василевский Андрей Витальевич – научный сотрудник отдела исследований в области гражданского, экологического и социального права, Институт правовых исследований Национального центра законодательства и правовых исследований Республики Беларусь

Адрес: 220030, Республика Беларусь, г. Минск, ул. Берсона, 1а

E-mail: VasileuskiAV@gmail.com

ORCID ID: <https://orcid.org/0000-0001-5457-3283>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/GVW-1967-2022>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1168843

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 2 ноября 2022 г.

Дата одобрения после рецензирования – 23 января 2023 г.

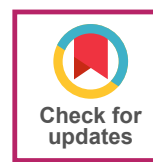
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Scientific review

DOI: <https://doi.org/10.21202/jdtl.2023.8>



Legal Regulation of Relations in the Sphere of Crowdfunding in the Republic of Belarus

Andrey V. Vasilevskii 

The National Centre of Legislation and Legal Research of the Republic of Belarus
Minsk, Republic of Belarus

Keywords

Contract,
crowdfunding,
crowd-investing,
crowd-lending,
crowd-rewarding,
digital technologies,
law,
legislation,
online-funding,
regulation

Abstract

Objective: to study the theoretical and legal bases of crowdfunding and to elaborate scientifically grounded proposals for improving the Republic of Belarus legislation in this sphere.

Methods: the methodological basis of the research is a system of principles, methods and techniques of studying the general regularities of emergence, formation and development of social-legal phenomena. In the research, general and specific methods of scientific cognition were used: analysis, synthesis, comparative-legal, logical, systemic, formal-legal, dialectic and other methods.

Results: the history of emergence and formation of crowdfunding was analyzed. The social-economic and technical-technological factors were revealed, which facilitate the popularization of crowdfunding among the Internet users. The origins of the "crowdfunding" notion were discussed, as well as its filling with a definite meaning. The types of crowdfunding were listed, depending on the goal of investment on the part of investors. The main subject composition of legal relations in crowdfunding was established, which consists of the following persons: funding seeker; funder; operator of online-funding service. The overall algorithm of legal relations between the main subjects of crowdfunding was described. The positive and negative aspects of crowdfunding were characterized. An overall analysis of foreign legislation in the crowdfunding legal regulation was performed. Based on the analysis, the general trends of legislation development were presented. The program and normative legal acts on developing crowdfunding in the Republic of Belarus were reviewed. The probable contract models of the parties' legal relations registering were named. The technical and legal requirements to the functional

© Vasilevskii A. V., 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 an online-funding service were determined. The minimal necessary set of measures was proposed, which may prevent risks and threats associated with procurement and extension of funds through online-funding services. Based on the operator functions, specific requirements to the rules of online-funding service were determined.

Scientific novelty: the author comprehensively studied the notion, legal nature and features of legal regulation of crowdfunding. The factors were revealed, which influence the formation of the legal norms regulating the procurement and extension of funds through online-funding services. The author elaborated proposals for improving the Republic of Belarus legislation in the sphere of social relations under study.

Practical significance: the research results are significant for developing the studies in the sphere of civil, economic, and informational law. The obtained results may be used in teaching a course in civil, economic, and informational law, as well as be applied by law subjects when elaborating and introducing the respective drafts of laws and be an object of further scientific research on the issue.

For citation

Vasilevskii, A. V. (2023). Legal Regulation of Relations in the Sphere of Crowdfunding in the Republic of Belarus. *Journal of Digital Technologies and Law*, 1(1), 191–234. <https://doi.org/10.21202/jdtl.2023.8>

References

- Armour, J., & Enriques, L. (2018). The Promise and Perils of Crowdfunding: Between Corporate Finance and Consumer Contracts. *The Modern Law Review*, 81(1), 51–84. <https://doi.org/10.1111/1468-2230.12316>
- Bandyk, O. I. (2019). Crowdfunding: notion and prospects of implementation. *Yuridicheskii mir*, 6, 49. (In Russ.).
- Bi, S., Liu, Z., & Usman, K. (2017). The influence of online information on investing decisions of reward-based crowdfunding. *Journal of Business Research*, 71, 10–18. <https://doi.org/10.1016/j.jbusres.2016.10.001>
- Boudreau, K. J., Jeppesen, L. B., Reichstein, T., & Rullani, F. (2021). Crowdfunding as Donations to Entrepreneurial Firms. *Research Policy*, 50(7). <https://doi.org/10.1016/j.respol.2021.104264>
- Cai, W., Polzin, F., & Stam, E. (2021). Crowdfunding and social capital: A systematic review using a dynamic perspective. *Technological Forecasting and Social Change*, 162(120412). <https://doi.org/10.1016/j.techfore.2020.120412>
- Duan, Y., Hsieh, T.-S., Wang, R. R., & Wang, Z. (2020). Entrepreneurs' facial trustworthiness, gender, and crowdfunding success. *Journal of Corporate Finance*, 64(101693). <https://doi.org/10.1016/j.jcorpfin.2020.101693>
- Ersh, E. A. (2021). Alternative sources of venture financing in the conditions of digital transformation. *Digital Transformation*, 4, 34–40. (In Russ.).
- Ferreira, V., Papaoikonomou, E., & Terceño, A. (2022). Unpeel the layers of trust! A comparative analysis of crowdfunding platforms and what they do to generate trust. *Business Horizons*, 65(1), 7–19. <https://doi.org/10.1016/j.bushor.2021.08.004>
- Furnari, S. L. (2021). Trough Equity Crowdfunding Evolution and Involution: Initial Coin Offering and Initial Exchange Offering. *Lex Russica*, 1, 101–117. <https://doi.org/10.17803/1729-5920.2021.170.1.101-117>
- Gedda, D., Nilsson, B., Sâthén, Z., & Søylen, K. S. (2016). Crowdfunding: finding the optimal platform for funders and entrepreneurs. *Technology Innovation Management Review*, 6(3), 31–40. <https://doi.org/10.22215/timreview/973>
- Golikova, A. S. (2019). Key aspects of crowdfunding functioning. *Bankovskii vestnik*, 9(674), 33–43. (In Russ.).
- Gorovaya, V. V., & Murachkovskii, F. V. (Ed.). (2016). *Practical tutorial on crowdfunding*. Moscow: Global Networks. (In Russ.).

- Kamenkov, V. S. (2022). Crowdfunding: content, legal regulation, scope. *Satsyyal'na-ehkanamichnyya i pravavyya dasledavanni*, 2(68), 12–17. (In Russ.).
- Karpoff, J. M. (2021). The future of financial fraud. *Journal of Corporate Finance*, 66(101694). <https://doi.org/10.1016/j.jcorpfin.2020.101694>
- Klinov, A. O. (2018). The legal regulation of crowdfunding in Russia and foreign jurisdictions. *Statute*, 2, 90–105. (In Russ.).
- Kuchko, E. E., & Levitskaya, I. V. (2018). Practices in the field of social entrepreneurship: experience of Belarus. In *Business. Innovations. Economics* (pp. 95–103). Minsk: Belorusskii gosudarstvennyi universitet, Institut biznesa. (In Russ.).
- La Viña, L. Y. De, & Black, S. L. (2018). US Equity Crowdfunding: A Review of Current Legislation and a Conceptual Model of the Implications for Equity Funding. *The Journal of Entrepreneurship*, 27(1), 83–110. <https://doi.org/10.1177/0971355717738600>
- Lihn, D. H. (2019). Impacts of Founder on the Success of Crowdfunding in Vietnam. *Journal of Economics and Business*, 2(2), 356–362. <https://doi.org/10.31014/aior.1992.02.02.92>
- Lukkarinen, A. (2020). Equity Crowdfunding: Principles and Investor Behaviour. In *Advances in Crowdfunding: Research and Practice* (pp. 93–118). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-46309-0_5
- Mikhaleva, N. V. (2019). Issue of legal regulation of crowdfunding in the Russian Federation. *Vestnik Mezhdunarodnogo yuridicheskogo instituta*, 1(68), 24–30. (In Russ.).
- Mollick, E., & Nanda, R. (2016). Wisdom or Madness? Comparing Crowds with Expert Evaluation in Funding the Arts. *Management Science*, 62(6), 1533–1553. <https://doi.org/10.1287/mnsc.2015.2207>
- Odorović, A., & Wenzlaff, K. (2020). The joint production of confidence – self-regulation in European crowdfunding markets. *Baltic Journal of Management*, 15(2), 303–331. <https://doi.org/10.1108/BJM-04-2019-0119>
- Papaskua, G. T. (2021). Crowdfunding: the concept, types and risks. *Actual Problems of Russian Law*, 16(7), 77–85. (In Russ.). <https://doi.org/10.17803/1994-1471.2021.128.7.077-085>
- Parukova, E. V. (2020). Legal regulation of crowdfunding as an investment activity in the republic of Belarus. *Bulletin of Surgut State University*, 2(28), 68–74. (In Russ.). <https://doi.org/10.34822/2312-3419-2020-2-68-74>
- Sanderson, L., Wright McNaughton, G., & Yashiro, N. (2022, 13 October). Does faster internet increase exports? Evidence from New Zealand. In *OECD Economics Department Working Papers*, 1730. <https://doi.org/10.1787/18151973>
- Sannajust, A., Roux, F., & Chaibi, A. (2014). Crowdfunding in France: A New Revolution? *Journal of Applied Business Research (JABR)*, 30(6), 1919–1928. <https://doi.org/10.1016/j.respol.2021.104264>
- Savelyev, A. I. (2016). *Electronic commerce in Russia and abroad: legal regulation* (2nd edition, reviewed and complemented). Moscow: Statut. (In Russ.).
- Selyava, G. (2021). Online borrowing services as an alternative mechanism of financing. *Bankovskii vestnik*, 7(696), 17–20. (In Russ.).
- Shchetinina, E. A. (2016). Equity crowdfunding as an alternative financing model for early stage businesses and startups. International approaches. *Economic Vector*, 1(4), 22–27. (In Russ.).
- Shneor, R., Zhao, L., & Fabian Michael Goedecke, J. (2023). On relationship types, their strength, and reward crowdfunding backer behavior. *Journal of Business Research*, 154 (113294). <https://doi.org/10.1016/j.jbusres.2022.08.058>
- Stepuro, I. A. (2021). Crowdlending: mechanism of functioning and legislative regulation of services of online borrowing. *Pravo.by*, 5(73), 89–94. (In Russ.).
- Tkachev, A., & Bataiko, V. (2018). Possibilities and risks of crowdfunding and p2p loans. *Bankovskii vestnik*, 5(658), 37–44. (In Russ.).
- Usenya, E. V. (2018). Legal frameworks of free crowdfunding in the Republic of Belarus. *Vesnik of Yanka Kupala State University of Grodno. Series 4. Jurisprudence*, 8(3), 23–28. (In Russ.).
- Usenya, E. V. (2019). Legal conditions for the development of crowdinvesting in the Republic of Belarus. *Pravo.by*, 4, 40–45.
- Usenya, E. V. (2020). Crowdlending: concept and prospects of development in the Republic of Belarus. *Pravo.by*, 3(65), 40–44. (In Russ.).
- Vasilevskii, A. V. (2020a). Crowdfunding: innovative investment. In *XIV Masharov Readings: works of the International scientific-practical conference of students, post-graduate students and young researchers, Vitebsk, October 21, 2020* (pp. 430–432). Vitebsk: VGU imeni P. M. Masharova. (In Russ.).

- Vasilevskii, A. V. (2020b). Legal regulation of relations in the sphere of crowdfunding. In O. A. Bakinovskaya (Ed.), *Topical issues of legal provision of digital economy in the Republic of Belarus* (pp. 147–173). Minsk: Kolograd. (In Russ.).
- Vishnyakova, M. V. (2018). Conditions for social entrepreneurship in the Republic of Belarus. *Vestsi BDPU. Seryya 2. Gistoryya. Filasofiya. Palitalogiya. Satsyyalogiya. Ehkanomika. Kul'turalogiya*, 3(97), 93–98. (In Russ.).
- Voytova, O., Gerasimchik, Yu., & Shilina, L. (2022). Directions of development of the non-bank activities in the financial market of the republic of belarus. *Bankovskii vestnik*, 4(705), 23–35. (In Russ.).
- Wang, W., Chen, W., Zhu, K., & Wang, H. (2020). Emphasizing the entrepreneur or the idea? The impact of text content emphasis on investment decisions in crowdfunding. *Decision Support Systems*, 136(113341). <https://doi.org/10.1016/j.dss.2020.113341>
- Wolfe, M. T., Patel, P. C., & Manikas, A. S. (2021). Shock and awe: Loudness and unpredictability in Twitter messages and crowdfunding campaign success. *Journal of Innovation & Knowledge*, 6(4), 246–256. <https://doi.org/10.1016/j.jik.2021.06.002>
- Yasar, B. (2021). The new investment landscape: Equity crowdfunding. *Central Bank Review*, 21(1), 1–16. <https://doi.org/10.1016/j.cbrev.2021.01.001>
- Zhao, L., & Ryu, S. (2020). Reward-Based Crowdfunding Research and Practice. In *Advances in Crowdfunding: Research and Practice* (pp. 119–143). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-46309-0_6

Author information



Andrey V. Vasilevskii – Researcher of the Department of Civil, Ecological and Social Legal Research of the National Centre of Legislation and Legal Research of the Republic of Belarus

Address: 1a Berson Str., 220030 Minsk, Republic of Belarus

E-mail: VasileuskiAV@gmail.com

ORCID ID: <https://orcid.org/0000-0001-5457-3283>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/GVW-1967-2022>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1168843

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – November 2, 2022

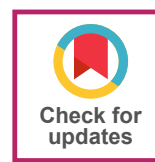
Date of approval – January 23, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 343.2/.7:343.9:004
EDN: <https://elibrary.ru/zmirlt>
DOI: <https://doi.org/10.21202/jdtl.2023.9>



Цифровые тренды криминологии и уголовного правосудия XXI века

Мехрдад Райеджиан Асли 

Институт исследования и развития гуманитарных дисциплин
г. Тегеран, Исламская Республика Иран

Ключевые слова

Алгоритмическая криминология, кибервиктимология, киберкриминология, киберпространство, криминология, риск, уголовное право, уголовное правосудие, цифровизация, цифровые технологии

Аннотация

Цель: определение ключевых трендов развития криминологии и уголовного правосудия в условиях значительного расширения цифровизации и применения современных технологий.

Методы: приоритет аналитического метода в его сочетании с описательным методом обеспечили оптимальный инструментарий для поиска и выявления основных цифровых трендов развития криминологии и уголовного правосудия в XXI веке.

Результаты: выявлена возрастающая зависимость уголовно-правовой науки от развития цифровых технологий, которая приводит к изменению сущности и типов современной преступности, моделей поведения преступников, методов и механизмов контроля и предотвращения преступности в свете требований уголовной политики и уголовного правосудия. Подчеркивается двоякая роль глобального тренда цифровизации, достижения которой используются как органами системы уголовного правосудия (в частности, для контроля, управления и предотвращения преступности), так и преступниками – при осуществлении своих преступных замыслов. Установлено, что существенная трансформация криминологии и уголовного правосудия вызвана в значительной степени резким развитием в XXI веке цифровизации и созданных на ее основе современных технологий, являющихся более эффективными, чем обычные методы традиционной криминологии, такие как количественные и качественные оценки, наблюдения, интервью, опросы и др.

Научная новизна: вводятся новые области уголовно-правового знания и соответствующие им дисциплины, образованные исключительно под влиянием цифровизации, такие как киберкриминология и кибервиктимология; в качестве новейшего направления криминологической науки выделяется алгоритмическая (вычислительная) криминология, основанная на страховом праве и теории рисков.

© Райеджиан Асли 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: учет трендов и положительного опыта, полученного в области цифровизации, обуславливает успешное решение задач, связанных с противодействием преступности, трансформацию подходов к содержанию, целям и методологии прикладной криминологии и уголовного правосудия. Глобальный мегатренд цифровизации существенно меняет облик уголовно-правовой науки, задает новые теоретические и прикладные направления ее развития. Своевременное обновление и адаптирование знаний, умений и навыков согласно достижениям цифровизации позволит криминологии и уголовному правосудию соответствовать задачам нового тысячелетия.

Для цитирования

Райеджиан Асли, М. (2023). Цифровые тренды криминологии и уголовного правосудия XXI века. *Journal of Digital Technologies and Law*, 1(1), 235–250. <https://doi.org/10.21202/jdtl.2023.9>

Содержание

Введение

1. Теория риска в контексте цифровизации

1.1. Административная криминология в свете требований предотвращения преступности

1.2. Управление рисками и страховое право в свете проблемы рецидивизма

2. Киберкриминология и виктимология

2.1. Возникновение киберкриминологии в качестве объяснения этиологии киберпреступности

2.2. Необходимость кибервиктимологии для противодействия киберпреступности и виктимизации

3. Алгоритмическая, или вычислительная, криминология

Выводы

Введение

Цифровизация определяется как «интеграция цифровых технологий в повседневную жизнь во всех сферах, где это возможно» (Ochs & Reinmann, 2018). Также ее определяют как применение цифровых технологий для изменения труда в целях создания ценности путем использования новых прогрессивных технологий, развития цифровых сетей и гигантского цифрового потока информации (Scuotto et al., 2019; Cho et al., 2021; Moneva et al., 2022; Khan et al., 2020; van de Weijery & Moneva, 2022; Sampson, 2014). Цифровизация может быть реализована как процесс трансформации чего-либо в цифровую форму, возникающую при использовании цифровых технологий для усовершенствования процессов (Cabada García et al., 2022; Abubotain & Chamakiotis, 2020; Lallie et al., 2021; Okutan & Çebi, 2019; Solak & Topaloglu, 2015).

Учитывая вышеуказанные определения, цифровизация может найти применение во многих областях науки, включая, в частности, гуманитарные и общественные дисциплины. При этом уголовно-правовые дисциплины относятся к тем областям гуманитарных и общественных наук, в которых цифровизация может сыграть значительную роль. Два основных направления исследований в уголовно-правовой науке, которые испытали особенно сильное влияние цифровизации и развития технологий в последние десятилетия, – это криминология и уголовное правосудие.

По сравнению с 1980–1990-ми годами в области криминологии появились новые подходы и теории, связанные с развитием общественных наук и критического знания, которые привели к созданию критической криминологии и других современных тенденций в этой науке. В начале XXI века криминология и уголовное правосудие начали развиваться в свете цифровизации и технологий, особенно компьютеризации. Таким образом, в этих областях возникло несколько тенденций и даже новых направлений науки. Три из которых рассматриваются в данной статье, а именно: теория управления рисками и страховое правосудие – тенденция, появившаяся в последние десятилетия прошлого века; киберкриминология и кибервиктимология, а также алгоритмическая, или вычислительная, криминология, возникшая за два десятилетия третьего тысячелетия.

В широком смысле, учитывая вышеуказанные определения, роль и положение цифровизации в криминологии и уголовном правосудии описываются концепциями и теориями, берущими начало в возникновении криминологии. Автор делает попытку обнаружить и показать самые значимые примеры и проявления тех концепций и теорий, которые могут продемонстрировать процесс цифровизации этих двух важнейших направлений уголовно-правовой науки через их достижения за два десятилетия XXI века. Соответственно, в данной статье выделены три основные части. В первой части речь идет об управлении рисками как криминологической теории, связанной со страховым правом и исследуемой в контексте цифровизации. Во второй части два новых раздела уголовно-правовой науки – киберкриминология и кибервиктимология – рассматриваются в свете компьютерных наук. Третья часть посвящена алгоритмической, или вычислительной, криминологии, развившейся за последние два десятилетия в рамках криминологии и уголовного правосудия.

1. Теория риска в контексте цифровизации

Риск – важнейшее ключевое понятие нескольких разделов криминологии, включая функционирование системы уголовного правосудия, модели предотвращения преступности и криминальную этиологию, базирующуюся на теории рационального выбора (O'Malley, 2009). Прежде чем стать центральным объектом науки уголовного правосудия, риск изучался в рамках классической криминологии с точки зрения рационального выбора при преступном поведении. Такая точка зрения предполагает, что криминальное поведение дает преступникам преимущество и основывается на их свободно принимаемых решениях. Однако ранее было показано, что эта теория применима лишь к определенным типам преступлений – так называемым утилитарным преступлениям, при которых преступное поведение направлено на получение выгоды (McLaughlin & Muncie, 2019).

1.1. Административная криминология в свете требований предотвращения преступности

Независимо от применимости теории рационального выбора к определенным типам преступлений, она используется для объяснения ситуационного, или оппортунистического, предотвращения преступлений. Эта модель предотвращения преступлений возникла в рамках «административной криминологии» в 1980-е гг. Она определяется как направление криминологии, фокусирующееся на повышении эффективности системы уголовного правосудия, в частности, путем ситуационного, или оппортунистического, предотвращения преступлений (Halder, 2021). Постулируя, что преступники действуют рационально и обдуманно, административная криминология рассматривает преступление как событие, в котором роли преступника и жертвы и другие обстоятельства являются компонентами преступного поведения (McLaughlin & Muncie, 2019). Согласно теоретическим и прикладным положениям криминологии и уголовного правосудия, административная криминология базируется на этиологической точке зрения, которая носит название «криминология преступного поведения». Эта точка зрения берет начало в европейском (особенно французском) подходе к изучению преступности. Как указывает французский криминолог Raymond Gassin, криминология преступного поведения включает в себя теорию совершения действия, которая объясняет преступное поведение как процесс, в ходе которого формируется поведение от намерения до самого акта (Gassin, 1990). Таким образом, эта теория учитывает преступный расчет как существенный элемент административной криминологии. Преступный расчет предполагает, что преступник действует на основе рациональной оценки. Поэтому для контроля и предотвращения преступности необходим ряд технико-технологических инструментов и средств измерения. Они составляют модель ситуационного, или оппортунистического, предотвращения преступлений, которая включает такие средства и методы, как системы видеонаблюдения и охранной сигнализации.

Введя административную криминологию как новое направление уголовной этиологии и уголовной политики, криминологические исследования перешли к оценке рисков в системе уголовного правосудия.

1.2. Управление рисками и страховое право в свете проблемы рецидивизма

На раннем этапе оценка риска имела критическое значение для клинического прогнозирования и судебной экспертизы. В то же время она использовалась для работы с факторами риска с этиологической точки зрения (Pritchard et al., 2014). Сегодня оценка риска получила новую трактовку в рамках страхового права. Страховое право – это подход в криминологии, возникший из сферы страхования. Он предполагает использование компьютерного программного обеспечения (McLaughlin & Muncie, 2019) и представляет собой теоретическую модель на основе концепций и методов, сходных со страховой математикой (Bosworth, 2005).

Распространение этой модели в уголовном праве произошло благодаря актуарному статистическому моделированию рисков, т. е. в рамках страховой отрасли (Metcalf, 2004). В криминологии и уголовном правосудии страховое право использует расчетные методы, которые формируют основу для уголовной политики, в частности, в области коррекции и пенитенциарной системы. Таким образом, это одна

из моделей уголовного правосудия, в рамках которой реабилитация как механизм уголовных санкций получает новую интерпретацию через вероятностное исчисление и статистические распределения для управления заключенными, особенно в тюремной системе. В свете этого подхода управление заключенными осуществляется на основе технологий и практики оценки рисков (McLaughlin & Muncie, 2019). Ярким примером служит использование таких мер и средств, как пробация, при управлении рисками в приложении к проблеме рецидивизма опасных, в частности сексуальных, преступлений. Например, сегодня суды в США используют компьютерные программы, чтобы предсказать вероятность повторения преступления в будущем. Этот метод внедряется как в процесс принятия судебных решений, так и в тюремную систему. Рассматривая такие переменные, как точность и справедливость, критики заявляют, что компьютерная программа может демонстрировать расовую предвзятость, особенно в пользу белых по сравнению с чернокожими (Dressel & Farid, 2018).

На уровне профилактики в аспекте ситуационного, или оппортунистического, предотвращения преступлений управление рисками связано с теми методами сокращения уровня преступности (McLaughlin & Muncie, 2019), которые используют технологии и стратегии снижения возможностей для совершения преступлений в отношении их организации и сопутствующих обстоятельств. Как писал один из основателей новой пенологии Feeley, «страховое правосудие стремится предсказать будущее преступное поведение человека, в настоящий момент осужденного системой уголовного правосудия, а затем применить к нему меры, снижающие его возможности для совершения будущих преступлений» (Feeley, 2004). Типичным примером могут служить США, где применяются различные меры оценки рисков, основанные на страховом праве. Одним из значимых методов оценки риска является метод COMPAS – профилирование осужденного преступника для управления альтернативными санкциями. Этот метод используется с 1998 г. для оценки более миллиона лиц в системе уголовного правосудия. При этом с 2000 г. используется компонент прогнозирования рецидивизма из шкалы COMPA (шкала риска рецидивизма). Эта компьютерная программа предсказывает риск совершения преступления лицом в течение двух лет с момента оценки на основании личных демографических данных и уголовного прошлого (Dressel & Farid, 2021). Данный метод оценки риска позволил концептуализировать «прогнозирование совершения преступлений» в качестве ключевого понятия криминологии и уголовного правосудия. Это понятие относится к рецидивизму (повторению преступления), которое играет важную роль в контроле преступности. Используя методы и технологии, позволяющие предсказать преступления, можно достичь более адекватных результатов применения мер уголовного правосудия.

Сегодня ученые признают, что инструменты управления рисками и оценки рисков, применяемые для предотвращения и прогнозирования преступлений, достойны более пристального внимания со стороны юристов и судебных органов¹. Таким образом, можно утверждать, что необходимо создать юриспруденцию рисков для судей и других органов уголовного правосудия (например, прокуратуры).

¹ A Primer on Risk Assessment Instruments for Legal Decision-Makers. Vanderbilt Law School. https://law.vanderbilt.edu/academics/academic-programs/criminal-justice-program/Primer_on_Risk_Assessment.pdf

2. Киберкриминология и виктимология

Широкое использование технологий и Интернета в современном мире, особенно с наступлением третьего тысячелетия, выдвинуло на первый план их криминальные аспекты во всех сообществах. Одним из основных аспектов развития технологий и Интернета являются киберпреступность и виктимизация. Эта проблема привлекает внимание криминологов уже несколько десятилетий. Результатом такого внимания стало развитие киберкриминологии и виктимологии.

2.1. Возникновение киберкриминологии в качестве объяснения этиологии киберпреступности

Киберкриминология – это одно из новейших направлений междисциплинарных исследований в уголовно-правовой науке, которое объединило достижения уголовного правосудия и компьютерных наук для изучения углубляющихся проблем компьютерной преступности. С развитием технологий и науки преступность и преступное поведение также изменились. Следовательно, необходимо пересмотреть теории и типологии преступности на основе этого развития. Это означает, что киберпреступность и преступники изменяются с течением времени, осваивая новую деятельность, получая новый опыт и совершенствуя навыки (Jahankhani, 2018). Киберпреступность определяется как преступная деятельность с использованием технологий и цифровизации. Она включает незаконные деяния и действия, в том числе доступ к информации, перехват или повреждение данных, вмешательство в работу компьютерных систем или устройств и т. д. Обычно киберпреступность подразделяют на преступления, связанные с информацией, и преступления, связанные с компьютерными сетями. Киберкриминология позволяет узнать, каким образом компьютеры можно использовать для совершения преступлений и какие преступления можно совершить с помощью компьютера. Как указывают некоторые авторы, «интегрированный характер Интернета и преступлений, совершаемых с его помощью, привели к экстренной необходимости анализировать киберпреступность иначе, чем другие виды преступлений» (Maheshwari, 2021).

С исторической точки зрения, начиная с 1990-х гг. криминологи обратили внимание на то, что киберпространство стало новой площадкой для совершения преступлений. Это пошатнуло парадигму классической криминологии, которая оказалась неспособна объяснить новые формы девиаций, преступлений и социального контроля в киберпространстве. Как писал основатель киберкриминологии Jaishankar, «криминология потерпела поражение в исследовании феномена киберпреступности и не смогла вовремя признать важность киберпространства в изменении природы и масштаба преступности и виктимизации» (Jaishankar, 2007). Он ввел киберкриминологию как отдельную дисциплину, чтобы объяснить и проанализировать преступления, совершаемые в Интернете. Как междисциплинарное направление, киберкриминология является областью исследований на стыке между компьютерными науками и криминологией. Jaishankar определяет киберкриминологию как «науку о причинах преступлений, совершаемых в киберпространстве, и их влияние на физический мир» (Jaishankar, 2007). В книге «Изучение преступлений и преступного поведения в Интернете с помощью киберкриминологии», вышедшей под редакцией Jaishankar, он объясняет, почему он ввел киберкриминологию как отдельную

дисциплину, изучающую киберпреступность с точки зрения общественных наук, и выделил отдельный корпус знаний для рассмотрения киберпреступности отдельно от компьютерно-технической экспертизы (Jaishankar, 2011). Будучи первопроходцем в области киберкриминологии, Jaishankar внес большой вклад в развитие теории перехода пространства для объяснения причин совершения преступлений в киберпространстве (Jaishankar, 2011). Согласно его теории, перемещение людей из физического пространства в киберпространство и наоборот происходит по-разному. Другими словами, люди действуют и ведут себя по-разному, перемещаясь из физического пространства в киберпространство (Jaishankar, 2007).

Рассматривая место киберкриминологии в дискурсе общественных и уголовно-правовых наук, некоторые ученые признают, что «хотя киберкриминология – это развивающаяся область криминологии, которая еще не получила адекватного внимания от классической криминологии, будущее обещает огромные перспективы этой новой дисциплине. По мере того, как виртуальные сообщества и электронные племена будут распространяться по киберпространству, а уровень преступности будет повышаться, киберкриминология получит толчок к развитию и свою долю внимания. Она будет по-прежнему активно искать ответы на фундаментальные вопросы о контекстах и причинах преступности в киберпространстве, как и пути достижения общественного порядка» (Ndubuez, 2019).

2.2. Необходимость кибервиктимологии для противодействия киберпреступности и виктимизации

Наряду с развитием киберкриминологии, необходимость общественно-правового взгляда на виктимизацию в киберпространстве определила появление параллельного направления исследований – кибервиктимологии. Этот термин был предложен индийскими криминологами-виктимологами К. Jaishankar и Debarati Halder для изучения виктимизации в Сети и выработки практических решений данной проблемы (Jaishankar, 2020; Halder, 2022).

В книге «Кибервиктимология: новое направление виктимологии XXI века» Jaishankar пишет: «Примечательно, что некоторые ученые не воспринимают виктимизацию от киберпреступности как новую форму виктимизации, а некоторые отказываются признавать их общие черты. В любом случае многие страны борются с виктимизацией от киберпреступности с помощью своих обычных законов, не создавая особых законов. Эти новые явления позволили изучать кибервиктимизацию с различных точек зрения. Я подчеркиваю необходимость выделить особое направление виктимологии, то есть кибервиктимологию, для изучения киберпреступности с точки зрения жертв/виктимизации, так как я убежден, что виктимизация от киберпреступности является новой формой виктимизации. В данной главе мы обсудим формирование нового направления виктимологии, называемого кибервиктимологией» (Jaishankar, 2020).

Как показал Jaishankar, виктимизация от киберпреступности является новой формой виктимизации (Jaishankar, 2020). Общим для киберкриминологии и виктимологии является изучение различных аспектов виктимизации от киберпреступности. Индийский коллега этого исследователя, Halder, также утверждает, что характеристики различных групп жертв составляют профиль жертв киберпреступности. Одним из важнейших результатов кибервиктимологии является открытие эффектов

киберпреступлений на различные слои общества. Иными словами, даже индивидуальная кибервиктимизация может повлечь за собой значительный ущерб для другого члена общества (Halder, 2022).

Что касается вопросов цифровизации и новых технологий, киберкриминология и виктимология привлекают наше внимание к Интернету и киберпространству, которые трансформировали жизнь и повседневную деятельность миллионов людей. В то же время эти новые направления общественных и уголовно-правовых наук показали, что Интернет и новые технологии как явления современного мира часто используются недобросовестно (Jaishankar, 2020). Другими словами, Интернет и киберпространство могут сыграть двоякую роль, предоставляя преступникам возможности для их противозаконной деятельности. Что касается различных форм и функций технологий, связанных с Интернетом и киберпространством, исследователи рассматривают преступления и преступную деятельность в них или посредством их, включая компьютерные преступления, цифровые преступления, преступления в сфере информационных технологий, интернет-преступления, виртуальные преступления, электронную преступность, сетевую преступность (Jaishankar, 2020).

Таким образом, нет сомнений, что Интернет и современные технологии играют важную роль в киберпреступности и защите от нее². И все же криминологически-виктимологическая точка зрения не должна игнорироваться в этом отношении, поскольку эти технологии могут предоставлять новые возможности для совершения преступлений и виктимизации онлайн и офлайн.

3. Алгоритмическая, или вычислительная, криминология

Третье направление цифровизации в криминологии, которое мы обсудим в данной статье, возникло под влиянием математики и компьютерных наук. Алгоритмическая криминология и вычислительная криминология – это синонимичные термины, обозначающие данное новое направление, которое связывает криминологию и компьютерные науки. Оно также включает прикладную математику как компьютерные симуляции преступного поведения (Berk, 2013). В свете математики и компьютерных наук криминологические теории получают новый импульс для объяснения вопросов преступности и охраны правопорядка. В то же время существенную роль в вычислительной криминологии играет статистика. Кроме страхового права, основанного на теории управления рисками и оценки риска, вычислительная криминология применяется в сфере правоприменения и системе уголовного правосудия. Она также используется для моделирования и симулирования преступных событий, таких как терроризм или киберпреступления, в сложной обстановке. Вычислительная криминология применяется посредством использования вычислительной топологии и алгоритмов, дающих информацию для теории картины преступления (Brantingham, 2011). Это направление решает задачи криминологии с помощью прикладной математики, компьютерных наук и криминологии. Прикладные методы в этой области включают составление алгоритмов, поиск данных, разработку структур данных и программного обеспечения (Harris, 2014).

² Don't Forget Victimology as a Cybersecurity Strategy. <https://www.secureworks.com/blog/dont-forget-victimology-as-a-cybersecurity-strategy>

Наряду с практическими и прикладными задачами, необходимость эмпирических исследований в криминологии, обусловленная поиском этиологии и причин преступности, требует алгоритмического подхода, в частности, для прогнозирования преступлений. Эта концепция связана с проблемой рецидивизма, которая является одной из важнейших в криминологических дискуссиях и теориях. Профилактика рецидивизма – главная цель криминологических санкций и механизмов вынесения приговора, таких как probation и условное освобождение. Эти механизмы связаны с переменной оценки риска в криминологии, что обсуждалось ранее. Они требуют тщательного изучения и точной оценки возможности рецидивизма и соответствия осужденного критериям участия в указанных программах. Прогнозирование совершения преступления занимает особое место в этих процессах изучения и оценки. Используемые при этом алгоритмические методы являются более эффективными, чем обычные методы исследования традиционной криминологии, такие как количественные и качественные оценки, наблюдения, интервью, опросы и др.

В целом преступность развивается по тем же закономерностям, что и неправомерное поведение (Brantingham, 2011). Следовательно, точное понимание этих закономерностей будет зависеть от использования современных методов и механизмов, которые применяются в алгоритмической, или вычислительной криминологии.

Выводы

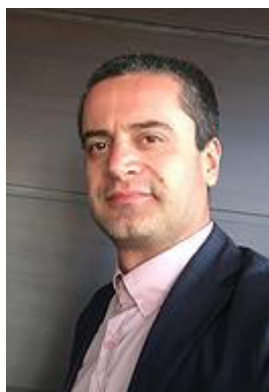
Современные технологии, Интернет и киберпространство изменили природу, типы и обстоятельства преступлений и преступников, а также инструменты контроля над ними. Новые формы преступности (например, киберпреступность) представляют более серьезную угрозу и опасность для всех слоев общества. Эта реальность значительно влияет на технологии контроля и предотвращения преступности, что в свою очередь приводит к появлению новых форм преступности. Рассматривая эти изменения в третьем тысячелетии, необходимо радикально изменить подходы к содержанию, целям, а особенно методологии криминологии, чтобы успешно разрешать проблемы и справляться с задачами, связанными с преступностью. Соответственно, криминология должна обновиться в форме различных дисциплин и разделов дисциплин, чтобы соответствовать задачам нового тысячелетия. Три направления криминологии и уголовного правосудия, обсуждавшиеся в этой статье, обнаруживают взаимосвязи и взаимовлияние друг на друга. Общим элементом их взаимодействия является цифровизация, которая ознаменовала появление современных направлений криминологии в последние десятилетия. С точки зрения взаимодействия механизмы управления рисками и оценки рисков в свете страхового права требуют использования и развертывания алгоритмической, или вычислительной, криминологии. Более того, киберкриминология и виктимология, как еще один новый тренд в этой основной дисциплине уголовно-правовой науки, явились результатом требования и запроса компьютерных наук и киберпространства по отношению к киберпреступности, киберпреступникам и их жертвам.

Список литературы

- Abubotain, F., & Chamakiotis, P. (2020). FinTech in the Saudi Context. *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*, 188–208. <https://doi.org/10.4018/978-1-5225-9550-2.ch009>
- Berk, R. (2013). Algorithmic criminology. *Security Informatics*, 2(1). <https://doi.org/10.1186/2190-8532-2-5>
- Bosworth, M. (2005). Actuarial justice. In *Encyclopedia of prisons & correctional facilities* (Vol. 1, pp. 12–14). SAGE Publications, Inc. <https://dx.doi.org/10.4135/9781412952514.n5>
- Brantingham, P. L. (2011). Computational Criminology. *2011 European Intelligence and Security Informatics Conference*. <https://doi.org/10.1109/eisic.2011.79>
- Cabada García, M. J., Quezada Ramírez, S. I., Negrete Gómez, G. A., Villarreal Serrano, E., Colín García, D. L., Villar Cantón, C., Baca Luna, A., Díaz Villanueva, P. D., & Segura-Azuara, N. D. (2022). Social Media Campaign as a Tool for Patient Education of Disease Prevention and Health Promotion: Digital Health Campaign on Osteoporosis Knowledge. In M. Lopez (Ed.), *Advancing Health Education With Telemedicine* (pp. 183–208). IGI Global. <https://doi.org/10.4018/978-1-7998-8783-6.ch010>
- Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*, 121, 105840. <https://doi.org/10.1016/j.childyouth.2020.105840>
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1). <https://doi.org/10.1126/sciadv.aao5580>
- Dressel, J., & Farid, H. (2021). The Dangers of Risk Prediction in the Criminal Justice System. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. <https://doi.org/10.21428/2c646de5.f5896f9f>
- Feeley, Malcolm M. (2004). Actuarial justice and the modern state. *Punishment, Places and Perpetrators*, 78–93. <https://doi.org/10.4324/9781843924760>
- Gassin R. (1990). *Criminologie*. Paris: Dalloz.
- Halder, D. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimization* (1st ed.). Routledge.
- Harris, P. (2014). *Computational Analysis and Public Policy of Criminology* (First). Koros Press Limited.
- Jahankhani, Hamid (2018). *Cyber Criminology*. Springer Nature Switzerland AG. <https://doi.org/10.1007/978-3-319-97181-0>
- Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *CERN European Organization for Nuclear Research – Zenodo*. <https://doi.org/10.5281/zenodo.18276>
- Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1, 7–9. <https://doi.org/10.5281/zenodo.18792>
- Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press: Taylor & Francis Group.
- Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In *An International Perspective on Contemporary Developments in Victimology*, pp. 3–19. https://doi.org/10.1007/978-3-030-41622-5_1
- Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 148, 105837. <https://doi.org/10.1016/j.aap.2020.105837>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R., 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>
- Maheshwari, R. (2021). Changing Paradigms of Victimization in Cybercrimes: An Analysis, *International Journal of Law Management & Humanities*, 4(3), 2871–2883.
- McLaughlin, E., & Muncie, J. (2019). *The Sage Dictionary of Criminology*. Sage: EBooks.
- Metcalf, C. (2004). Managing Risk and the Causes of Crime. *Criminal Justice Matters*, 55(1), 8–42. <https://doi.org/10.1080/09627250408553585>
- Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, 126, 106984. <https://doi.org/10.1016/j.chb.2021.106984>
- Ndubuez, P. N. (2019). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace, *The Nigerian Journal of Sociology and Anthropology*, 14(1), 32–48.
- O'Malley, Pat (2009). Risk and Criminology. *Legal Studies Research Paper*, 9(87), 1–29.

- Ochs, T., & Riemann, U. A. (2018). IT Strategy Follows Digitalization. *Encyclopedia of Information Science and Technology* (4th ed., pp. 873–887). <https://doi.org/10.4018/978-1-5225-2255-3.ch075>
- Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, 158, 287–294. <https://doi.org/10.1016/j.procs.2019.09.054>
- Pritchard, A. A., Blanchard, A. J. E., & Douglas, K. S. (2014). Risk Assessment. *Criminology*. <https://doi.org/10.1093/obo/9780195396607-0095>
- Sampson, F. (2014). Cyberspace. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 1–10. <https://doi.org/10.1016/b978-0-12-800743-3.00001-3>
- Scuotto, V., Serravalle, F., Murray, A., & Viassone, M. (2019). The Shift Towards a Digital Business Model. *Women Entrepreneurs and Strategic Decision Making in the Global Economy*, 120–143. <https://doi.org/10.4018/978-1-5225-7479-8.ch007>
- Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences*, 182, 590–595. <https://doi.org/10.1016/j.sbspro.2015.04.787>
- van de Weijer, S. G., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, 8, 100249. <https://doi.org/10.1016/j.chbr.2022.100249>

Сведения об авторе



Мехрдад Райеджиан Асли – доктор наук, доцент Института исследования и развития гуманитарных дисциплин

Адрес: 1463645851, Исламская Республика Иран, г. Тегеран, мост Ядегар, шоссе Аль-Ахмад

E-mail: m.rayejian@samt.ac.ir

ORCID ID: <https://orcid.org/0000-0003-0693-1888>

Web of Science Researcher ID:

<https://www.researchgate.net/profile/Mehrdad-Rayejian-Asli>

ScopusAuthorID: <https://www.scopus.com/authid/detail.uri?authorId=57195374005>

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

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 13 декабря 2022 г.

Дата одобрения после рецензирования – 18 января 2023 г.

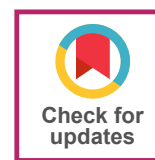
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.9>



Digital Trends of Criminology and Criminal Justice of the 21st Century

Mehrdad Rayejian Asli 

Institute for Research and Development in the Humanities (SAMT),
Tehran, Iran

Keywords

Cyber criminology,
cyber victimology,
cyber space,
criminology,
criminal law,
criminal justice,
digitalization,
digital technologies,
risk

Abstract

Objective: to define the key trends in the development of criminology and criminal justice under significant broadening of digitalization and using modern technologies.

Methods: the priority of analytical method combined with descriptive method provided an optimal set of tools for searching and revealing the main digital trends in the development of criminology and criminal justice in the 21st century.

Results: the growing dependence was revealed between criminal-legal science and digital technologies, which leads to the change in essence and types of contemporary criminality, models of criminals' behavior, methods and mechanism of crime control and prevention in the light of requirements of criminal policy and justice. The dual role of the global digitalization trend is highlighted, the achievements of which are used both by the agencies of criminal justice system (in particular, for crime control, management and prevention) and criminals when implementing their criminal intents. It was determined that the essential transformation of criminology and criminal justice is largely caused by a dramatic development of digitalization in the 21st century, as well as by the modern technologies created on its basis, which appear to be more effective than the standard methods of traditional criminology, including quantitative and qualitative estimations, observation, interviews, polls, etc.

Scientific novelty: new spheres of criminal-legal knowledge are introduced, as well as the corresponding disciplines formed exclusively under the influence of digitalization, such as cyber criminology and cyber victimology; algorithmic (computational) criminology, based on actuarial justice and the theory of risks, is highlighted as the most recent trend in criminological science.

Practical significance: the account of trends and positive experience gained in the sphere of digitalization determines the successful solution of the tasks associated with crime counteraction, transformation of approaches to the content, goals and

© Rayejian Asli 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.

methodology of applied criminology and criminal justice. The global megatrend of digitalization essentially changes the appearance of the criminal-legal science, sets the new theoretical and applied directions of its development. Timely upgrade and adaptation of knowledge, skills and capabilities in compliance with the achievements of digitalization will allow criminology and criminal justice to correspond to the tasks of the new millennium.

For citation

Rayejian Asli, M. (2023). Digital Trends of Criminology and Criminal Justice of the 21st Century. *Journal of Digital Technologies and Law*, 1(1), 235–250. <https://doi.org/10.21202/jdtl.2023.9>

References

- Abubotain, F., & Chamakiotis, P. (2020). FinTech in the Saudi Context. *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*, 188–208. <https://doi.org/10.4018/978-1-5225-9550-2.ch009>
- Berk, R. (2013). Algorithmic criminology. *Security Informatics*, 2(1). <https://doi.org/10.1186/2190-8532-2-5>
- Bosworth, M. (2005). Actuarial justice. In *Encyclopedia of prisons & correctional facilities* (Vol. 1, pp. 12–14). SAGE Publications, Inc. <https://dx.doi.org/10.4135/9781412952514.n5>
- Brantingham, P. L. (2011). Computational Criminology. *2011 European Intelligence and Security Informatics Conference*. <https://doi.org/10.1109/eisic.2011.79>
- Cabada García, M. J., Quezada Ramírez, S. I., Negrete Gómez, G. A., Villarreal Serrano, E., Colín García, D. L., Villar Cantón, C., Baca Luna, A., Díaz Villanueva, P. D., & Segura-Azuara, N. D. (2022). Social Media Campaign as a Tool for Patient Education of Disease Prevention and Health Promotion: Digital Health Campaign on Osteoporosis Knowledge. In M. Lopez (Ed.), *Advancing Health Education With Telemedicine* (pp. 183–208). IGI Global. <https://doi.org/10.4018/978-1-7998-8783-6.ch010>
- Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*, 121, 105840. <https://doi.org/10.1016/j.childyouth.2020.105840>
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1). <https://doi.org/10.1126/sciadv.aao5580>
- Dressel, J., & Farid, H. (2021). The Dangers of Risk Prediction in the Criminal Justice System. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. <https://doi.org/10.21428/2c646de5.f5896f9f>
- Feeley, Malcolm M. (2004). Actuarial justice and the modern state. *Punishment, Places and Perpetrators*, 78–93. <https://doi.org/10.4324/9781843924760>
- Gassin R. (1990). *Criminologie*. Paris: Dalloz.
- Halder, D. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimisation* (1st ed.). Routledge.
- Harris, P. (2014). *Computational Analysis and Public Policy of Criminology* (First). Koros Press Limited.
- Jahankhani, Hamid (2018). *Cyber Criminology*. Springer Nature Switzerland AG. <https://doi.org/10.1007/978-3-319-97181-0>
- Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *CERN European Organization for Nuclear Research – Zenodo*. <https://doi.org/10.5281/zenodo.18276>
- Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1, 7–9. <https://doi.org/10.5281/zenodo.18792>
- Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press: Taylor & Francis Group.
- Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In *An International Perspective on Contemporary Developments in Victimology* (pp. 3–19). https://doi.org/10.1007/978-3-030-41622-5_1

- Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 148, 105837. <https://doi.org/10.1016/j.aap.2020.105837>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R., 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>
- Maheshwari, R. (2021). Changing Paradigms of Victimization in Cybercrimes: An Analysis, *International Journal of Law Management & Humanities*, 4(3), 2871–2883.
- McLaughlin, E., & Muncie, J. (2019). *The Sage Dictionary of Criminology*. Sage: EBooks.
- Metcalf, C. (2004). Managing Risk and the Causes of Crime. *Criminal Justice Matters*, 55(1), 8–42. <https://doi.org/10.1080/09627250408553585>
- Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, 126, 106984. <https://doi.org/10.1016/j.chb.2021.106984>
- Ndubuez, P. N. (2019). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace, *The Nigerian Journal of Sociology and Anthropology*, 14(1), 32–48.
- O'Malley, Pat (2009). Risk and Criminology. *Legal Studies Research Paper*, 9(87), 1–29.
- Ochs, T., & Riemann, U. A. (2018). IT Strategy Follows Digitalization. *Encyclopedia of Information Science and Technology* (4th ed., pp. 873–887). <https://doi.org/10.4018/978-1-5225-2255-3.ch075>
- Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, 158, 287–294. <https://doi.org/10.1016/j.procs.2019.09.054>
- Pritchard, A. A., Blanchard, A. J. E., & Douglas, K. S. (2014). Risk Assessment. *Criminology*. <https://doi.org/10.1093/obo/9780195396607-0095>
- Sampson, F. (2014). Cyberspace. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 1–10. <https://doi.org/10.1016/b978-0-12-800743-3.00001-3>
- Scuotto, V., Serravalle, F., Murray, A., & Viassone, M. (2019). The Shift Towards a Digital Business Model. *Women Entrepreneurs and Strategic Decision Making in the Global Economy*, 120–143. <https://doi.org/10.4018/978-1-5225-7479-8.ch007>
- Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences*, 182, 590–595. <https://doi.org/10.1016/j.sbspro.2015.04.787>
- van de Weijer, S. G., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, 8, 100249. <https://doi.org/10.1016/j.chbr.2022.100249>

Author information



Mehrdad Rayejian Asli – Assistant Professor of Institution for Research and Development in the Humanities (SAMT); Deputy of Research in the UNESCO Chair for Human Rights, Peace and Democracy, Tehran, Iran

Address: 1463645851, SAMT Organization, Al-e-Ahmad Highway, Yadegar Bridge, Tehran, Iran

E-mail: m.rayejian@samt.ac.ir

ORCID ID: <https://orcid.org/0000-0003-0693-1888>

Web of Science Researcher ID:

<https://www.researchgate.net/profile/Mehrdad-Rayejian-Asli>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57195374005>

Google Scholar ID: <https://scholar.google.com/citations?user=WKgazNEAAAAJ&hl=en>

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – December 13, 2022

Date of approval – January 18, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023

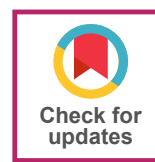


Научная статья

УДК 343.3/.7:004

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

DOI: <https://doi.org/10.21202/jdtl.2023.10>



Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию

Елена Юрьевна Антонова 

Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации
г. Владивосток, Российская Федерация

Ключевые слова

Вербовка,
криминализация,
право,
преступление,
пропаганда,
пространство,
противодействие,
терроризм,
финансирование,
цифровые технологии

Аннотация

Цель: выработка рекомендаций по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Методы: методологическую основу исследования составляют всеобщий диалектический метод познания, совокупность общенаучных и частнонаучных методов исследования, таких как анализ, синтез, логический, восхождения от абстрактного к конкретному, индукция, дедукция и др.

Результаты: определено, что развитие цифрового (кибер-) пространства и цифровых технологий способствует интенсивности терроризма, а также привело к изменению механизма совершения преступлений террористической направленности. Сделан вывод о том, что для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий, необходимы четкая стратегия и соответствующая нормативная правовая база.

Научная новизна: в работе проанализированы такие формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, как распространение идеологии насилия и пропаганда террористической деятельности, вербовка новых членов и их обучение, применения цифровых технологий в процессе приговорительной и непосредственной террористической деятельности, финансирование.

© Антонова 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.

Выявлены преимущества использования цифрового пространства и (или) цифровых технологий в процессе совершения преступлений террористической направленности. Изменение механизма совершения преступлений террористической направленности в связи с использованием цифровых технологий, по мнению автора, должно учитываться в процессе криминализации (изменении интенсивности пенализации) общественно опасных деяний. К важным направлениям государственной политики в сфере противодействия данным преступлениям отнесены воспитательно-просветительская деятельность, обучение сотрудников правоохранительных органов, расширение их полномочий для обеспечения четкого и эффективного контроля цифрового контента.

Практическая значимость: определяется возможностью использования сформулированных выводов и предложений для дальнейшей научной разработки уголовной политики государства в сфере противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Для цитирования

Антонова, Е. Ю. (2023). Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию. *Journal of Digital Technologies and Law*, 1(1), 251–269. <https://doi.org/10.21202/jdtl.2023.10>

Содержание

Введение

1. Формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий
 - 1.1. Распространение идеологии насилия, пропаганда террористической деятельности через цифровое (кибер-) пространство
 - 1.2. Вербовка новых членов террористических формирований и их обучение
 - 1.3. Применение цифровых технологий в процессе приготовительной и непосредственной террористической деятельности
 - 1.4. Цифровые каналы финансирования терроризма
2. Преимущества использования цифрового пространства и (или) цифровых технологий в процессе совершения преступлений террористической направленности
3. Противодействие преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий

Выводы

Введение

Преступления в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий/систем/программ представляют естественную эволюцию преступности, обусловленную научно-техническим прогрессом и новыми разработками, и относятся к числу серьезных проблем современного мира.

Не являются исключением и преступления террористической направленности. Отмечается, что уровень терроризма продолжает расти, как и «технологические достижения, способствующие привлечению внимания и эмоционального воздействия террористов» (Orehek & Vazeou-Nieuwenhuis, 2014). Исследователями фиксируется прямая связь между цифровым (кибер-) пространством и различными формами социально-политической дестабилизации: антиправительственными демонстрациями, беспорядками и террористическими актами (Khokhlov & Korotayev, 2022).

Заместитель секретаря Совета безопасности России Ю. Коков справедливо замечает, что наступает эра цифрового терроризма, который по масштабам возможных последствий может быть сопоставим с оружием массового уничтожения. По его данным, в Интернете действуют около 30 тыс. террористических и экстремистских сайтов¹. Данные обстоятельства требуют серьезной работы по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий/систем/программ.

1. Формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий

Лица, вовлеченные в террористическую деятельность, активно используют современные цифровые технологии как в процессе совершения преступлений, так и в повседневной жизни. Такие технологии применяются внутри террористических сообществ/организаций (далее – формирований) в качестве инструмента коммуникации, в том числе в процессе организации и руководства террористической деятельностью, а также при вербовке новых членов террористических формирований, распространении идеологии насилия, пропаганды террористической деятельности, призывов к совершению конкретных террористических актов. Члены террористических формирований стремятся донести такие сообщения, а также продемонстрировать свои противоправные деяния максимально широкой аудитории, поскольку основной их целью является дестабилизация общества, его моральная и политическая нестабильность.

¹ СБ РФ: цифровой терроризм может быть сопоставим с оружием массового уничтожения. (2022, 18 мая). ТАСС. <https://tass.ru/politika/14658343/amp>

1.1. Распространение идеологии насилия, пропаганда террористической деятельности через цифровое (кибер-) пространство

Идеология насилия играет одну из ведущих ролей в совершении преступлений террористической направленности (Антонова, 2018). Терроризм – это политический инструмент, требующий мотивации и способностей, которые определяют его масштабы, происхождение, идеологию и контрстратегии (Orehek & Vazeou-Nieuwenhuis, 2014). Отмечается, что успех ИГИЛ* зависит в том числе от того, что группа «работает как организация хорошо подготовленных, идеологически мотивированных и безжалостных бойцов» (Makinda, 2016). Интернет стал неуправляемым цифровым пространством, используемым в том числе для распространения и культивирования идеологии терроризма.

К примеру, субъекты групп крайне правого крыла (XRW) используют Интернет для обращения в свою веру, пропаганды зверств террористов и для их максимальной огласки, транслируя свои атаки в прямом эфире. Так, из 22 террористических заговоров, раскрытых в Великобритании, в период с марта 2017 г. по сентябрь 2019 г., семь были вдохновлены идеологией XRW. В этот же период лица, вдохновленные идеологией XRW, совершили три террористических акта со смертельным исходом (Zedner, 2021). Таким образом, в цифровую эпоху можно чувствовать себя очень тесно связанным с онлайн-группами и онлайн-контактами, которые могут иметь схожие интересы и идеологию насилия (Liem et al., 2018), хотя и не быть членом этих групп, действуя в одиночку, в том числе в террористических целях.

Террористические формирования пользуются тем, что цифровое (кибер-) пространство позволяет передавать информацию мгновенно, за считанные секунды, на неопределенно широкую территорию. Через Интернет, мобильные устройства и платформы социальных сетей быстро распространяется очень возбуждающий и потенциально тревожный видеоконтент событий, в том числе в прямом эфире можно наблюдать за международными террористическими атаками, сопровождающимися взрывами и стрельбой (Huddy et al., 2021). Кроме того, по каналам социальных сетей происходит реагирование официальных властей и широкой общественности на опасные ситуации. Растущий рост использования Twitter** и Facebook*** во время чрезвычайных ситуаций является ярким свидетельством того, что общественность принимает публикуемую или размещаемую в цифровом (кибер-) пространстве информацию как «правду». Несмотря на то, что настоящее время называют эпохой фальшивых новостей или дезинформации, общественность по-прежнему в целом доверяет информации, получаемой в Интернете или социальных сетях (Grobbelaar, 2022).

Распространяя через цифровое (кибер-) пространство информацию, не всегда соответствующую действительности (это может быть и дезинформация, слухи, угрозы применения насилия или изображения актов насилия), террористические формирования оказывают воздействие не только на возможных или действительных сторонников террористических воззрений, идеологии насилия (что используется в первую очередь для вербовки новых членов, радикализации, подстрекательства к терроризму, подрыва веры в социальные ценности), но и на прямых или косвенных жертв террористических актов (устрашение населения путем психологического манипулирования, распространения чувств повышенного беспокойства, тревоги, страха или паники среди населения) или на органы власти и международное сообщество в целом (дестабилизация деятельности органов власти или международных организаций либо воздействие на принятие ими решений).

Это обусловлено и тем обстоятельством, что терроризм понимают и как преднамеренное использование или угрозу применения насилия отдельными лицами или субнациональными группами для достижения политической или социальной цели путем запугивания большой аудитории, помимо непосредственной жертвы (Sandler, 2013). Так, в период с 2014 по 2017 г. ИГИЛ* обезглавила 296 человек и опубликовала видеозаписи западных заложников, в том числе американских журналистов Джеймса Фоули и Стивена Сотлоффа, а также британских гуманитарных работников Дэвида Хейнса и Алана Хеннинга. Все четверо заложников были казнены в 2014 г. В ходе опроса HuffPost-YouGov, проведенного в ноябре 2014 г., 32 % американцев заявили, что видели, по крайней мере, несколько видеороликов с обезглавливанием ИГИЛ*, а 9 % заявили, что видели фактическое обезглавливание. Согласно данным, полученным на национальном уровне от репрезентативной онлайн-группы, опрошенной примерно через шесть-девять месяцев после самых известных казней в США, 25 % американцев заявили, что видели часть или все видео с обезглавливанием (Huddy et al., 2021). Такие действия направлены в первую очередь на устрашение населения и распространение чувства повышенной тревоги и страха, которые могут привести к панике среди населения.

Кроме того, действия террористов часто направлены на то, чтобы спровоцировать реакцию правительства, такую как территориальные уступки или политические реформы посредством актов запугивания, которые истощают решимость противостоящего правительства или подчеркивают его неэффективность (Huddy et al., 2021). Именно поэтому террористические формирования стремятся адаптировать экстремальные средства коммуникации для привлечения внимания и видимости в глобальной медиасреде. Насилие террористов, в высшей степени опосредованное и зрелищное, порождает превращение атак в медиасобытия, которые разворачиваются в гибридном пространстве и укореняются в доступных возможностях и технологиях (Uusitalo et al., 2021).

Для совершения пропагандистских действий террористические формирования задействуют широкий спектр технических средств: веб-сайты, чат-группы и чат-форумы, онлайн-журналы, платформы таких социальных сетей, как Twitter** и Facebook***, популярные видео- и файлообменные веб-сайты, например, YouTube. Поисковые системы Интернета упрощают нахождение террористического контента.

На слушаниях в подкомитете по информации и борьбе с терроризмом Комитета Национальной безопасности палаты представителей Правительства США были приведены примеры использования террористами систем искусственного интеллекта (далее – ИИ). Так, один из сторонников превосходства белой расы открыл огонь по двум мечетям в Крайстчерче (Новая Зеландия), убив 51 человека и ранив еще 49. Террорист смог транслировать нападение в прямом эфире на Facebook***, потому что ИИ этой сети не счел отснятый материал достаточно ужасным. Затем видео было 300 000 раз успешно загружено на Facebook*** другими пользователями. Это доказывает, что технологии ИИ, призванные блокировать такие видео, еще не справляются с поставленной задачей. Более того, имеются факты, свидетельствующие о том, что ИИ Facebook*** снимает видео и продвигает террористический контент, который он должен был удалить².

² Artificial Intelligence and Counterterrorism: Possibilities and Limitations. (2020). *Hearing Before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security House of Representatives One Hundred Sixteenth Congress. First Session. June 25, 2019* (Serial № 116-28). Washington: U.S. Government Publishing Office.

Но даже если преступники не транслируют атаку в прямом эфире, свидетели визуально записывают события, и эти видеоматериалы включаются в сегменты новостей, которые часто загружаются на онлайн-сайты, такие как YouTube, а также на платформы социальных сетей, такие как WhatsApp и Snapchat. Этот необработанный графический видеоконтент легкодоступен (иногда сопровождается необоснованным предупреждением) и может вызвать сильные эмоции у зрителей, потенциально усиливая общественную реакцию на акт террора (Huddy et al., 2021).

1.2. Вербовка новых членов террористических формирований и их обучение

Важную роль в деятельности террористических формирований играет вербовка новых членов, поскольку неспособность набрать достаточное количество членов и провести успешные атаки свидетельствует о слабости группы (Polo, 2020). Развитие информационных-телекоммуникационных технологий, особенно Интернета и его инструментов, обеспечивает платформу, используемую террористическими формированиями для вербовки новых членов и распространения своей пропаганды (Dingji Maza, 2020), а также для их онлайн-обучения и планирования террористических атак.

Так, использование «Аш-Шабааб» видео и сообщений через Интернет сделало эту террористическую организацию известной во всем мире. До 2009 г. «Аш-Шабааб» набирала в свои ряды исключительно сомалийцев. Однако с тех пор, как начались их публичные связи с «Аль-Каидой»*, были завербованы иностранные боевики, которые идеологически отождествляли себя с глобальным джихадом. Один из их самых известных международных бойцов Омар Хаммами, также известный как Абу Мансур аль-Амрики, начиная с 2010 г. регулярно публиковал в Интернете сообщения и распространял их как вербовка «Аш-Шабааб» (Grobbelaar, 2022).

Отмечается, что создание локальных сетей террористических формирований или присоединение к ним способствует передаче знаний и обучению; позволяет проводить совместные тренировки и планирование атак; увеличивает доступность, поставку и обмен оружия, личного состава и другого капитала, связанного с терроризмом; локальные сети даже позволяют группам создавать альянсы, объединяться и проводить скоординированные кампании против государства. Террористические сети, таким образом, действуют как решающий фактор, увеличивающий силу, поддерживая потенциал групп, их возможности и эффективность (Polo, 2020).

Кроме того, специализированные террористические сайты работают как онлайн-библиотеки идеологических текстов, платформы для вербовщиков и форумы для обмена информацией. Фото- и видеоматериалы, игры (имитирующие террористические атаки и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста), учебные пособия и технические инструкции, подготовленные террористическими группами, способствуют радикализации их сторонников (Khokhlov & Korotayev, 2022). Пропагандистские материалы могут содержать идеологические или практические руководства, разъяснения, оправдания или рекламу деятельности террористов.

Так, в ходе проверки Шахунской городской прокуратурой Нижегородской области интернет-ресурсов, осуществляемой с использованием программы браузера Google Chrome, в поисковом ресурсе «Яндекс» при введении ключевых слов: «Expedient Homemade Firearms», отобразился список интернет-сайтов, содержащий ссылки:

<данные изъяты>. На указанных интернет-страницах размещена подробная информация о способах самостоятельного изготовления оружия, проходит ее обсуждение. Доступ к материалам свободный для всех пользователей, сайт и интернет-страницы не содержат ограничений к его доступу по кругу лиц, не требуются предварительная регистрация и пароль, ознакомиться с содержанием данной интернет-страницы и скопировать материалы в электронном варианте может любой пользователь, ограничения на передачу, копирование и распространение отсутствуют³.

Как отмечают специалисты, воздействие на компьютерную информацию позволяет преступнику «манипулировать эмоциями и сознанием потерпевшего, вызывая серьезные психофизиологические последствия. Психоэмоциональный эффект сравним по силе с эффектом от событий в реальном мире, в то же время он смоделирован путем изменения компьютерной информации» (Дремлюга, 2022).

Исследования показывают, что социальные движения часто используют цифровое медиапространство для работы с идентификацией, используя цифровые сообщения для развития здравого смысла «мы» (Gaudette et al., 2020). Собраны значительные доказательства того, что социальные медиа стали местом формирования идентичностей и способствуют формированию сообществ с сильным чувством групповой солидарности (Törnberg & Törnberg, 2022). К таким психологическим приемам и прибегают террористические формирования в процессе вербовки новых членов и пропаганды своей идеологии.

1.3. Применение цифровых технологий в процессе приговорительной и непосредственной террористической деятельности

В науке отмечаются феноменальные успехи систем ИИ не только в области цифровых платформ, но и в материальной, непосредственной среде. Это напрямую видно на примере внедрения цифровых технологий (современной робототехники) в систему беспилотного управления транспортных средств, что облегчает совершение террористических актов. Уже на практике встречаются случаи применения цифровых технологий, в том числе беспилотников, в процессе приговорительной и непосредственной террористической деятельности, в частности для доставки наркотиков, психоактивных веществ и других запрещенных предметов – оружия, взрывчатых веществ, взрывных устройств и пр.

Так, террористические группы все чаще используют беспилотники для наблюдения, взрывов и других общественно опасных действий как на стадии приговорения, так и непосредственного совершения актов терроризма. Сообщается, что ИГИЛ* начала использовать боевые дроны в Ираке и объявила о создании подразделения «Беспилотные летательные аппараты моджахедов»⁴. Кроме того, ИГИЛ* провела несколько бомбардировок с использованием беспилотников, нацеленных

³ Архив Шахунского районного суда Нижегородской области. Решение № 2А-214/2021 от 22 марта 2021 г. Дело № 2А-214/2021. (2021). Судебные и нормативные акты РФ. <https://sudact.ru/regular/doc/AAQ1OEJsQbb9/>

⁴ Joby, Warrick. (2017, February 17). Use of weaponized drones by ISIS spurs terrorism fears. *The Washington Post*. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

как на гражданские, так и на военные цели, и даже предпринимала попытки атаковать беспилотниками глав государств⁵. По мере увеличения производства этих гаджетов и снижения себестоимости эти новшества станут более привлекательными и полезными для отдельных террористов и террористических формирований. Ножи и грузовики все еще могут быть более простыми и дешевыми вариантами, но новые методы террористической атаки начнут реализовываться⁶.

3D-принтеры также могут сделать сложные и дорогие технологии доступными для террористов. Так, напавший на немецкую синагогу в Йом-Кипур в начале октября 2019 г. использовал напечатанные на 3D-принтере компоненты самодельного оружия⁷. В 2020 г. немецкий террорист потратил всего 50 долларов на 3D-печать деталей для оружия, которое использовалось при попытке нападения в Галле⁸.

Цифровое (кибер-) пространство используется и в качестве средства для совершения кибератак, призванных нарушить нормальное функционирование компьютерных систем, серверов с помощью компьютерных вирусов, вредоносных и шпионских программ или других средств неправомерного доступа к компьютерной информации. Этим действиям характерны такие черты террористического акта, как стремление путем устрашения населения способствовать дестабилизации деятельности органов власти или международных организаций, воздействовать на принятие ими решений и таким образом достичь политических или иных социальных целей.

1.4. Цифровые каналы финансирования терроризма

Для достижения поставленных целей и эффективной деятельности террористические формирования привлекают значительные материальные (финансовые) ресурсы. Цифровое (кибер-) пространство и новые цифровые технологии только способствуют быстрому получению доходов, которые в последующем используются для нужд террористов.

Различные исследования показывают, что террористические группы, такие как «Аль-Каида»*, «Хамас» и моджахеды, получают финансирование и поддержку посредством цифровых платежей от групп и отдельных лиц, симпатизирующих их делу. Примеры таких цифровых платежей включают интернет-банкинг, мобильный перевод средств, онлайн-торговлю и более широкое использование криптовалют, таких как биткоин (Dingji Maza et al., 2020). Руководитель Антитеррористического центра СНГ А. Новиков отмечает, что «произошла цифровая трансформация механизмов и каналов финансирования терроризма». В качестве источников доходов террористы используют онлайн-казино, прибегают к хищениям денежных средств через подставные интернет-магазины и сайты-двойники, используют фишинговые и фарминг-атаки, не санкционированный доступ к банковским ресурсам и криптовалютным биржам⁹.

⁵ Gavin, J. *Trends in Terrorism* [2022]. Vision of Humanity. <https://www.visionofhumanity.org/trends-in-terrorism/>

⁶ Noor, E. (2020, January 29). *Sharing space: Tech and terrorism*. Observer Research Foundation. <https://www.orfonline.org/expert-speak/sharing-space-tech-terrorism-60862/>

⁷ Beau Jackson. (2019, October 18). "Interview with the ICSR: A 3D printed gun was not used in the Halle terror attack". *3D Printing Industry*. <https://3dprintingindustry.com/news/interview-with-the-icsr-a-3d-printed-gun-was-not-used-in-the-halle-terrorattack-163643/>

⁸ Gavin, J. *Trends in Terrorism* [2022]. Vision of Humanity. <https://www.visionofhumanity.org/trends-in-terrorism/>

⁹ *Террористы все активнее используют IT-технологии, заявили в АТЦ СНГ*. (2020, 3 марта). РИА Новости. <https://ria.ru/amp/20200218/1564913906.html>

Кроме того, через цифровое (кибер-) пространство террористические формирования обращаются с прямыми просьбами о пожертвованиях. Для этого используются веб-сайты, чат-группы, массовые рассылки сообщений с просьбами о пожертвованиях.

Так, Северо-Кавказский окружной военный суд вынес обвинительный приговор в отношении Ш., который опубликовал в Интернете призыв к сбору денежных средств на нужды ИГ*. Полученные деньги он перевел на счет террористической группировки¹⁰. В другом случае следствием и судом установлено, что М. перечислил через платежный терминал 7 000 руб. на счет электронного кошелька, который использовался для сбора денежных средств с целью оказания финансовой помощи членам группировки «Хайят Тахрир аш-Шам»*, являющейся структурным подразделением запрещенной террористической организации «Джебхат ан-Нусра»*¹¹.

Веб-сайты используются и в качестве интернет-магазинов, предлагающих книги, аудио-, видеозаписи и иные материалы с соответствующим содержанием. Продажа такого товара позволяет не только получить дополнительный доход, но и способствует распространению идеологии терроризма.

2. Преимущества использования цифрового пространства и (или) цифровых технологий в процессе совершения преступлений террористической направленности

Преимущества использования цифрового пространства и (или) цифровых технологий обусловлены, во-первых, скоростью передачи данных и распространения информации (дезинформации), а также обработки большого массива информации, позволяющей, например, оперативно отыскивать сторонников, вербовать новых членов террористических формирований и т. д.; во-вторых, охватом неопределенно широкой аудитории и расширением географии распространения деструктивной идеологии насилия в условиях относительной анонимности; в-третьих, сложностью контроля содержания части распространяемой информации; в-четвертых, упрощением координации действий членов террористических формирований.

Кроме того, к очевидным преимуществам цифровых технологий относят возможность их использования на любых, в том числе представляющих опасность территориях (зоны военных конфликтов); физическую безопасность субъектов, их применяющих (при использовании опасных предметов – химических, отравляющих или взрывчатых веществ и др.), и сложность их обнаружения (Антонова, 2022).

Перечисленные и иные факторы во многих случаях увеличивают степень общественной опасности совершаемых деяний, что должно быть отражено и в нормах уголовного закона.

¹⁰ В Дагестане суд приговорил собиравшего средства для ИГ мужчину к 17 годам (2019, 2 августа). РБК. <https://www.rbc.ru/rbcfreenews/5d44544c9a7947190c12566e>

¹¹ В Российской Федерации вынесен приговор за финансирование терроризма. (2020, 30 сентября). Eurasian Group. URL: <https://eurasiangroup.org/ru/sentence-for-terrorist-financing-in-russian-federation34>

Особо привлекательной для террористических формирований в этом плане является несовершеннолетняя аудитория, поскольку она не имеет необходимого жизненного опыта, устойчивых положительных ориентаций и является активным пользователем цифрового (кибер-) пространства. К тому же как отмечается в научной литературе, «подростки подвержены формированию установок на агрессивное поведение». Наиболее действенными в отношении них являются технологии разжигания агрессии посредством экстремистских лозунгов, политизации социально-экономических проблем, романтизации образов «отрицательных героев», навязывания идей, пропагандирующих насилие как социальную норму и погружения их в деструктивные интернет-сообщества (Щетинина, 2018). Для вербовки несовершеннолетних применяются популярные музыкальные видеоролики, компьютерные игры, мультипликационные фильмы, рассказы, поощряющие и прославляющие действия террористов, миссии террористов-смертников и др.

Так, трое 15-летних подростков с октября 2019 г. по июнь 2020 г. «путем общения в одной из социальных сетей и мессенджерах, придерживаясь идей анархизма... объединились в группу для последующего совместного осуществления террористической деятельности на территории города Канска». Распределив между собой роли, подростки самостоятельно проходили обучение путем чтения запрещенной, признанной решением суда экстремистской литературы и просмотра видеофильмов по изготовлению взрывчатых веществ и взрывных устройств в целях осуществления террористической деятельности. Они самостоятельно изготавливали взрывчатые вещества и взрывные устройства и отрабатывали их применение на практике в заброшенном доме, на пустырях и стройках с целью подготовки к совершению террористического акта путем подрыва здания полиции или Управления Федеральной службы безопасности (далее – ФСБ). В материалах дела фигурировали скриншоты переписок в социальных сетях, в которых фигуранты дела обсуждали, где и как приобрести компоненты взрывчатки. Кроме того, школьники намеревались «для наглядности» построить в игре Minecraft здание ФСБ и взорвать его¹².

Все вышесказанное подтверждается и специалистами в области противодействия терроризму. Так, директор Контртеррористического управления Организации Объединенных Наций В. Воронков отмечает, что террористы активно пользуются различными технологическими достижениями. Используя социальные сети, зашифрованные сообщения («даркнет»), они распространяют свою человеконенавистническую идеологию, собирают и переводят средства, радикализуют молодежь и вербуют новых сторонников, координируют теракты. Причем они задействуют алгоритмы социальных сетей так, чтобы как можно быстрее и шире распространять свой контент. Есть данные о попытках террористического подполья использовать лекарственные препараты для создания биологического оружия. Для доставки химических, биологических или радиологических материалов террористы могут применять беспилотники, в том числе автоматические¹³.

¹² Подростка из Канска приговорили к 5 годам колонии за подготовку теракта. (2022, 10 февраля). Деловой Петербург. https://www.dp.ru/a/2022/02/10/Podrostka_iz_Kanska_prigo

¹³ В Минске обсуждают возможности новых технологий и искусственного интеллекта в борьбе с терроризмом. (2019, 3 сентября). Организация Объединенных Наций. <https://news.un.org/ru/story/2019/09/1362292>

3. Противодействие преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий

Сложность противодействия цифровой преступности в первую очередь обусловлена тем, что она «не поддается внятному количественному измерению; объяснение этому имеет комплексный характер: противоречия действующего нормативного регулирования, несовершенство правоприменительной деятельности и механизмов статистического учета... бесчисленность и постоянно видоизменяющаяся природа цифровой преступности» (Рускевич и др., 2022).

Для противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, требуется выработка эффективных механизмов, в том числе уголовно-правового воздействия, которые позволят своевременно реагировать на террористические угрозы в цифровой среде.

Отметим, что сложность противодействия общественно опасным деяниям, в том числе террористической направленности, совершаемым в цифровом пространстве, как правило, приводит к изменениям в нормативных правовых базах государств. Чаще всего такие изменения связаны с усилением правовой ответственности за совершение подобных деяний.

Так, в связи с тем, что виновными в терроризме часто являются субъекты-одиночки, радикализирующиеся в Интернете, в Разделе 3 Закона Великобритании о борьбе с терроризмом и безопасности границ (CTBSA) 2019 г. установлена уголовная ответственность за однократный просмотр в Сети «материалов, которые могут быть полезны лицу, совершающему или готовящему террористический акт». Такое деяние влечет назначение максимального наказания в виде 15 лет лишения свободы (Zedner, 2021).

В российское уголовное законодательство также вносятся изменения: нормы дополняются квалифицирующим (особо квалифицирующим) признаком «совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет», видоизменяются и появляются новые нормы о преступлениях в сфере компьютерной информации. Несмотря на все законодательные нововведения констатировать наличие должной, эффективной системы мер уголовно-правового воздействия на лиц, совершающих рассматриваемые деяния в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, пока нельзя. Анализ норм уголовного закона показывает, что к настоящему времени российский законодатель усилил лишь ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма (ст. 2052), в случае их совершения в цифровом (кибер-) пространстве (ч. 2). Во всех остальных нормах о преступлениях террористической направленности соответствующий квалифицирующий (особо квалифицирующий) признак отсутствует. Вместе с тем практика показывает, что цифровое (кибер-) пространство используется не только для распространения пропагандистской информации в террористических целях, но и для содействия террористической деятельности, включая вербовку новых членов террористических формирований, финансирование, обучение исполнителей, подстрекательство к совершению террористических актов и др.

Следует иметь в виду, что противодействовать преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или)

с использованием цифровых технологий, только путем криминализации новых общественно опасных деяний или усиления интенсивности пенализации невозможно. Необходимо четкое понимание механизма совершения таких преступлений. Отсюда новые задачи стоят и перед правоохранными органами, которые должны уметь оперативно выявлять источник террористической угрозы и блокировать/ликвидировать его.

К тому же, как отмечается в научной литературе, быстрое развитие цифровых технологий, интеллектуальных устройств и социальных сетей ухудшило способность сотрудников служб общественной безопасности управлять общественным реагированием на террористическую атаку. Поскольку люди (спецслужбы) все больше полагаются на цифровые технологии, неизвестно как они начнут действовать в случае сбоя киберсистем. В связи с этим возрастает вероятность каскадной катастрофы и возникновения киберуязвимости (Keenan, 2019). Все это может быть использовано террористическими формированиями и должно учитываться при выработке мер по противодействию таким преступлениям.

Выводы

Проведенный анализ различных форм преступной деятельности террористических формирований, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, позволяет констатировать, что:

1) развитие цифрового (кибер-) пространства (социальных сетей, электронных СМИ и других интернет-ресурсов), увеличение числа пользователей таким пространством и цифровыми технологиями/системами/программами способствуют расширению идеологии насилия за счет активной пропагандистской деятельности террористических формирований и, как результат, интенсивности терроризма;

2) использование цифровых технологий террористическими формированиями, по сути, ведет к изменению механизма совершения преступлений террористической направленности – от стадии приготовления до оконченого преступления и сокрытия его следов.

Данные обстоятельства должны быть учтены и при выработке конструктивных, эффективных мер по противодействию преступлениям террористической направленности. Современные цифровые технологии необходимо активнее использовать в процессе выявления, раскрытия и расследования преступлений террористической направленности, особенно когда таковые совершаются в цифровом (кибер-) пространстве, а также с использованием IT-технологий. Важным аспектом в этой связи является возможность использования ИИ оперативно-разыскными подразделениями (например, система распознавания лиц, идентификация личности, номеров транспортных средств, мониторинг социальных сетей и т. д.).

Цифровое (кибер-) пространство может эффективно быть использовано для проведения оперативно-разведывательных действий, сбора информации, извлекаемой из сообщений на веб-сайтах, в чатах и других цифровых ресурсах, что будет способствовать своевременному предотвращению и пресечению террористических актов, сбору доказательственной базы для привлечения субъектов террористической деятельности к уголовной ответственности.

Еще одной контрмерой является создание веб-сайтов, чат-групп, чат-форумов и других интернет-платформ для ведения конструктивных онлайн-дискуссий, демонстрации контртеррористических и иных воспитательно-просветительских материалов, опирающихся на конкретные факты, изложения альтернативных ненасильственных методов решения политических и иных социальных проблем.

Для эффективного выявления, раскрытия и расследования преступлений террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, сотрудники правоохранительных органов должны обладать не только правовыми, но и специальными техническими знаниями по механизму совершения данных преступлений. Они должны знать современные цифровые (компьютерные, информационно-коммуникационные) технологии/системы/программы, механизм и порядок их работы.

Таким образом, для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, необходима четкая стратегия и соответствующая нормативная правовая база, которые должны быть нацелены:

1) на криминализацию (изменение интенсивности пенализации) общественно опасных деяний (в том числе террористической направленности), совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Для этого необходима ревизия уголовного закона и иных нормативных правовых актов в сфере цифровых технологий в целях выявления пробелов правовой защиты объектов от террористических угроз и определения потребности усиления ответственности в конкретных случаях. Допускаем, что совершение преступлений в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий не во всех случаях может увеличивать степень общественной опасности запрещенных деяний. В этой связи на современном этапе считаем достаточным дополнить ст. 63 УК РФ частью 12 и изложить ее в следующей редакции «12. Судья (суд), назначающий наказание, в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признатьотягчающим обстоятельством совершение преступления с использованием цифровых и информационно-телекоммуникационных технологий»;

2) усиление сил и средств на воспитательно-просветительскую деятельность, в том числе в цифровом (кибер-) пространстве, направленную на пропаганду «мирного сосуществования всех народов независимо от расы, национальности, языка, происхождения в противовес негативному информационно-идеологическому воздействию на личность извне, в том числе пропаганды идеологии терроризма» ([Ищук и др., 2021](#));

3) обучение сотрудников правоохранительных органов, выявляющих, раскрывающих и расследующих преступления, в том числе террористической направленности, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий;

4) расширение полномочий сотрудников правоохранительных органов для обеспечения четкого и эффективного контроля цифрового контента;

5) выработку соглашений по международному сотрудничеству в области противодействия преступлениям, в том числе террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

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

** Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

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

Список литературы

- Антонова, Е. Ю. (2018). Терроризм как идеология насилия. *Вестник Дальневосточного юридического института МВД России*, 2(43), 69–74. <https://elibrary.ru/usgvtk>
- Антонова, Е. Ю. (2022). Технологии искусственного интеллекта – субъект преступления или орудие/средство совершения преступления? *Юридический вестник Кубанского государственного университета*, 1, 31–39. EDN: <https://elibrary.ru/liybvhv>. DOI: <https://doi.org/10.31429/20785836-14-1-31-39>
- Дремлюга, Р. И. (2022). Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. Москва: Юрлитинформ. <https://elibrary.ru/hsbxrm>
- Ищук, Я. Г., Пинкевич, Т. В., Смольянинов, Е. С. (2021). *Цифровая криминология: учебное пособие*. Москва: Академия управления МВД России. <https://elibrary.ru/vckoeef>
- Русскевич, Е. А., Дмитренко, А. П., Кадников, Н. Г. (2022). Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации. *Вестник Санкт-Петербургского университета. Право*, 13(3), 585–598. EDN: <https://elibrary.ru/xlyjys>. DOI: <https://doi.org/10.21638/spbu14.2022.301>
- Щетинина, Е. В. (2018). Проблемы развития культуры насилия в интернет-пространстве. *Инновационное развитие профессионального образования*, 18(2), 127–130. <https://elibrary.ru/xrzrml>
- Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGE Open*, 10(2), 215824402093449. <https://doi.org/10.1177/2158244020934494>
- Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*. Epub ahead of print 16 July.
- Grobbelaar, A. (2022). Media and Terrorism in Africa: Al-Shabaab's Evolution from Militant Group to Media Mogul. *Insight on Africa*, 15(1), 7–22. <https://doi.org/10.1177/09750878221114375>
- Huddy, L., Smirnov, O., Snider, K. L. G., & Perliger, A. (2021). Anger, Anxiety, and Selective Exposure to Terrorist Violence. *Journal of Conflict Resolution*, 65(10), 1764–1790. <https://doi.org/10.1177/00220027211014937>
- Keenan, P. K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, 37(1), 81–101. <https://doi.org/10.1177/2399654418776660>
- Khokhlov, N., & Korotayev, A. (2022). Internet, Political Regime and Terrorism: A Quantitative Analysis. *Cross-Cultural Research*, 56(4), 385–418. <https://doi.org/10.1177/10693971221085343>
- Liem, M., van Buuren, J., de Roy van Zuijdewijn, J., Schönberger, H., & Bakker, E. (2018). European Lone Actor Terrorists Versus “Common” Homicide Offenders: An Empirical Analysis. *Homicide Studies*, 22(1), 45–69. <https://doi.org/10.1177/1088767917736797>
- Makinda, S. (2016). Terrorism in International Society: An Eclectic Perspective. *Journal of Asian Security and International Affairs*, 3(1), 90–101. DOI: <https://doi.org/10.1177/2347797015626053>
- Orehek, E., & Vazeou-Nieuwenhuis, A. (2014). Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism. *Policy Insights From the Behavioral and Brain Sciences*, 1(1), 248–255. <https://doi.org/10.1177/2372732214549747>
- Polo, S. M. T. (2020). How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism. *Journal of Conflict Resolution*, 64(10), 1916–1942. <https://doi.org/10.1177/0022002720930811>
- Sandler, T. (2013). The analytical study of terrorism. *Journal of Peace Research*, 51(2), 257–271. <https://doi.org/10.1177/0022343313491277>
- Törnberg, P., & Törnberg, A. (2022). Inside a White Power echo chamber: Why fringe digital spaces are polarizing politics. *New Media & Society*, 146144482211229. <https://doi.org/10.1177/14614448221122915>
- Uusitalo, N., Valaskivi, K., & Sumiala, J. (2021). Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence. *Journalism*, 23(9), 1811–1827. <https://doi.org/10.1177/14648849211015601>
- Zedner, L. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. *Common Law World Review*, 50(1), 57–75. <https://doi.org/10.1177/1473779521989349>

Сведения об авторе



Антонова Елена Юрьевна – доктор юридических наук, профессор, декан юридического факультета, Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации

Адрес: 690091, Российская Федерация, г. Владивосток, ул. Суханова, 8

E-mail: antonovy@yandex.ru

ORCID ID: <https://orcid.org/0000-0001-6605-3699>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/rid/ABD-6781-2021>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57205298413>

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

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=261147

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 24 октября 2022 г.

Дата одобрения после рецензирования – 6 декабря 2022 г.

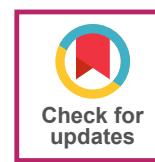
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.10>



Terrorist Crimes in the Era of Digitalization: Forms of Activity and Measures for Counteraction

Elena Yu. Antonova 

Far East Juridical Institute (branch) of the University of Public Prosecution of the Russian Federation
Vladivostok, Russian Federation

Keywords

Counteraction,
crime,
criminalization,
digital funding,
law,
propaganda,
recruitment,
space,
technologies,
terrorism

Abstract

Objective: to elaborate recommendations on counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

Methods: the methodological basis of the research are the universal dialectic method of cognition, the integrity of general and specific scientific methods such as analysis, synthesis, logical method, ascent from the abstract to the specific, induction, deduction, etc.

Results: it was determined that the development of the digital (cyber-) space and digital technologies promotes the intensity of terrorism and has led to the change of the mechanism of terrorist crimes commitment. A conclusion was made that, to provide the efficiency of measures for counteracting terrorist crimes committed in the digital (cyber-) space and/or using digital technologies, a distinct strategy is necessary, as well as the appropriate regulatory basis.

Scientific novelty: the article analyzes such forms of criminal activities of terrorist groups, committed in the digital (cyber-) space and/or using digital technologies, as dissemination of the ideology of violence and propaganda of terrorist activity, recruiting new members and their training, implementing digital technologies for preparation and immediate terrorist activity, and funding. The advantages were revealed of the use of digital space and/or digital technologies when committing terrorist crimes. In the author's opinion, the change of the mechanism of terrorist crimes commitment associated with the use of digital technologies should be taken into account during criminalization (change of the intensity of penalization) of publicly dangerous deeds. The important areas of state policy in the sphere of counteraction against these crimes are education and enlightenment activity, training of the personnel of law-enforcement agencies, broadening their authorities to ensure a clear and effective control over digital content.

© Antonova 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.

Practical significance: is due to the possibility to use the formulated conclusions and proposals for further scientific elaboration of the state criminal policy in the sphere of counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

For citation

Antonova, E. Yu. (2023). Terrorist Crimes in the Era of Digitalization: Forms of Activity and Measures for Counteraction. *Journal of Digital Technologies and Law*, 1(1), 251–269. <https://doi.org/10.21202/jdtl.2023.10>

References

- Antonova, E. Yu. (2018). Terrorism as the ideology of violence. *Vestnik Dalnevostochnogo yuridicheskogo instituta MVD Rossii*, 2(43), 69–74. (In Russ.).
- Antonova, E. Yu. (2022). Technologies of artificial intelligence – a subject or a tool/means of crime? *Yuridicheskii vestnik Kubanskogo gosudarstvennogo universiteta*, 1, 31–39. <https://doi.org/10.31429/20785836-14-1-31-39>
- Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGEOpen*, 10(2), 215824402093449. <https://doi.org/10.1177/2158244020934494>
- Dremlyuga, R. I. (2022). *Criminal-legal protection of digital economy and informational society against cyber-criminal infringements: doctrine, law, and law enforcement*. Moscow: Yurlitinform. (In Russ.).
- Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*. Epub ahead of print 16 July.
- Grobbelaar, A. (2022). Media and Terrorism in Africa: Al-Shabaab's Evolution from Militant Group to Media Mogul. *Insight on Africa*, 15(1), 7–22. <https://doi.org/10.1177/09750878221114375>
- Huddy, L., Smirnov, O., Snider, K. L. G. & Perliger, A. (2021). Anger, Anxiety, and Selective Exposure to Terrorist Violence. *Journal of Conflict Resolution*, 65(10), 1764–1790. <https://doi.org/10.1177/00220027211014937>
- Ishchuk, Ya. G., Pinkevich, T. V., & Smolyaninov, E. S. (2021). *Digital criminology: tutorial*. Moscow: Akademiya upravleniya MVD Rossii. (In Russ.).
- Keenan, P. K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, 37(1), 81–101. <https://doi.org/10.1177/2399654418776660>
- Khokhlov, N., & Korotayev, A. (2022). Internet, Political Regime and Terrorism: A Quantitative Analysis. *Cross-Cultural Research*, 56(4), 385–418. <https://doi.org/10.1177/10693971221085343>
- Kraidy, M. (2018). Terror, territoriality, temporality: Hypermedia events in the age of Islamic state. *Television and New Media*, 19(2), 170–176.
- Kydd, Andrew H., Walter, & Barbara F. (2006). The Strategies of Terrorism. *International Security*, 31(1), 49–80.
- Liem, M., van Buuren, J., de Roy van Zuijdewijn, J., Schönberger, H. & Bakker, E. (2018). European Lone Actor Terrorists Versus “Common” Homicide Offenders: An Empirical Analysis. *Homicide Studies*, 22(1), 45–69. <https://doi.org/10.1177/1088767917736797>
- Makinda, S. (2016). Terrorism in International Society: An Eclectic Perspective. *Journal of Asian Security and International Affairs*, 3(1), 90–101. <https://doi.org/10.1177/2347797015626053>
- Nossek, H. (2008). ‘News media’-media events: Terrorist acts as media events. *Communications*, 33(3), 313–330.
- Orehek, E., & Vazeou-Nieuwenhuis, A. (2014). Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism: Policy Implications of a Motivational Account of Terrorism. *Policy Insights From the Behavioral and Brain Sciences*, 1(1), 248–255. <https://doi.org/10.1177/2372732214549747>
- Polo, S. M. T. (2020). How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism. *Journal of Conflict Resolution*, 64(10), 1916–1942. <https://doi.org/10.1177/0022002720930811>
- Russkevich, E. A., Dmitrenko, A. P., & Kadnikov, N. G. (2022). Crisis and palingenesis (re-birth) of criminal law under digitalization. *Vestnik Sankt-Peterburgskogo universiteta. Pravo*, 13(3), 585–598. (In Russ.). <https://doi.org/10.21638/spbu14.2022.301>
- Sandler, T. (2013). The analytical study of terrorism. *Journal of Peace Research*, 51(2), 257–271. <https://doi.org/10.1177/0022343313491277>

- Schwartz, Carly. (2014, November 11). Majority of Americans Think Watching ISIS Beheadings Is Disrespectful to the Victims. *Huffpost*. https://www.huffingtonpost.com.au/entry/isis-beheading-videos_n_6194498
- Shchetinina, E. V. (2018). Problems of development of the culture of violence in the Internet space. *Innovatsionnoe razvitie professionalnogo obrazovaniya*, 18(2), 127–130. (In Russ.).
- Törnberg, P., & Törnberg, A. (2022). Inside a White Power echo chamber: Why fringe digital spaces are polarizing politics. *NewMedia & Society*, 146144482211229. <https://doi.org/10.1177/14614448221122915>
- Uusitalo, N., Valaskivi, K., & Sumiala, J. (2021). Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence. *Journalism*, 23(9), 1811–1827. <https://doi.org/10.1177/14648849211015601>
- Zedner, L. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. *Common Law World Review*, 50(1), 57–75. <https://doi.org/10.1177/1473779521989349>

Author information



Elena Yu. Antonova – Doctor of Law, Professor, Dean of Law Faculty, Far East Juridical Institute (branch) of the University of Public Prosecution of the Russian Federation

Address: 8 Sukhanov Str., 690091 Vladivostok, Russian Federation

E-mail: antonovy@yandex.ru

ORCID ID: <https://orcid.org/0000-0001-6605-3699>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/rid/ABD-6781-2021>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57205298413>

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

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=261147

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – October 24, 2022

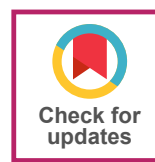
Date of approval – December 6, 2022

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023



Научная статья
УДК 343.1:168.3:004.91
EDN: <https://elibrary.ru/sgaoks>
DOI: <https://doi.org/10.21202/jdtl.2023.11>



Концепция электронного доказательства в уголовном судопроизводстве

Анна Александровна Дмитриева ✉

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Павел Сысоевич Пастухов

Пермский государственный национальный исследовательский университет
г. Пермь, Российская Федерация;
Пермский институт Федеральной службы исполнения наказаний
г. Пермь, Российская Федерация

Ключевые слова

Информация,
право,
процесс доказывания,
расследование,
суд,
уголовное дело,
уголовный процесс,
цифровые технологии,
электронное
взаимодействие,
электронные
доказательства

Аннотация

Цель: раскрытие потенциала цифровой трансформации для выработки оптимальных средств и методов собирания доказательств, внедрения научной организации труда должностных лиц, осуществляющих уголовное судопроизводство. Научный подход концепции состоит в минимизации затрат на собирание доказательственной информации по уголовным делам в электронной форме и электронным способом, а также сохранении материалов уголовного дела в электронной форме.

Методы: ведущее место среди методов исследования занимает диалектический метод, в соответствии с которым проблема электронного документа рассматривается во взаимосвязи и взаимозависимости с информационно-технологическим развитием общества. Совокупность методов научного познания в исследовании создает предпосылки для объективного и комплексного подхода к выделенным проблемам.

Результаты: авторская концепция электронного доказательства представляет собой систему информационно-технологических и правовых взглядов на уголовно-процессуальную форму, призванную оптимизировать процесс их собирания, фиксации и сохранения в материалах уголовного дела. Развитие концепции нацелено на выработку новых подходов к организации деятельности органов расследования и суда с учетом достижений в сфере информационных технологий, обеспечивающих новые способы собирания уголовно-релевантной,

✉ Контактное лицо

© Дмитриева А. А., Пастухов П. С., 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.

уголовно-процессуальной, криминалистически значимой информации при расследовании и рассмотрении уголовного дела. Представленная концепция направлена также на совершенствование взаимодействия и служебной коммуникации должностных лиц органов предварительного расследования с должностными лицами информационно-технологических систем для собирания доказательственной информации в электронной форме.

Научная новизна: системно проанализированы изменения, происходящие в современном информационном обществе через призму возникающих проблем между отраслевым уголовно-процессуальным доказательственным правом и более современными технологическими способами собирания доказательственной информации. В статье демонстрируется новый подход к созданию технологического взаимодействия с использованием цифровых технологий на научной основе организации доказательственной деятельности, призванной оптимизировать и рационализировать процесс доказывания в уголовном судопроизводстве.

Практическая значимость: материалы исследования могут быть использованы в работе по подготовке предложений о внесении изменений и дополнений в действующее законодательство с целью реализации практического опыта уже действующих моделей уголовно-процессуальной деятельности зарубежных стран, неисчерпаемого потенциала информационных технологий, программного обеспечения, искусственного интеллекта для рационализации доказывания по уголовным делам.

Для цитирования

Дмитриева, А. А., Пастухов, П. С. (2023). Концепция электронного доказательства в уголовном судопроизводстве. *Journal of Digital Technologies and Law*, 1(1), 270–295. <https://doi.org/10.21202/jdtl.2023.11>

Содержание

Введение

1. Методы и научные подходы к понятию электронных доказательств в российском праве

1.1. Понятие электронного доказательства в российском уголовно-процессуальном законодательстве

2. Результаты концептуального исследования о преимуществах внедрения понятия электронного доказательства

3. Исследование электронного доказательства в правовых системах зарубежных государств

3.1. Понятие электронного доказательства в законодательстве европейских государств

3.2. Понятие электронных доказательств в Китайской Народной Республике

3.3. Выработка международных стандартов к электронным доказательствам

Выводы

Список литературы

Введение

Процесс доказывания по уголовным делам является преимущественно мысленной сферой человеческой деятельности, имеет логическое содержание, а поэтому оперирует множественными теоретическими понятиями, но имеющими важное практическое значение. Важнейшее место в совершенствовании уголовно-процессуального доказывания занимает понятие доказательств, так как уголовный процесс представляет собой практическую деятельность по собиранию, проверке и оценке доказательств. Доказательство, как и всякое понятие, имеет содержание и объем, т. е. такую совокупность существенных признаков, отраженных в этом понятии, чтобы обеспечить правоприменителю максимально допустимую свободу в их собирании, проверке и оценке, но в то же время обладать свойствами относимости, допустимости и достоверности. Установление существенных признаков применительно к определению понятия уголовно-процессуального доказательства требует особой осторожности, так как в уголовном процессе на основании доказательств принимаются все решения, в том числе и об ограничении прав и свобод, виновности или невиновности. Поэтому нельзя допустить, чтобы такие важные решения принимались на основе ошибочной или ложной информации.

Осознавая важность существенных признаков для установления ограничительного содержания и объема понятия доказательства как базового элемента процесса доказывания, полагаем, что понятие доказательств должно быть закреплено в законе с учетом изменяющихся условий развития общества. Если цифровая трансформация изменила все базовые устои общества, то право должно соответствовать изменяющимся условиям. Если же право, консервативное по своей природе, не будет меняться в соответствии с трансформацией общества, то у правоприменителя будет возникать все больше проблем.

Произошедшая цифровая трансформация общества, рост киберпреступлений, а поэтому увеличение доказательственного значения цифровых следов преступлений, повсеместное использование де-факто электронных доказательств в практике деятельности правоохранительных органов наталкиваются на проблему отсутствия понятия «электронных доказательств» в уголовно-процессуальном законе. Поэтому ключевая проблема статьи заключается в обосновании необходимости включения понятия «электронное доказательство» в уголовно-процессуальный закон в целях оптимизации процесса доказывания и повышения его эффективности.

Эффективность мы понимаем как соотношение использованных ресурсов и полученных результатов. В информационном обществе гигантский объем электронной информации в современной инфраструктуре создает трудности при работе с информацией для любого человека, но в то же время открывает огромные возможности для органов расследования. В этой связи возникает закономерный вопрос, как добиваться максимального результата при минимуме затрат сил, средств и времени. В этом и заключается концептуальная идея эффективности в соотношении использованных ресурсов и полученных результатов. Авторы статьи нацелены продемонстрировать потенциал информационного общества, раскрыть содержание электронных доказательств в нормативной системе уголовно-процессуальных доказательств и сформулировать концепцию электронного доказательства, а следовательно, более эффективный процесс доказывания. Для достижения поставленной цели в статье

проанализированы тенденции развития электронных доказательств в отдельных системах зарубежных государств.

Исследование проведено в соответствии с диалектическим методом, позволившем авторам рассмотреть проблему электронного документа во взаимосвязи с информационно-технологическим развитием общества.

1. Методы и научные подходы к понятию электронных доказательств в российском праве

Продолжающаяся дискуссия среди ученых о понятии, сущности; особенностях собирания, сохранения; проверке электронных доказательств свидетельствует о неоднозначном подходе к названным аспектам. При обсуждении проблемы внедрения электронной доказательственной информации в качестве доказательств в уголовное судопроизводство мы утверждали, что она может быть представлена в классической системе уголовно-процессуальных доказательств. Практика показывает представление электронной доказательственной информации в ином документе, запрашиваемом у субъектов информационно-технологических систем, таких как обладатели информации, системные администраторы, сотрудники служб информационной безопасности, интернет-провайдеры, провайдеры связи, работники банковских и платежных систем, операторы систем видеонаблюдения. Зачастую электронная доказательственная информация представлялась в вещественном доказательстве, а точнее электронных носителях информации, например, смартфонах, планшетах, ноутбуках. После проведения экспертных исследований такая информация приводится в заключении эксперта (специалиста). Мы утверждали, что не следует менять уголовно-процессуальное законодательство с целью включения «электронного доказательства» как нового вида. Мы предлагали расширительное толкование действующего понятия доказательств (Пастухов, 2019). Существующие признаки понятия доказательств в виде «любых сведений», отраженных в ст. 74 Уголовно-процессуального кодекса Российской Федерации (далее – УПК), казалось бы, не делают исключений для какой-либо информации. На расширительное толкование понятия доказательств указывает ст. 84 УПК, предусматривающая закрепление доказательственной информации не только в письменном виде («иные документы»), но и на иных носителях информации, к числу которых можно отнести электронные носители информации.

Мы исходили из того, что относительная новизна электронной информации, несовершенство цифровой инфраструктуры побуждали ученых говорить о новом типе «электронных доказательств» в качестве отдельного самостоятельного уголовно-процессуального источника доказательств. При этом мы полагали, что с адаптацией общества к многочисленным гаджетам и информационным системам опасения относительно электронной информации исчезнут сами по себе. Данный тезис можно проследить на освоении каждым из нас смартфона, компьютеров и их приложений. В настоящее время смартфон в наших руках является банком в кармане, почтовым сервисом, телевизором, а в принципе, рабочим местом. Каждый из нас легко принимает информацию, создает, пересылает, т. е. выполняет все информационные функции. Подтверждением нашему тезису служат государственные и корпоративные тенденции по отказу от бумажных денег, банковских карт, документарных ценных бумаг, трудовых и сберегательных книжек, бумажных медицинских карт и т. д.

Анализируя различные взгляды, выделим сторонников и противников придания самостоятельного статуса электронным доказательствам. Так, В. Г. Голубцов, возражая против признания электронных доказательств, пишет о том, что электронно-цифровые технологии не обладают признаками и сущностными особенностями, влекущими необходимость изменять основные институты процессуального законодательства (Голубцов, 2019).

Отрицая самостоятельное значение электронного доказательства, Л. А. Головкин подчеркнул отсутствие новизны (Головкин, 2019), полагая, что уголовно-процессуальная категория доказательства гораздо шире и может включать в себя все электронные данные.

За включение электронных доказательств в сферу доказывания выступает М. И. Воронин (Воронин, 2019). По мнению этого автора, в уголовно-процессуальное законодательство следует ввести понятия «электронное доказательство», «электронный документ», «электронный носитель информации». При этом автор предлагает заимствовать понятие «электронный документ» из Федерального закона «Об информации, информационных технологиях и о защите информации»¹. Основной закон об информационных технологиях определяет электронный документ как документированную информацию, представленную в электронной форме (п. 11.1 ст. 2). От себя выделим ключевой признак электронного документа в законодательном определении – это способность человека его воспринимать с использованием электронных вычислительных машин. Этот признак является ключевым, так как при производстве по уголовным делам человекочитаемость имеет решающее значение при работе со сложной информационно-технологической средой. Помимо этого, следует отметить еще один признак – это возможность передачи электронного документа по информационно-телекоммуникационным сетям или обработки в информационных системах. Данное законодательное определение распространяется на любую электронную информацию, циркулирующую в цифровой среде. Поддерживая включение электронных доказательств, С. В. Зуев считает, что они должны отвечать четким требованиям допустимости, относимости и достоверности (Зуев, Сутягин, 2016).

Принимая во внимание всю полемичность понятия, сущности и перспектив использования электронных доказательств, мы выработали новый подход и сформулировали концепцию, нацеленную на информационно-технологический прорыв в модернизации уголовно-процессуального доказывания и всей уголовно-процессуальной деятельности. Предлагаемая концепция направлена на отрыв от устаревшей (архаичной) документарной (бумажной) технологии фиксации доказательств посредством включения в уголовно-процессуальное законодательство и сопутствующие акты нормативного толкования понятия «электронные доказательства». Данное нововведение разрешит давнюю проблему архаичной документарной формы удостоверения доказательственной информации и позволит применять более совершенные, научно обоснованные способы сохранения доказательственной информации электронным способом при производстве следственных и иных процессуальных действий или изначально запрашивать у обладателей информации, получать и сохранять доказательственную информацию в электронной форме. Сущностным

¹ Об информации, информационных технологиях и о защите информации. № 149-ФЗ (2006). *Собрание законодательства РФ*, 31 (1 ч.), ст. 3448.

элементом предлагаемой концепции является отрыв электронной информации от документарного (бумажного) протокола следователя и электронного носителя информации с перспективой формирования электронного документооборота.

Предлагаемое нами понятие электронных доказательств должно обеспечить преодоление архаичных методов при обращении с электронной доказательственной информацией, внедрить научные методы организации труда, а поэтому важно раскрыть не только их потенциал, но и все современные информационно-технологические конкурентные преимущества электронных способов и электронных форм доказательственной деятельности. Предлагая вышеуказанные нововведения, авторы полагают, что при электронной форме собирания доказательств должны обеспечиваться все необходимые свойства и предъявляемые требования в части их достоверности и допустимости. Ранее мы уже пришли к пониманию необходимости закрепления в уголовно-процессуальном законе понятия «электронных доказательств» в контексте выработки новых подходов к информационному обеспечению уголовно-процессуальной деятельности и предложили включить его в ст. 5 УПК в следующей редакции: «...электронное доказательство – это зафиксированная электронным способом или представленная в электронной форме юридически значимая информация в соответствии с уголовно-процессуальными требованиями, предъявляемыми к доказательствам, в целях установления истины по уголовному делу» (Пастухов, 2022а).

Понятие «данные» также имеет важнейшее значение, так как информационное общество представляет собой «общество данных», где информация кардинально изменяет все условия жизнедеятельности, а скорость обращения информации в цифровой инфраструктуре увеличилась в разы, поэтому возникает настоятельная необходимость предоставить правоприменителю возможности использования электронной информации, электронные данные без жесткой привязки к бумажному или электронному носителю информации. Из сказанного следует, что решение заявленной в статье проблемы мы видим в устранении чрезмерной формализации, упрощении уголовно-процессуальной формы, выработки новых требований допустимости доказательств за счет развития концепции электронных данных и электронных доказательств.

1.1. Понятие электронного доказательства в российском уголовно-процессуальном законодательстве

Как ранее уже отмечено нами, российское законодательное определение доказательств как «любых сведений, на основе которых должностные лица, осуществляющие производство, устанавливают обстоятельства, подлежащие доказыванию по уголовному делу», закреплено в ч. 1 ст. 74 УПК РФ². Такое широкое понимание доказательств, казалось бы, легко позволяет органам предварительного расследования и суду использовать доказательственную информацию в любой форме, в том числе электронной.

² Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. (2001). *Собрание законодательства РФ*, 52 (ч. I), ст. 4921.

Между тем, провозглашая свободу собирания доказательственной информации в виде «любых сведений», ч. 2 ст. 74 УПК ограничивает перечень уголовно-процессуальных источников доказательств как средств доказывания семью видами: показаниями подозреваемого, обвиняемого; показаниями потерпевшего, свидетеля; заключением и показанием эксперта; заключением и показаниями специалиста; вещественными доказательствами; протоколами следственных и судебных действий; иными документами. Как можно увидеть, среди перечисленных уголовно-процессуальных средств доказывания нет упоминания об электронных данных, что и представляет собой главную проблему, образующую противоречие между традиционной консервативной следственной моделью и более современными, а поэтому эффективными методами работы с доказательственной информацией. Это противоречие является главной проблемой настоящей статьи. Как уже сказано выше, российская модель уголовного судопроизводства является «следственной», означающей наличие самостоятельной стадии предварительного расследования, связанной с формированием доказательств в письменных материалах уголовного дела. Термин «предварительное» имеет два значения: во-первых, предшествует стадии судебного разбирательства, а во-вторых, выводы органов расследования являются предварительными. Окончательные выводы о виновности или невиновности делаются в суде на основании исследования представленных в материалах уголовного дела доказательствах.

Отмечая в целом важность стадии предварительного расследования, на которой устанавливаются все обстоятельства дела, а в суд направляются только уголовные дела, имеющие реальную судебную перспективу, считаем необходимым отметить недостатки следственной модели, связанные с дефиницией «доказательство». Одним из важных из значимых недостатков российской следственной модели является ее письменный характер, а точнее бумажная форма, что затрудняет эффективное использование электронной доказательственной информации. Следователь формирует все материалы уголовного дела, словно книгу, в протоколах которой подробно описаны получаемые сведения, вместо более современных, малозатратных способов фиксации и сохранения доказательственной информации в электронной форме. Все это происходит потому, что в российской доктрине основным способом фиксации доказательственной информации является описание в протоколе. Все иные способы фиксации считаются факультативными, что вынуждает следователя подробно описывать уже зафиксированное в человекочитаемой форме на различных носителях информации или даже переписывать увиденное, т. е. зафиксированную на видео информацию. Для следователя российский УПК является вроде «инструкции по применению», отклонение от которой влечет нарушение закона или даже недопустимость доказательств. Следственная модель не позволяет ему широко толковать нормы, касающиеся понятия, содержания и объема доказательств. В сложившейся правовой парадигме и уголовно-процессуальной практике любая доказательственная информация, в том числе электронная, должна быть зафиксирована в письменной форме в протоколе следственного действия, в одном из указанных источников (ч. 2 ст. 74 УПК).

Выделенную в статье проблему не решает уголовно-процессуальная норма, предусматривающая собирание доказательств в виде «иных документов» (ч. 2 ст. 84 УПК), в которой говорится, что сведения могут содержаться как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи

и иные носители информации. Проблема не решается названной нормой по причине требований к письменной процессуальной форме доказательства для обеспечения его допустимости. Кроме того, «иные документы» как вид доказательств создаются вне рамок уголовного процесса, а только приобщаются следователем к материалам уголовного дела. Подавляющее же большинство доказательств формируется следователем посредством составления бумажных протоколов в ходе производства следственных действий. Хотя большинство протоколов составляется с помощью компьютерных средств, они все равно должны распечатываться в бумажной форме и прилагаться к материалам уголовного дела.

Включение в 2012 г. в УПК РФ понятия «электронные носители информации», на которых содержится доказательственная цифровая информация (ч. 4 ст. 81, ч. 1 и 4 ст. 81.1, ст. 164.1 УПК РФ), тоже не решает заявленную проблему и не обеспечивает эффективность деятельности. Сложившиеся требования к процессуальной форме обязывают следователя составлять протокол и приобщать к протоколу скопированную на оптический диск доказательственную информацию. Такой подход означает ручной режим работы и дополнительные расходы. Несовершенство ручного режима работы становится более очевидным в информационном обществе, где цифровая инфраструктура автоматически регистрирует огромное количество юридически значимой информации, которая потенциально может быть криминалистически значимой и использоваться в качестве доказательств по уголовным делам. Собираение такой информации в процессе доказывания должно происходить в автоматизированном режиме, но для этого в уголовно-процессуальном законе должно применяться понятие «электронные доказательства». Отсутствие такого понятия побуждает должностных лиц, осуществляющих производство по делу, собирать доказательственную информацию устаревшим, архаичным способом, сохранять ее в бумажных протоколах. Ввиду сохранения такого порядка вышеобозначенное противоречие будет только усугубляться, так как объемы доказательственной информации в цифровой инфраструктуре только растут, а человеческие ресурсы по ее переписыванию ограничены.

Хотя понятие электронных доказательств можно увидеть в ст. 186.1 УПК, где упоминаются «данные о соединениях», но это частный случай упоминания в законе, который не решает всех проблем. Данные – это факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации³.

Далее будут раскрыты преимущества введения в уголовный процесс понятий электронных данных и электронных доказательств.

2. Результаты концептуального исследования о преимуществах внедрения понятия электронного доказательства

Заявленная концепция электронного доказательства состоит во включении в уголовно-процессуальный закон понятий «электронные данные» и «электронные доказательства» с целью преодоления бумажного способа оформления материалов уголовного дела. Реализация концепции направлена на оптимизацию работы

³ ГОСТ Р 50922-2006: Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. (2008). Москва: Стандартинформ.

с доказательствами в двух направлениях: во-первых, позволит собирать электронную доказательственную информацию из цифровой инфраструктуры электронным способом; во-вторых, проводить электронным способом следственные и иные процессуальные действия. В обеих ситуациях обеспечивается возможность фиксировать и сохранять полученную доказательственную информацию в электронной форме в материалах уголовного дела. Полагаем, что в результате реализации данной концепции будет обеспечена процессуальная и материальная экономия процесса доказывания по следующим направлениям.

1. Включение этих понятий позволит должностным лицам не только собирать и сохранять в электронной форме доказательственную информацию без привязки и переноса ее на электронном носителе информации, но и фиксировать традиционную аналоговую доказательственную информацию электронным способом, применяя компьютерные, аудио-, видеосредства фиксации. Как известно, собирание доказательств осуществляется двумя основными способами: 1) путем производства следственных действий и составления соответствующих протоколов; 2) путем приобщения доказательственной информации из современной инфраструктуры. В связи с тем, что в настоящее время в банковской, платежной, навигационной системах, сетях сотовой связи, коммуникационных сервисах и мгновенных мессенджерах, информационно-телекоммуникационной сети Интернет, системах видеонаблюдения, огромном количестве интернет-вещей, персональных устройствах пользователей накапливается гигантский объем криминалистически значимой информации, то приобщение электронной доказательственной информации из перечисленных электронных носителей становится приоритетным. Электронный способ изъятия и приобщения электронной доказательственной информации из вышеперечисленных устройств и систем кардинально сократит время по их получению.

2. Получение электронной доказательственной информации в целостном и неизменном виде, а не в виде частичного описания в протоколе следователя, позволит органам расследования получать оригинал, который намного информативнее описания в протоколе. В англосаксонской системе доказательственного права действует правило наилучшего доказательства, согласно которому в любой доказательственной информации первостепенное значение имеет первоисточник (первоначальная форма), содержащий данные о факте. Правило лучшего доказательства, направленного на представление оригинала записи в суд, закреплено в ст. 1002 Федеральных правил доказывания США⁴. Относительно электронных данных утверждается, что к ним применяются обычные требования: надежность способа создания и хранения сообщения данных; надежность способа, которым была проверена целостность сообщения данных; способ, которым был идентифицирован его создатель. Исследование оригинала электронной информации позволяет дополнительно выявить криминалистическое значение метаданных (metadata), позволяющих верифицировать происхождение документа, его автора, изменения электронного документа с момента создания до получения органами расследования⁵.

⁴ Federal Rules of Evidence. (2020). federal_rules_of_evidence_-_december_2020_0.pdf

⁵ Национальный стандарт Российской Федерации: Обеспечение долговременной сохранности электронных документов ГОСТ Р 54989-2012/ISO/TR 18492:2005. (2013). Москва: Стандартинформ.

3. Получение электронной информации в оригинале снимает противоречия между доказательственной информацией на электронных документах и электронных носителях информации. Данный тезис важен в связи с тем, что в научной литературе продолжается дискуссия в части признания электронной информации в качестве вещественного доказательства (ст. 81, 82 УПК) или иного документа (ст. 84 УПК). Проблема использования электронного документа не решена даже после придания легального статуса электронному документу в судах общей юрисдикции в 2016 г. Федеральным законом от 23 июня 2016 г. № 220-ФЗ в Уголовно-процессуальный кодекс РФ была введена ст. 474.1, устанавливающая порядок использования в уголовном судопроизводстве электронных документов. Сторонам предоставлено право обращаться в суд с ходатайствами, заявлениями, жалобами, представлениями в форме электронного документа, подписанного электронной подписью, посредством заполнения формы, размещенной на официальном сайте суда в сети Интернет. Приказом Судебного департамента возможность использования электронного документа была детализирована в судах общей юрисдикции⁶. Чуть позже, в 2017 г., легальность статуса электронного документа была подтверждена постановлением Пленума Верховного Суда РФ. Согласно вышеуказанным актам нормативного толкования, под электронным документом понимается документ, созданный в электронной форме без предварительного документирования на бумажном носителе, подписанный электронной подписью в порядке, установленном законодательством Российской Федерации⁷. Указанными документами введено понятие «электронный образ документа» (электронная копия документа, изготовленного на бумажном носителе), т. е. переведенная в электронную форму с помощью средств сканирования копия документа, изготовленного на бумажном носителе, заверенная в соответствии с Порядком подачи документов простой электронной подписью или усиленной квалифицированной электронной подписью. Несмотря на разъяснения в вышеуказанных актах нормативного толкования о необходимости использования электронных документов в производстве по уголовным делам, прорыва в цифровизации в уголовном судопроизводстве не произошло.

4. В условиях развития цифровых технологий к настоящему времени разработаны гарантии от модификации электронной доказательственной информации, ее целостности, неизменности, заключающиеся в ее копировании, дублировании, вычислении контрольной суммы; требование ее сохранности как по месту изъятия, так и в ведомственной информационной системе инфраструктуры правоохранительных органов. Одним из самых точных и надежных методов от модификации является вычисление контрольной суммы, т. е. значение хэш-функции (hash value), которая представляет собой битовую строку с выходным результатом хэш-функции⁸. Применение хэш-функций позволяет сжать электронные документы до фиксированного

⁶ Приказ Судебного департамента при Верховном Суде РФ № 251 от 27.12.2016. (2017). *Бюллетень актов по судебной системе*, 2.

⁷ Постановление Пленума Верховного Суда РФ № 57 от 26.12.2017 (2017, 29 декабря). *Российская газета*.

⁸ ГОСТ Р ИСО/МЭК 27037-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. (2014). Москва: Стандартинформ.

числа битов, т. е. вычислить уникальный «дактилоскопический отпечаток» соответствующих документов, который можно использовать для идентификации и неизменности информации⁹. При проверке доказательств сравниваются контрольные числа оригинала и копии электронной доказательственной информации, которые должны совпадать при верификации. Для создания и обеспечения надежного способа получения доказательств в вышеупомянутом стандарте предлагается сохранять электронные данные посредством применения метода, основанного на 128-битном алгоритме хеширования MD5, по своему назначению заменяющему цифровую подпись по отпечатку пальца. Криминалистическое значение алгоритма хеширования заключается в получении фиксированной длины цифровой информации файла вместо произвольной, что является идентифицирующим свойством полученного электронного документа. Дополнительной гарантией использования хэш-функций является сохранение сгенерированного отпечатка в нескольких экземплярах (двух-трех), причем на разных электронных носителях информации и разных устройствах. Например, один экземпляр должен оставаться у обладателя изъятой информации по аналогии с копией протокола обыска, а второй может сохраняться на сервере правоохранительного органа или на цифровой платформе. Названные технические процедуры полностью решают проблемы с идентификацией, изъятой электронной доказательственной информацией.

5. Признание электронного способа фиксации доказательственной информации открывает возможности и перспективы доказывания удаленным способом. Особо остро эта проблема возникла в период пандемии коронавируса, карантина, изоляции. Необходимость осуществления правосудия сделала электронное онлайн-правосудие чуть ли не основным направлением развития российской правовой системы. Элементы дистанционного производства по уголовным делам уже реализуются посредством использования систем видео-конференц-связи. Более того, даже наблюдается процесс расширения технологии видео-конференц-связи на проведение процессуальных действий на стадию предварительного расследования. Вначале видео-конференц-связь применялась только в апелляционном (ч. 2 ст. 389 УПК РФ) и кассационном (ч. 2 ст. 401 УПК РФ) суде, да и то только для участия лиц, содержащихся под стражей. В судах первой инстанции видео-конференц-связь применялась при рассмотрении жалоб в порядке ст. 125 УПК РФ, вопросов, связанных с исполнением приговора (ч. 2 ст. 399 УПК РФ). Наиболее перспективными были положения УПК в части применения видео-конференц-связи, позволявшие допрашивать в суде первой инстанции свидетелей и потерпевших, находящихся в других населенных пунктах (ч. 4 ст. 240 УПК РФ). Самым перспективным решением российского законодателя видится расширение электронного способа при проведении допроса, очной ставки и опознания в ходе предварительного расследования (ст. 189 УПК РФ) с января 2022 г.

6. Придание электронному доказательству легального статуса позволит интегрировать информационные возможности управленческой, административной, информационно-технологической, оперативно-разыскной, технико-криминалистической и уголовно-процессуальной доказательственной деятельности. Интеграция отраслей права и видов правоприменительной деятельности обеспечит кумулятивный

⁹ Национальный стандарт Российской Федерации: Обеспечение долговременной сохранности электронных документов ГОСТ Р 54989-2012/ISO/TR 18492:2005. (2013). Москва: Стандартинформ.

эффект уголовно-процессуального доказывания. Объединение информационных возможностей видится во внедрении цифровых платформ как наиболее приемлемых комплексных аппаратно-программных решений для обеспечения как межведомственного электронного взаимодействия, так и органов уголовного преследования, всех участников уголовного процесса, стороны защиты и суда. С использованием цифровых платформ формируются новая форма и содержание информационного взаимодействия в автоматизированном режиме, минимизируя медлительность человеческого фактора. Цифровая технология коммуникаций должностных органов предварительного расследования с должностными лицами информационных систем увеличивает скорость обмена информацией, обратную связь между органами и должностными лицами (Зайцев, Пастухов, 2019). Изучение практики деятельности правоохранительных органов показывает тенденции к созданию цифровых платформ: в Министерстве внутренних дел, прокуратуре, адвокатуре, а тем более в корпоративных организациях. Использование цифровых платформ должно трансформировать бумажное делопроизводство в электронный документооборот.

7. Включение понятия «электронное доказательство» открывает перспективы использования искусственного интеллекта, больших данных, видеоаналитики и видеосемантики (Zaytsev et al., 2021; Пастухов, 2022b; Reedy, 2023; Horsman, 2023; Wu & Zheng, 2020; Chen et al., 2020) как наиболее рациональных методов автоматизации при собирании доказательств. Искусственный интеллект вкупе с цифровыми платформами открывает новую эпоху автоматизации и роботизации в доказательственной деятельности по собиранию информации из сетей сотовой связи, навигационных систем, информационных систем и баз данных. Автоматизация исследования всевозможных банков данных намного повысит информационно-аналитические возможности криминалистической регистрации, учетов органов внутренних дел, иных правоохранительных органов, что позволяет обрабатывать большие объемы данных через совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных источников информации, в объемах, которые невозможно обработать вручную за разумное время (Horsman, 2021).

8. Благодаря электронным доказательствам доказывание в перспективе станет процессом идентификации личности (de Hert et al., 2018), информационно-технологических устройств, действий людей, событий, результатов. Для идентификации будут использоваться цифровые способы, основанные на цифровых идентификаторах, цифровом профиле лица (Hoile et al., 2011), цифровых платформах, системе межведомственного электронного взаимодействия, учетов криминалистической регистрации и иных видах автоматической регистрации.

9. Использование Единой системы идентификации и аутентификации, доказавшей свою эффективность за последнее десятилетие, в целях внедрения цифровых платформ для межведомственного взаимодействия правоохранительных органов и судов для идентификации пользователей¹⁰. К настоящему времени разработана более эффективная система – единая биометрическая система, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных,

¹⁰ Постановление Правительства РФ № 584 от 10.07.2013. (2013). *Собрание законодательства РФ*, 30 (Ч. II), ст. 4108.

их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в целях идентификации и аутентификации физического лица¹¹. Единая биометрическая система с использованием информационных технологий наиболее быстро позволяет идентифицировать человека по уникальным физическим признакам, таким как ДНК, лицо, отпечатки пальцев, голос, по подписи, удостоверяющим личность документам (Зайцев, Пастухов, 2022).

10. Использование электронных доказательств открывает перспективы для формирования информационно-технологического режима доказывания, новых стратегий раскрытия и расследования преступлений (Wu & Zheng, 2020). Формирование нового уклада свидетельствует о переходе «от документов к данным», который переводит бумажный документооборот в цифровую форму. В новом цифровом укладе общества перспективной технологией в документообороте является технология блокчейн, которая основывается на принципе контекстовой зависимости. При использовании такой технологии обеспечиваются подлинность, достоверность, неизменность и безопасность электронных документов.

11. На этапе судебного разбирательства в ходе судебного следствия обеспечение проверки электронных доказательств посредством визуализации доказательственной информации с использованием компьютерных, аудио-, видеосредств всеми участниками судебного разбирательства, а не только государственным обвинителем, держащим в руках бумажные материалы уголовного дела. Визуализация оригиналов значительно упрощает демонстрацию технических деталей электронных данных, таких как метаданные, хронология, геолокация, цифровые идентификаторы и другие числовые, временные, навигационные данные на электронных картах.

12. Внедрение электронного документооборота как необходимого условия для процессуальной и материальной экономии как итоговое значение легализации понятия электронного доказательства. Использование понятий электронных данных и электронных доказательств в правовых системах разных государств мира показывает, что бумажные (документарные) материалы уголовного дела стали за последние два десятилетия анахронизмом и атавизмом. Полагаем, что ключевое значение для внедрения электронного документооборота имеет именно использование понятий электронных данных и электронных доказательств в уголовно-процессуальном законодательстве.

Для реализации вышеназванных положений предложенной концепции необходимо проанализировать зарубежное уголовно-процессуальное законодательство.

3. Исследование электронного доказательства в правовых системах зарубежных государств

Недопустимо медленные изменения в российском законодательстве и кардинальные изменения в зарубежных правовых системах показали преимущества использования электронных доказательств в уголовно-процессуальных законодательствах для правоприменения, в частности для внедрения электронного документооборота.

¹¹ Банк России. Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов. (2022). <https://www.cbr.ru>

Анализ понятий электронного доказательства в англосаксонской правовой системе показывает, что цифровые доказательства определяются как информация и данные, которые представляют ценность для расследования и хранятся, принимаются или передаются с помощью электронного устройства¹². Причем доказательства, полученные из электронных устройств, таких как компьютеры и их периферийные устройства, компьютерных сетей, мобильных телефонов, цифровых камер, устройств хранения данных, а также из Интернета, используются в процессе доказывания на тех же правовых основаниях, что и традиционные формы доказательств (Rogers et al., 2023; Reedy, 2023; Horsman, 2023). Законодательное регулирование электронных доказательств в Великобритании регламентируется Законом о полиции и уголовных доказательствах 1984 г.¹³ На все цифровые доказательства распространяются те же правила и законы, которые применяются к документальным доказательствам¹⁴.

Полномочия полиции, закрепленные в ст. 19 Закона полиции, распространяются на истребование любой информации, в том числе в электронной форме. Главное условие заключается в том, чтобы электронная доказательственная информация имела отношение к совершению или предотвращению преступлений, а также когда ее изъятие способствует предотвращению сокрытия, потери, подделки или уничтожения доказательств в любой форме. Аналогичные подходы к цифровым доказательствам изложены в руководстве для полицейских Великобритании¹⁵.

В юридических словарях англосаксонской системы права цифровые доказательства (digital evidence) тоже определяются широко – как информация, имеющая доказательную ценность, хранящаяся или передаваемая в цифровой форме, т. е. любые данные, записанные или сохраненные на любом носителе в компьютерной системе или другом подобном устройстве, которые могут быть прочитаны или восприняты человеком или компьютерной системой¹⁶. В другом юридическом словаре цифровые доказательства или электронные доказательства понимаются как любая доказательная информация, хранящаяся или передаваемая в цифровом виде, а сторона судебного спора может использовать ее во время судебного разбирательства¹⁷.

В ст. 402 Федеральных правил о доказательствах США цифровые доказательства (digital evidence) и понимаются как данные (data) и носитель, на котором хранятся данные (media storing the data)¹⁸. Широкое толкование понятия

¹² National Institute of Justice. (2008, April). *Electronic CSI, a Guide For First Responders, Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition ([ojp.gov](https://www.ojp.gov)).

¹³ *Police and Criminal Evidence Act 1984*. (1984). <https://www.legislation.gov.uk/>

¹⁴ *Digitally Stored Evidence Standard Operating Procedure. Police Service of Scotland Standard Operating Procedure (SOP)*. (2018). <https://www.scotland.police.uk/spa-media/ercbdgot/indecent-images-children-digital-media-sop.pdf>

¹⁵ *ACPO Good Practice Guide for Digital Evidence*. (2012, March). https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

¹⁶ *Lawinsider*. (2021). <https://www.lawinsider.org/>

¹⁷ *US Legal Forms*. (2022). <https://uslegal.com/wp-signup.php?new=www.definitions>

¹⁸ *Federal Rules of Evidence*. (2020). [federal_rules_of_evidence_-_december_2020_0.pdf](https://www.uscourts.gov/federal-rules-of-evidence/_documents/federal-rules-of-evidence_-december-2020_0.pdf) ([uscourts.gov](https://www.uscourts.gov))

доказательств и использование в законодательстве понятия «данных» уже давно позволило в США применить электронный документооборот при производстве по уголовным делам. Для реализации этой технологии были разработаны руководства¹⁹, руководящие правила судов всех уровней и регламенты представления документов, технические требования к электронным документам при их копировании, сканировании, к формату, объему, в том числе по использованию электронных автоматизированных банков данных²⁰. Размещение материалов уголовного дела в информационно-технологической среде предоставляет участникам уголовного процесса доступ к материалам уголовного дела для ознакомления, уведомления, извещения. Ключевое значение в опубликованных руководствах и практической деятельности по использованию электронного документооборота (Case Management and Electronic Case Files (CM/ECF) system)²¹ имеет учетная запись или личный кабинет пользователя. Должностные лица, осуществляющие производство по делу, адвокаты и заявители должны создать учетную запись, в автоматическом режиме получить сгенерированный пароль²². За злоупотребление своей учетной записью предусмотрена строгая дисциплинарная и юридическая ответственность.

Введение системы электронного документооборота значительно упрощает судам ведение электронной регистрации и производство дел в электронном виде²³. Разработанные руководства устанавливают требования к качеству уголовно-процессуальных документов в электронной форме, распределенный доступ сторонам²⁴.

3.1. Понятие электронного доказательства в законодательстве европейских государств

В континентальной системе права на территории Евросоюза расширительное определение электронных доказательств как «любой информации, созданной, сохраненной или переданной в цифровом виде, позволяющей опровергнуть факт, оспариваемый в ходе судебного разбирательства»²⁵, свидетельствует о наиболее эффективном использовании их при производстве по уголовным делам. Наиболее интенсивная работа в эпоху цифровых технологий по внедрению электронных доказательств в странах Евросоюза началась с принятием в 2018 г. Европейским парламентом Регламента,

¹⁹ *Electronic case filing administrative policies and procedures manual*. (2020, October). <https://www.azd.uscourts.gov/sites/default/files/documents/adm%20manual.pdf>

²⁰ *Federal Rules of Evidence. R. 402. 2 Federal Rules of Evidence. R. 803*. (2020). https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_december_2020_0.pdf

²¹ *Electronic case filing administrative policies and procedures*. <https://www.ncmd.uscourts.gov/sites/ncmd/files/ecfprocman.pdf>

²² *Electronic case filing (ECF) Manuals and Training*. (2016). <http://www.kywd.uscourts.gov/ecf-manuals-and-training>

²³ *SEC Center for Complaints and Enforcement Tips*. (2021). <https://www.sec.gov/whistleblower/submit-a-tip>

²⁴ *Enforcement Manual*. (2017, November 28). <https://www.sec.gov/divisions/enforce/enforcementmanual.pdf>

²⁵ *Electronic evidence guide. A basic guide for police officers, prosecutors and judges. Version 2.1, Strasbourg*. (2020, March). https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

обеспечивающего механизмы сотрудничества²⁶. Расширительное определение электронных доказательств и принятие Регламента наделило правоохранительные и судебные органы современными инструментами по собиранию доказательств в электронной форме и таким образом ускорило процесс их защиты и получения у субъектов информационно-технологических систем, независимо от юрисдикции страны (Horsman, 2023; Hoile et al., 2011; Mason, 2014).

Признание электронных данных в качестве уголовно-процессуального доказательства в странах Евросоюза упрощает взаимодействие при расследовании уголовных дел в разных странах. В целях развития правовой помощи по уголовным делам и оперативного сохранения доказательственной информации Европарламентом принят Регламент, устанавливающий обязательные европейские ордера на сохранение электронных данных (European Preservation Order). По установленной процедуре выдается приказ, который утверждается судебным органом запрашивающей страны. За непредоставление запрашиваемой информации предусмотрена жесткая административная ответственность в виде штрафов. Наряду с ордерами о сохранении информации Европарламентом принят Европейский ордер о предоставлении (European Production Order). Исполнителями ордеров признаны обладатели цифровой доказательственной информации в информационно-телекоммуникационных сетях, такие как интернет-провайдеры, провайдеры связи, системные администраторы, так называемые поставщики услуг электронной связи.

3.2. Понятие электронных доказательств в Китайской Народной Республике

Созданный в Китайской Народной Республике (далее – КНР) информационно-технологический потенциал создает базис для собирания электронной доказательственной информации, обеспечивая новый информационно-технологический режим доказывания. Цифровое развитие в Китае в корне изменяет информационно-аналитическое и информационно-технологическое обеспечение расследования преступлений. Произошедшие в КНР изменения позволили перейти от документов к данным с одновременным упрощением процессуальной формы уголовного судопроизводства. Новые подходы позволили, по существу, ликвидировать документарный (письменный) характер производства по делу и перейти на электронный формат уголовного дела.

Эпоха электронных доказательств началась с принятием поправок УПК КНР в 2012 г. К существующим устным доказательствам: заявлениям потерпевших, показаниям свидетелей, показаниям и объяснениям подозреваемых и обвиняемых в совершении преступления; вещественным и письменным доказательствам; заключениям эксперта; протоколам осмотра и освидетельствования; видео- и аудиоматериалам – были добавлены электронные данные²⁷. Таким образом, УПК КНР

²⁶ *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.* (2018). <https://www.eclan.eu/en/eu-legislatory/proposal-for-a-regulation-of-the-european-parliament-and-of-the-council-on-european-production-and-preservation-orders-for-electronic-evidence-in-criminal-matters-e-evidence>

²⁷ *Уголовно-процессуальный кодекс КНР.* (2012). <https://asia-business.ru/law/law1/criminal/procedurallaw/>

с 2012 г. «электронные данные» признаются доказательствами, хотя уголовно-процессуальный закон не раскрывал это понятие (Юншен, 2014).

В развитие уголовно-процессуального закона в КНР разработано совместное Положение «О решении некоторых вопросов, касающихся собирания, получения и анализа электронных данных по уголовным делам», в котором закреплено понятие электронных данных. В ст. 1 названного положения «электронные данные» определяются как информация, собранная в рамках уголовного дела, сохраненная и передаваемая в электронной форме, которая может служить доказательством по уголовному делу»²⁸.

В ст. 2 положения дана классификация электронных данных, признаваемых доказательствами по уголовному делу, среди которых: веб-сайты, блоги (онлайн-дневники), микроблоги, страницы в социальных сетях, идентификаторы приложения (например, WeChat), форумы, онлайн-диски (онлайновые хранилища). Самое многочисленное значение имеют коммуникации в сети Интернет и сетях связи, например, мобильных сообщениях, электронных письмах, сообщениях из мессенджеров, сообщениях в группах. Особо важное значение имеет идентификационная информация, полученная при регистрации пользователя на сайте, электронных транзакциях, журналах регистрации.

С включением электронных доказательств в уголовно-процессуальное законодательство некоторые ученые оптимистично отмечали, что в эру электронных доказательств произойдет исторический скачок в теории доказательств (Guo, 2023; Wu & Zheng, 2020; Chen et al., 2020).

В целях обеспечения гарантий целостности и неизменности при собирании электронных доказательств в ст. 7 Положения предписывается производить их извлечение одновременно двумя следователями. В Положении указывается на строгое соблюдение всех перечисленных технических стандартов и юридических требований под угрозой их недопустимости, указанных в уголовно-процессуальном законодательстве.

Так, при изъятии исходный носитель данных опечатывается и производится стенограмма состояния хранения первоначального носителя. Опечатка оригинального носителя электронных данных и его фотосъемка должны защитить информацию от редактирования. В случае невозможности изъятия исходного носителя и находящегося в нем электронных данных производится стенограмма с указанием причин невозможности изъятия, источника электронных данных и места его хранения. Электронные данные, находящиеся вне территории КНР, могут быть извлечены через Интернет. По окончании расследования уголовного дела оригинальный носитель или собранные электронные данные должны быть переданы вместе с делом в опечатанном виде. Кроме того, в народную прокуратуру и суд передаются резервные копии (Юань, 2017).

При проверке электронных данных в прокуратуре и суде подлежат анализу, изучению законность их получения, подлинность и действительность (актуальность).

²⁸ Положение Верховного народного суда КНР, Верховной народной прокуратуры КНР и Министерства общественной безопасности КНР. (2016). <https://splcgk.court.gov.cn/gzfwwww//spyw/spywDetail?id=84ba1d7cbc0540d59fe49341f8b1ef85>

Во всех юрисдикциях возникают проблемы с хранением электронных данных в органах расследования и передачи материалов дела в суд. Во всем мире разрабатываются цифровые платформы, создаются базы данных, используются межведомственные информационные сети. В этом плане в КНР создали интегрированную базу данных, основанную на технологии онлайн-хранилища (по типу iCloud) для фиксации, хранения и передачи материалов уголовных дел в электронной форме в суд. Основными функциями облачного хранилища китайских правоприменителей являются не только хранение и архивирование, но и быстрый поиск нужных материалов в больших массивах электронных данных. Разработчики данной информационной платформы предусмотрели функции по надзору за всеми стадиями уголовно-процессуальной деятельности, от надзора за предварительным расследованием до стадий по пересмотру вышестоящими инстанциями.

Итак, анализ китайского уголовно-процессуального законодательства в части закрепления электронных данных в качестве доказательств в КНР свидетельствует о модернизации китайского уголовного процесса.

3.3. Выработка международных стандартов к электронным доказательствам

Во всех междугородных документах по киберпреступности отмечается, что цифровые данные являются основой большинства расследований преступлений и предпринимаются усилия по дополнительному правовому регулированию. В Европейской конвенции по киберпреступности компьютерные данные означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию (п. 6 ст. 1) ²⁹.

В Конвенции «данные о потоках» определяются как любые компьютерные данные, относящиеся к передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса (п. д ст. 1). Понятиями «данные» Конвенция оперирует при оперативном обеспечении и сохранности, обыске и выемке хранимых компьютерных данных. Самые перспективные положения были заложены в ст. 20 Конвенции, предусматривающей сбор в режиме реального времени данных о потоках информации. В частности, на государства возлагались обязанности по принятию законодательных и иных мер, необходимых для предоставления компетентным органам полномочий по собиранию или записыванию с применением технических средств в реальном режиме времени данных о потоках информации и в рамках правового сотрудничества передаче данных заинтересованной стороне.

Международная организация уголовной полиции, более известная как Интерпол, является организацией, содействующей полицейскому сотрудничеству между

²⁹ Конвенция о преступности в сфере компьютерной информации (ETS № 85). <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#OB9knUTgvfe6Gfbu1>

странами-членами. В правилах Интерпола по обмену информацией «данные» означают любую информацию, независимо от ее источника, относящуюся к составляющим элементам общеуголовных преступлений, расследованию и предотвращению таких преступлений, уголовному преследованию правонарушителей и наказанию за них³⁰. В принятом в Интерполе руководстве по обращению с электронными доказательствами при проведении обыска и выемки, их идентификации с помощью методов, гарантирующих их целостность, рекомендуется обращаться с ними, как и со всеми другими традиционными доказательствами. Необходимо учитывать, что некоторые электронные устройства требуют особых процедур сбора, упаковки и транспортировки либо потому, что они подвержены повреждению электромагнитными полями, либо потому, что их содержимое может измениться во время обращения и резервирования³¹.

Российский стандарт по информационным технологиям, методам обеспечения безопасности, выявлению и раскрытию электронной информации вводит новое понятие «электронное раскрытие» (electronic discovery), которое служит движущей силой как при проведении расследований, так и в ходе работы по сбору и обработке доказательств³². Электронное раскрытие (э-раскрытие) представляет собой процесс выявления и представления соответствующей сохраняемой в электронном виде информации (Electronically Stored Information, ESI) или данных одной или несколькими сторонами, участвующими в расследовании или судебном разбирательстве либо в аналогичных процедурах. Составными элементами э-раскрытия стандарт предусматривает сбор, обеспечение сохранности, представление, передачу сохраняемой в электронном виде информации. Это один из современных стандартов, основанный на более ранних стандартах, которые также рассматривали свидетельства, представленные в цифровой форме (digital evidence). В этом стандарте говорится, что информацию или данные, хранящиеся или передаваемые в виде двоичного кода, можно использовать в качестве доказательства³³.

Выводы

Завершая исследование, отметим, что авторская концепция электронного доказательства представляет собой систему информационно-технологических и правовых взглядов на уголовно-процессуальную форму, призванную оптимизировать процесс их собирания, фиксации и сохранения в материалах уголовного дела. Основная цель

³⁰ Interpol's Rules on the Processing of Data. (2021, March). https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

³¹ Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence. (2021). https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

³² ГОСТ Р ИСО/МЭК 27050-1-2019 Информационные технологии. Методы обеспечения безопасности. Выявление и раскрытие электронной информации. Часть 1. Обзор и концепции. (2019). Москва: Стандартинформ.

³³ ИСО/МЭК 27037:2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме» (ISO/IEC 27037:2014 «Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence»). (2014).

заявленной концепции состоит в модернизации уголовно-процессуального доказывания при раскрытии потенциала электронных доказательств по вышеназванным направлениям.

Реализация заявленной концепции позволит совершить прорыв в архаичной системе доказательственного права и уйти от письменной (бумажной) формы фиксации доказательств. Первым шагом для реализации названной концепции должно стать включение в УПК понятия «электронные доказательства», что повлечет за собой свободное оперирование органами расследования и судом электронной доказательственной информацией и использовать ее в качестве средств доказывания. Сущностным элементом предлагаемой концепции является отрыв электронной информации от документарного (бумажного) протокола следователя и электронного носителя информации с перспективой формирования электронного документооборота в межведомственной цифровой платформе.

Предложенное нами ранее понятие об электронных доказательствах в контексте выработки новых подходов к информационному обеспечению уголовно-процессуальной деятельности мы предлагаем рассматривать в рамках более широкой концепции и включить в ст. 5 УПК в следующей редакции: «...электронное доказательство – это зафиксированная электронным способом или представленная в электронной форме юридически значимая информация в соответствии с уголовно-процессуальными требованиями, предъявляемыми к доказательствам, в целях установления истины по уголовному делу» (Пастухов, 2022а).

Наряду с введением понятия «электронные доказательства», в ст. 84 УПК необходимо включить понятие «электронные данные», предназначенные для слома устаревшей системы документарных «иных документов».

В условиях информационного общества, развитой цифровой инфраструктуры включение этих понятий позволит создать информационно-технологический режим доказывания на научной основе организации труда. Говоря практическим языком, это позволит по-новому обеспечить информационное преимущество органов расследования и судов перед криминальной деятельностью в части собирания и фиксации электронной доказательственной информации. В части взаимодействия органов предварительного расследования с любыми субъектами информационно-технологических систем позволит кардинально сократить временные, процессуальные, материальные издержки посредством электронного документооборота. Включение этого понятия позволит должностным лицам не только собирать и сохранять в электронной форме доказательственную информацию без привязки и переноса ее на электронном носителе информации, но и фиксировать традиционную аналоговую доказательственную информацию электронным способом, применяя компьютерные, аудио-, видеосредства фиксации.

Список литературы

- Воронин, М. И. (2019). Электронные доказательства в УПК: быть или не быть? *Lex russica*, 7, 74–84. EDN: <https://elibrary.ru/jzbdut>. DOI: <https://doi.org/10.17803/1729-5920.2019.152.7.074-084>
- Головки, Л. В. (2019). Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? *Вестник экономической безопасности*, 1, 15–25. EDN: <https://elibrary.ru/korqgw>. DOI: <https://doi.org/10.24411/2414-3995-2019-10002>
- Голубцов, В. Г. (2019). Теория доказательств и цифровизация в гражданском судопроизводстве. *Пермский юридический альманах. Ежегодный научный журнал*, 1, 379–387. <https://elibrary.ru/zywect>

- Зайцев, О. А., Пастухов, П. С. (2019). Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации. *Вестник Пермского университета. Юридические науки*, 46, 752–777. <https://doi.org/10.17072/1995-4190-2019-46-752-775>
- Зайцев, О. А., Пастухов, П. С. (2022). Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений. *Вестник Пермского университета. Юридические науки*, 56, 281–308. <https://doi.org/10.17072/1995-4190-2022-56-281-309>
- Зуев, С. В., Сутягин, К. И. (2016). *Уголовный процесс: учебник*. Челябинск: Издательский центр ЮУрГУ.
- Пастухов, П. С. (2019). Электронные доказательства в нормативной системе уголовно-процессуальных доказательств. *Пермский юридический альманах*, 2, 695–707. <https://elibrary.ru/htypyz>
- Пастухов, П. С. (2022a). Новые подходы к информационному обеспечению уголовно-процессуальной деятельности. В сб. Т. В. Евтух, Л. Ю. Мхитарян и др. (ред. кол.), А. Н. Самойлов (отв. ред.), С. А. Котова (отв. за вып.), *Государственное и муниципальное управление в России: состояние, проблемы и перспективы: материалы Всерос. науч.-практ. конф., г. Пермь, 17 ноября 2022 г.* (с. 139–143). Пермь: Перм. филиал РАНХиГС.
- Пастухов, П. С. (2022b). Цифровая идентификация личности. В книге: Т. П. Подшивалов, Е. В. Титова, Е. А. Громова (ред.). *Право цифровой среды: монография* (с. 625–632). Москва: Проспект. <https://elibrary.ru/zomcik>
- Юань, И. (2017). Проблемы рассмотрения доказательств по новому УПК КНР. *Социально-политические науки*, 3, 137–138.
- Юншэн, Ч. (2014). Законодательные правила использования электронных данных результатов обыска и ареста. *Современное право*, 36(5), 111–113.
- Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Science International: Digital Investigation*, 35, 301001. <https://doi.org/10.1016/j.fsid.2020.301001>
- de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Amp; Security Review*, 34(2), 327–336. <https://doi.org/10.1016/j.clsr.2018.01.003>
- Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Amp; Security Review*, 48, 105774. <https://doi.org/10.1016/j.clsr.2022.105774>
- Hoile, R., Banos, C., Colella, M., & Roux, C. (2011). Bioterrorism: The effects of biological decontamination on the recovery of electronic evidence. *Forensic Science International*, 209(1–3), 143–148. <https://doi.org/10.1016/j.forsciint.2011.01.017>
- Horsman, G. (2021). Digital evidence and the crime scene. *Science & Amp; Justice*, 61(6), 761–770. <https://doi.org/10.1016/j.scijus.2021.10.003>
- Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Amp; Justice*, 63(1), 116–126. <https://doi.org/10.1016/j.scijus.2022.11.004>
- Lippman, M. R. (2019). *Criminal Procedure*. Sage.
- Mason, S. (2014). Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Amp; Security Review*, 30(1), 80–84. <https://doi.org/10.1016/j.clsr.2013.12.005>
- Reedy, P. (2023). Digital Evidence: Overview. *Encyclopedia of Forensic Sciences* (3rd ed., pp. 21–24). <https://doi.org/10.1016/b978-0-12-823677-2.00268-3>
- Rogers, M., Piper, M., & Bates, S. (2023). A Brief History of Digital Forensics and Digital Evidence. In *Encyclopedia of Forensic Sciences* (3rd ed., pp. 9–18). <https://doi.org/10.1016/b978-0-12-823677-2.00029-5>
- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Amp; Security Review*, 42, 105575. <https://doi.org/10.1016/j.clsr.2021.105575>
- Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Amp; Security Review*, 36, 105401. <https://doi.org/10.1016/j.clsr.2020.105401>
- Zaytsev, O. A., Pastukhov, P. S., Fadeeva, M. Y., & Perekrestov, V. N. (2021). Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. *Lecture Notes in Networks and Systems*, 155, 1266–1273. https://doi.org/10.1007/978-3-030-59126-7_138

Сведения об авторах



Дмитриева Анна Александровна – доктор юридических наук, доцент, заведующий кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет (национальный исследовательский университет)

Адрес: 454080, Российская Федерация, г. Челябинск, проспект Ленина, 76

E-mail: annadm@bk.ru

ORCID ID: <https://orcid.org/0000-0002-1035-1387>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/GWU-5850-2022>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57281194100>

Google Scholar ID: <https://scholar.google.com/citations?user=B0PW0wEAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=312402



Пастухов Павел Сысоевич – доктор юридических наук, доцент, профессор кафедры уголовного процесса и криминалистики, Пермский государственный национальный исследовательский университет; профессор кафедры публичного права, Пермский институт Федеральной службы исполнения наказаний

Адрес: 614990, Российская Федерация, г. Пермь, ул. Букирева, 15;

614012, Российская Федерация, г. Пермь, ул. Карпинского, 125

E-mail: pps64@mail.ru

ORCID ID: <https://orcid.org/0000-0003-0391-5540>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/B-5451-2017>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56926673600>

Google Scholar ID: https://scholar.google.com/citations?user=fu844_kAAAAJ

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=405105

Вклад авторов

Обоснование концепции исследования; проведение сравнительного анализа; обобщение результатов исследования; формулировка выводов; интерпретация результатов исследования осуществлялись А. А. Дмитриевой и П. С. Пастуховым в равных долях.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 5 января 2023 г.

Дата одобрения после рецензирования – 5 февраля 2023 г.

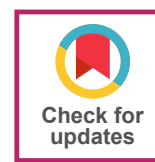
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.11>



Concept of Electronic Evidence in Criminal Legal Procedure

Anna A. Dmitrieva  

South Ural State University (National Research University)
Chelyabinsk, Russian Federation

Pavel S. Pastukhov 

Perm State National Research University
Perm, Russian Federation;
Perm Institute of the Federal Penitentiary Service
Perm, Russian Federation

Keywords

Court,
criminal case,
criminal procedure,
digital technologies,
electronic evidences,
electronic interaction,
Information,
investigation,
law,
proving process

Abstract

Objective: elucidating the potential of digital transformation for elaborating the optimal means and methods of collecting evidences and introducing scientific organization of labor of the officials implementing criminal procedure. The scientific approach within the concept consists in minimizing the costs of collecting evidentiary information in criminal cases in electronic form and by electronic means, as well as storing the criminal case materials in electronic form.

Methods: dialectic method occupies the leading position among the research methods, the issues of electronic documentation being considered in the interaction and interdependence with information-technological development of the society. The set of scientific cognition methods within the research creates prerequisites for objective and comprehensive approach to the problems under study.

Results: the authors' concept of electronic evidence is a system of information-technological and legal views on the criminal-procedural form, which is intended for optimizing the process of collecting, registering and preserving them in the criminal case materials. The concept development is aimed at elaborating new approaches to organizing the work of investigation agencies and courts, taking into account the achievements in the sphere of information technologies, providing new techniques of collecting criminal-relevant, criminal-procedural, criminological significant information when investigating and hearing of a criminal case. The proposed concept is also aimed at improving interaction and in-service communication of the officials of the preliminary

 Corresponding author

© Dmitrieva A. A., Pastukhov P. S., 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.

investigation bodies with the officials of information-technological systems for the purposes of collecting evidentiary information in electronic form.

Scientific novelty: the changes were systemically analyzed, which are taking place in the contemporary information society, through the prism of the emerging problems between the sectoral criminal-procedural evidentiary law and more modern technological means of collecting evidentiary information. The article demonstrates a new approach to creating technological interaction using digital technologies, on the scientific base of organization of proving activity, intended to optimize and rationalize the process of proving in criminal procedure.

Practical significance: the research materials can be used to prepare proposals on making changes and additions in the current legislation with a view of implementing the practice of already functioning models of criminal-procedural activity of foreign countries, an inexhaustible potential of information-technologies, software, and artificial intelligence to rationalize proving in criminal cases.

For citation

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, 1(1), 270–295. <https://doi.org/10.21202/jdtl.2023.11>

References

- Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. (2020). Study and implementation on the application of block-chain in electronic evidence generation. *Forensic Science International: Digital Investigation*, 35, 301001. <https://doi.org/10.1016/j.fsidi.2020.301001>
- de Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer Law & Amp; Security Review*, 34(2), 327–336. <https://doi.org/10.1016/j.clsr.2018.01.003>
- Golovko, L. V. (2019). The digitalization in criminal procedure: local optimization or global revolution? *Vestnik ekonomicheskoi bezopasnosti*, 1, 15–25. (In Russ.). <https://doi.org/10.24411/2414-3995-2019-10002>
- Golubtsov, V. G. (2019). Theory of evidence and digitization in civil proceedings. *Perm Legal Almanac*, 1, 379–387. (In Russ.).
- Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Amp; Security Review*, 48, 105774. <https://doi.org/10.1016/j.clsr.2022.105774>
- Hoile, R., Banos, C., Colella, M., & Roux, C. (2011). Bioterrorism: The effects of biological decontamination on the recovery of electronic evidence. *Forensic Science International*, 209(1–3), 143–148. <https://doi.org/10.1016/j.forsciint.2011.01.017>
- Horsman, G. (2021). Digital evidence and the crime scene. *Science & Amp; Justice*, 61(6), 761–770. <https://doi.org/10.1016/j.scijus.2021.10.003>
- Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Amp; Justice*, 63(1), 116–126. <https://doi.org/10.1016/j.scijus.2022.11.004>
- Lippman, M. R. (2019). *Criminal Procedure*. Sage.
- Mason, S. (2014). Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Amp; Security Review*, 30(1), 80–84. <https://doi.org/10.1016/j.clsr.2013.12.005>
- Pastukhov, P. S. (2019). Electronic evidence in the regulatory system of criminal procedural evidence. *Perm Legal Almanac*, 2, 695–707. (In Russ.).

- Pastukhov, P. S. (2022a). New approaches to information provision of criminal-procedural activity. In: T. V. Evtukh, L. Yu. Mkhitaryan et al. (Ed. board), A. N. Samoilov (xec. ed.), S. A. Kotova (in charge of the issue), *State and municipal governance in Russia: condition, problems and prospects: works of the All-Russia scientific-practical conference, Perm, November 17, 2022* (pp. 139–143). Perm: Perm. filial RANKhIGS. (In Russ.).
- Pastukhov, P. S. (2022b). Digital identification of a personality. In T. P. Podshivalov, E. V. Titova, E. A. Gromova (Eds.), *Digital environment law* (pp. 625–632). Moscow: Prospekt. (In Russ.).
- Reedy, P. (2023). Digital Evidence: Overview. *Encyclopedia of Forensic Sciences* (3rd ed., pp. 21–24). <https://doi.org/10.1016/b978-0-12-823677-2.00268-3>
- Rogers, M., Piper, M., & Bates, S. (2023). A Brief History of Digital Forensics and Digital Evidence. *Encyclopedia of Forensic Sciences* (3rd ed., pp. 9–18). <https://doi.org/10.1016/b978-0-12-823677-2.00029-5>
- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Amp; Security Review*, 42, 105575. <https://doi.org/10.1016/j.clsr.2021.105575>
- Voronin, M. I. (2019). Electronic Evidence in the Criminal Procedure Code: To Be or not to Be? *Lex Russica*, 7, 74–84. (In Russ.). <https://doi.org/10.17803/1729-5920.2019.152.7.074-084>
- Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Amp; Security Review*, 36, 105401. <https://doi.org/10.1016/j.clsr.2020.105401>
- Yuan, Yi. (2017). Study on judge's capacity on evidence review from the perspective of the revised criminal procedure law of China. *Sociopolitical Sciences*, 3, 137–138. (In Russ.).
- Yunsheln, Ch. (2014). Legislative rules of using electronic data on the results of search and arrest. *Sovremennoe Pravo*, 36(5), 111–113. (In Russ.).
- Zaytsev, O. A., & Pastukhov, P. S. (2019). Formation of a New Strategy for Crime Investigation in the Era of Digital Transformation. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, 46, 752–777. (In Russ.). <https://doi.org/10.17072/1995-4190-2019-46-752-775>
- Zaytsev, O. A., & Pastukhov, P. S. (2022). Digital personal profile as an element of the information and technological strategy of crime investigation. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, 56, 281–308. (In Russ.). <https://doi.org/10.17072/1995-4190-2022-56-281-309>
- Zaytsev, O. A., Pastukhov, P. S., Fadeeva, M. Y., & Perekrestov, V. N. (2021). Artificial Intelligence as a New IT Means of Solving and Investigating Crimes. *Lecture Notes in Networks and Systems*, 155, 1266–1273. https://doi.org/10.1007/978-3-030-59126-7_138
- Zuev, S. V., & Sutyagin, K. I. (2016). *Criminal procedure: tutorial*. Chelyabinsk: Izdatel'skii tsentr YUURGU. (In Russ.).

Authors information



Anna A. Dmitrieva – Doctor of Law, Associate Professor, Head of the Department of Criminal and Penal Law and Criminology, South Ural State University (National Research University)

Address: 76 prospekt Lenina, 454080 Chelyabinsk, Russian Federation

E-mail: annadm@bk.ru

ORCID ID: <https://orcid.org/0000-0002-1035-1387>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/GWU-5850-2022>

Scopus Author ID:

<https://www.scopus.com/authid/detail.uri?authorId=57281194100>

Google Scholar ID: <https://scholar.google.com/citations?user=B0PW0wEAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=312402



Pavel S. Pastukhov – Doctor of Law, Associate Professor, Professor of the Department of Criminal Procedure and Criminology, Perm State National Research University; Professor of the Department of Public Law, Perm Institute of the Federal Penitentiary Service

Address: 15 Bukirev Str., 614990 Perm, Russian Federation; 125 Karpinskiy Str., 614012 Perm, Russian Federation

E-mail: pps64@mail.ru

ORCID ID: <https://orcid.org/0000-0003-0391-5540>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/B-5451-2017>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56926673600>

Google Scholar ID: https://scholar.google.com/citations?user=fu844_kAAAAJ

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=405105

Authors' contributions

Substantiation of the research concept; comparative analysis; summarization of the research results; wording of conclusions; interpretation of the research results were carried out by A. A. Dmitrieva and P. S. Pastukhov in equal parts.

Conflict of interests

The authors declare no conflict of interests.

Funding

The research was not sponsored.

Article history

Date of receipt – January 5, 2023

Date of approval – February 5, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023

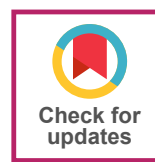


Научная статья

УДК 34:004

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

DOI: <https://doi.org/10.21202/jdtl.2023.12>



Илларию Лаврентьевну Бачило – основоположник информационного права в России

Эльвира Владимировна Талапина  

Институт государства и права Российской академии наук
г. Москва, Российская Федерация

Анна Константиновна Жарова 

Институт государства и права Российской академии наук
г. Москва, Российская Федерация

Ключевые слова

Илларию Лаврентьевна Бачило,
информационное право,
концепция развития
информационного
законодательства,
сектор информационного
права,
информационный кодекс

Аннотация

Цель: оценка научного вклада Илларию Лаврентьевны Бачило в формирование науки информационного права в России; роли и значения научных трудов И. Л. Бачило для отечественного информационного права.

Методы: в статье использовались методы ретроспективного научно-библиографического анализа, анализа и синтеза, сопоставления и взаимопроверки, библиографического изучения документов.

Результаты: проведен краткий анализ научной деятельности выдающегося ученого Илларию Лаврентьевны Бачило, описаны наиболее значимые работы, которые, по мнению авторов, явились базовыми в становлении и развитии науки информационного права.

Научная новизна: в статье представлены основные этапы и достижения научной жизни И. Л. Бачило, а также отражены персональные оценки и впечатления авторов, сформированные в процессе совместной работы с Илларию Лаврентьевной Бачило.

Практическая значимость: информация, представленная в статье, позволит ученым, в особенности молодым специалистам, начинающим исследователям, познакомиться с личностью и деятельностью великого ученого, глубокого и умного человека, память о котором останется навсегда в сердцах сотрудников созданного ею сектора информационного права Института государства и права Российской академии наук.

 Контактное лицо

© Талапина Э. В., Жарова А. К., 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.

Для цитирования

Талапина, Э. В., Жарова, А. К. (2023). Иллариya Лаврентьевна Бачило – основоположник информационного права в России. *Journal of Digital Technologies and Law*, 1(1), 296–307. <https://doi.org/10.21202/jdtl.2023.12>

Содержание

Введение
Результаты исследования
Выводы
Список литературы

Введение

Иллариya Лаврентьевна Бачило родилась в Ленинграде в 1926 г., образование получила в Минском юридическом институте. Свою кандидатскую диссертацию в 1955 г. она посвятила теме «Функции государственного управления в области культурно-просветительной работы и образования» (Теория государства и права). Несколько лет Иллариya Лаврентьевна работала в издательстве социально-экономической литературы в качестве ученого секретаря журнала «История СССР»¹, а с 1968 г. – в Институте государства и права Академии наук СССР, где в 1980 г. защитила докторскую диссертацию по административному праву на тему «Правовые проблемы организации структур и их функций в системе советского государственного управления»².

Результаты исследования

В разные годы сферу научных интересов И. Л. Бачило составляли проблемы теории административного права, методологии классификации функций государственного управления (Бачило, 1972), органов исполнительной власти, а также методики применения классификаторов функций в процессе формирования правового статуса органов государственной власти и совершенствования их структур, организации и правового регулирования процессов информатизации общества, включая информационные процессы в структурах государственного аппарата управления (Бачило, 1969). Наиболее весомый вклад ею внесен в решение правовых проблем формирования информационных ресурсов страны и их использования в процессах государственного управления, обеспечения прав граждан, исследование структур и функций исполнительной власти СССР, а затем и новой России. Но, пожалуй, главным делом научной жизни Иллариyi Лаврентьевны стало информационное право.

¹ Бачило Иллариya Лаврентьевна: информация о члене научного ред. совета интернет-проекта «Конституция России». <https://constitution.garant.ru/about/sovet/bachilo/>

² Бачило Иллариya Лаврентьевна. <https://igpran.ru/news/4464/>

Первые предложения по поводу формирования информационного права были сделаны теоретиком права А. Б. Венгеровым в середине 70-х гг. прошлого века. В то время в Академии наук СССР уже функционировала группа сотрудников, которая занималась правовыми проблемами АСУ (автоматизированных систем управления), возглавляемая И. Л. Бачило. К наиболее значимым ее работам того периода можно отнести: «Функции органов управления» (Бачило, 1976); «Организационно-правовые проблемы АСУ» (Бачило и др., 1979); «Организация советского государственного управления» (Бачило, 1984, 1980); «Ответственность в управлении» (Бачило, 1982, 1987); «Исполнительная власть в Российской Федерации. Проблемы развития» (Исполнительная власть в Российской Федерации. Проблемы развития, 1998).

По инициативе Илларию Лаврентьевны в 1998 г. был создан сектор информационного права Института государства и права Российской академии наук, который под ее руководством проработал до 2015 г. Она стала автором первого учебника по информационному праву, пережившего несколько переизданий. Илларию Лаврентьевна определила само понятие «информационное право» (Бачило, 1992, 2001a) как отрасли права (Бачило, 1999b), как области правоповедения (Бачило, 2012a, 2002) и как учебной дисциплины (Бачило, 2016a), внесла вклад в формирование понятийного аппарата информационного права (Бачило, 2013b, 2015). Значительные работы того периода – учебное пособие «Информационное право: Основы практической информатики» (Бачило, 2001a); учебник (в соавт.) «Информационное право» (Бачило и др., 2001); коллективная монография «Информационные ресурсы развития Российской Федерации: Правовые проблемы» (Информационные ресурсы развития Российской Федерации: Правовые проблемы, 2003). В сферу научных интересов Илларию Лаврентьевны входили проблемы классификации и гармонизации информационного законодательства (Бачило, 1999a, 1997; Бачило и др., 2019), обеспечения информационной безопасности на национальном и международном уровнях (Бачило и др., 1995), изучение правового режима информационных ресурсов (Бачило, 2013a), разработка институтов интеллектуальной собственности и исключительных прав в сфере информационной деятельности.

Обосновывая отрасль информационного права, она выделила его предмет (Бачило и др., 1995). Согласно ее определению, предметом, формирующим специальную отрасль отношений, условно называемых информационными, является совокупность реально существующих материализованных результатов творчества и труда, воплощенных: 1) в информации при разнообразии форм ее проявления и формируемых на этой основе информационных ресурсах; 2) средствах и технологиях работы с информацией; 3) средствах и технологиях передачи информации по сетям связи (Бачило, 2011).

Смена парадигмы в XXI в., развитие и распространение уже не просто компьютеров, но технологий, что отражалось в процессах «информатизации», получила естественный научный отклик. Так, в Институте государства и права РАН под руководством И. Л. Бачило была разработана Концепция развития информационного законодательства, учитывающая российскую специфику (Бачило и др., 2005). В концепции выделено шесть групп факторов сдерживания и развития процессов в информационной сфере.

1. Понимание и материализация феномена «свобода» в праве как приема, способа социального регулирования и обеспечения гарантий свободы в информационной сфере.

2. Легитимное введение в состав правоотношений предмета отношений субъектов в информационной сфере. Здесь возникает поле для дискуссий, в которых единственным предметом является «информация» (Гражданский кодекс РФ: документированная информация и формируемые на ее основе информационные ресурсы).

3. Факторы целеполагания в информационном законодательстве. Что ставится во главу угла при подготовке и принятии новых законов? Только ли интересы прибыли, вклад всего сектора экономики в бюджет или и иные цели, прежде всего социального, гуманитарного, управленческого характера?

4. Факторы управляемости информационными процессами и потенциал системизирующего влияния информации на сферу управления делами общества, государства, конкретных субъектов.

5. Неупорядоченность понятийного аппарата, двойное и тройное толкование однопорядковых терминов.

6. Влияние состояния социальной среды и государственно-властной системы на процесс правового регулирования отношений в информационной сфере.

Важно, что И. Л. Бачило обозначила формирование международного информационного права, нуждающегося в специальном исследовании (Бачило, 2011). Кроме того, в рамках гранта Российского фонда фундаментальных исследований «Человек в информационном обществе. Правовые проблемы» коллектив сектора информационного права подготовил три специальных выпуска журнала «Проблемы информатизации», посвященных правовым вопросам информационного общества, включая правовые аспекты регулирования отношений в Интернете и отношений, связанных с созданием и использованием информационных технологий (Бачило, 2016с) в экономике России³.

Наступление цифровых технологий не могло остаться без внимания, что отражено в соответствующей книге (Бачило, 2012а). Определяя информационное общество, она подчеркнула, что это общество, оснащенное таким уровнем информационных и коммуникационных технологий, которые становятся самостоятельным социально-технологическим ресурсом жизнедеятельности и развития социума и существенно влияют на парадигму смены его цивилизационной характеристики (Бачило, 2012а, 2013а).

Илларию Лаврентьевну выделяла роль информационного права как катализатора эволюции системы законодательства в целом (Бачило, 2012а). Стоит подчеркнуть, что Илларию Лаврентьевну, несмотря на высокую теоретическую подготовку, не была просто кабинетным ученым. Многие свои идеи она реализовывала в практических мероприятиях. Она являлась научным руководителем коллектива при подготовке проекта Федерального закона «Об информации, информатизации и защите информации», который был принят в 1995 г., разработала концепцию и проект Федерального закона «О праве на информацию». Под ее научным руководством сотрудниками сектора информационного права разработана концепция Информационного кодекса Российской Федерации (Бачило и др., 2014).

Можно по праву сказать, что И. Л. Бачило – инициатор формирования научной правовой дисциплины «Информационное право» и основатель школы этой

³ Бачило Илларию Лаврентьевна: информация о члене научного ред. совета интернет-проекта «Конституция России». <https://constitution.garant.ru/about/sovet/bachilo/>

отрасли права. Ею обоснованы направления гуманизации информационного общества, ориентации ИКТ-процессов на обеспечение и защиту прав граждан, разработанная концепция правового обеспечения информатизации и информационной безопасности; всесторонне проработана проблема мониторинга в праве.

Илларию Лаврентьевну долгое время возглавляла Диссертационный совет по присуждению степени кандидата юридических наук, доктора юридических наук по специальности 12.00.13 «Информационное право» при Института государства и права РАН. За время ее исследовательской деятельности под ее научным руководством защищено более 30 кандидатских и докторских диссертаций, выросли многие известные ученые.

И. Л. Бачило являлась членом редакционной коллегии журнала «Государство и право» и ряда профильных информационно-правовых изданий. Среди наград, полученных за большие заслуги в развитии юридических наук и подготовке юридических кадров, – почетное звание «Заслуженный юрист Российской Федерации», орден «Содружество», Почетная грамота Государственной Думы Федерального Собрания РФ.

Имя И. Л. Бачило как выдающегося ученого-юриста широко известно не только в России, но и за рубежом (Юсупов и др., 2017; Talapina & Bachilo, 2012; Bachilo, 2015). За время своей научной деятельности Илларию Лаврентьевну опубликовала более трехсот научных работ – статей, монографий (Медведев и др., 2013), учебников и учебных пособий (Бачило и др., 2019). Эти труды внесли значительный вклад в развитие отечественного права, многие работы можно считать достижениями советской и российской юриспруденции.

Отдельно стоит вспомнить про исключительные человеческие качества Илларию Лаврентьевну. Пройдя тяжелый жизненный путь, она не потеряла веру в людей, всегда с пониманием относилась к проблемам других и готова была помочь в любых жизненных ситуациях, неизменно оставалась интеллигентным, искренним, чутким и отзывчивым человеком. Она обладала такой жизненной энергией, которая спланивала вокруг себя совершенно разных и порой несовместимых друг с другом людей. Илларию Лаврентьевну полностью отдавала себя информационному праву, всегда находила время объяснить, научить, задуматься о новых перспективах. Ее энтузиазм, увлеченность своим делом заражали и других людей, привлекая их в науку информационного права.

Выводы

Роль научных трудов Илларию Лаврентьевну трудно переоценить, ценность их со временем будет только возрастать, и мы верим, что некоторые труды войдут в золотой фонд науки информационного права. Еще при жизни ее работы были высоко оценены в научной среде, послужили и служат основой для других научных исследований.

Способность Илларию Лаврентьевну увидеть будущее науки информационного права позволила ей показать последователям траекторию развития науки информационного права. Ее передовая научная мысль будет освещать дорогу многим ученым, вступившим на путь правового регулирования общественных отношений, возникающих в процессе обработки, накопления, поиска и хранения, передачи и распространения информации, а также создания и использования информационных технологий.

Хотелось бы, чтобы как можно больше людей, в особенности молодых специалистов, начинающих исследователей, знало об истоках и помнило имя одного из первых ученых, «почувствовавших», предсказавших и доказавших формирование новой отрасли – информационного права, которое так настойчиво и значимо проявляет себя в XXI в.

Список литературы

- Бачило, И. Л. (1969). Функции управления. Содержание и правовое управление. *Советское государство и право*, 12, 60.
- Бачило, И. Л. (1972). Факторы, влияющие на эффективность управления. *Советское государство и право*, 2, 74.
- Бачило, И. Л. (1976). *Функции органов управления (правовые проблемы оформления и реализации)*. Москва.
- Бачило, И. Л. (1980). Структуры в системе государственного управления. *Советское государство и право*, 5, 51.
- Бачило, И. Л. (1982). Компетенция и ответственность субъектов управления. *Советское государство и право*, 11, 22.
- Бачило, И. Л. (1984). *Организация советского государственного управления. Правовые проблемы*. Москва: Наука.
- Бачило, И. Л. (1987). Концепции совершенствования системы государственного управления. *Советское государство и право*, 6, 47.
- Бачило, И. Л. (1992). Методология решения правовых проблем в области информационной безопасности. *Информатика и вычислительная техника*, 2–3.
- Бачило, И. Л. (1997). Информация как предмет правоотношений. *Научно-техническая информация. Серия 1: Организация и методика информационной работы*, 9, 15–18. <https://elibrary.ru/wntvtp>
- Бачило, И. Л. (1999а). Глобальная информатизация и право. *Проблемы информатизации*, 3, 10–19. <https://elibrary.ru/wogtvr>
- Бачило, И. Л. (1999b). Информационные ресурсы как объект права и объект отношений, регулируемых ГК РФ. *Информационные ресурсы России*, 1.
- Бачило, И. Л. (2001а). Информационное право. Роль и место в системе права Российской Федерации. *Государство и право*, 2, 5–14. <https://elibrary.ru/umgrxk>
- Бачило, И. Л. (2001b). *Информационное право: Основы практической информатики: учеб. пособие*. Москва: Юринформсистема.
- Бачило, И. Л. (2002). Наиболее важные проблемы развития информационного права. *Государство и право*, 11, 8.
- Бачило, И. Л. (2011). *Информационное право: учебник*. Москва: Юрайт.
- Бачило, И. Л. (2012а). *Государство и право XXI в. Реальное и виртуальное*. Институт государства и права РАН. Москва: Юркомпани. <https://elibrary.ru/yltkzf>
- Бачило, И. Л. (2012b). Право как явление и феномен познания и практики (информационно-коммуникативный аспект). *Труды Института государства и права Российской академии наук*, 5, 175–190. <https://elibrary.ru/tjgggn>
- Бачило, И. Л. (2013а). Исчерпаны ли конституционные основы развития информационного общества и информационного права. *Государство и право*, 12, 95–108. <https://elibrary.ru/rrrbjn>
- Бачило, И. Л. (2013b). О методологии выявления связи феноменов «ПРАВО» и «ЗАКОН» и роли правосознания в этом процессе. Подход к проблеме через призму теории информационного права. *Вопросы правоведения*, 2(18), 46–60. <https://elibrary.ru/qbvmqn>
- Бачило, И. Л. (2015). О методологии выявления и классификации понятийного аппарата в информационном праве. В сб.: *Понятийный аппарат информационного права*, Москва, 19–20 февраля 2015 года (с. 8–17). Москва: Канон+. <https://elibrary.ru/ytdqpg>
- Бачило, И. Л. (2016а). *Информационное право: учебник (5-е изд., пер. и доп.)*. Москва: Юрайт. <https://elibrary.ru/vtxbbt>
- Бачило, И. Л. (2016b). Новый этап развития информационного общества и его институтов: правовой аспект. *Вопросы правоведения*, 2(36), 133–141. <https://elibrary.ru/xitblr>
- Бачило, И. Л. (2016с). Понятийный аппарат информационного права и система обеспечения инфор-

- мационной безопасности. *Труды Института государства и права Российской академии наук*, 3, 5–16. <https://elibrary.ru/wdjtkl>
- Бачило, И. Л., Антопольский, А. А., Белов, Г. В. и др. (2005). Концепция развития информационного законодательства в Российской Федерации. *Государство и право*, 7, 47–61. <https://elibrary.ru/gy-isjq>
- Бачило, И. Л., Бродский, И. Л., Венгеров, А. Б., Вишняков, В. Г. и др.; Бачило, И. Л., Тихомиров, Ю. А. (отв. ред.). (1979). *Организационно-правовые проблемы АСУ*. Москва: Наука.
- Бачило, И. Л., Букалерева, Л. А., Голоскоков, Л. В. и др. (2019). *Актуальные проблемы информационного права*. Москва: Компания КноРус. <https://elibrary.ru/zberch>
- Бачило, И. Л., Волокитин, А. В., Копылов, В. А. и др. (1995). О проблемах законодательства в сфере информации, информатизации и информационной безопасности. *Проблемы информатизации*, 1, 3–5. <https://elibrary.ru/mnsnsx>
- Бачило, И. Л., Лопатин, В. Н., Федотов, М. А.; Топорнин Б. Н. (ред.). (2001). *Информационное право: учебник*. Санкт-Петербург: Юрид. центр Пресс.
- Бачило, И. Л., Лазарев, Б. М. (отв. ред.) (1984). *Организация советского государственного управления. Правовые проблемы*. Москва: Наука.
- Бачило, И. Л., Андрющенко, Е. А., Демьянец, М. В. и др. (2014). Концепция Информационного кодекса Российской Федерации. Москва: Институт государства и права РАН – «Канон+» РООИ «Реабилитация». <https://elibrary.ru/cqqzag>
- Информационные ресурсы развития Российской Федерации: Правовые проблемы*. (2003). Москва: Наука.
- Исполнительная власть в Российской Федерации. Проблемы развития*. (1998). Москва: Юрист.
- Медведев, В. Н., Гришковец, А. А., Альхименко, В. В. и др. (2013). Двадцать лет Конституции Российской Федерации: юридическая наука и практика. Москва: Институт государства и права РАН. <https://elibrary.ru/xvokmt>
- Юсупов, Р. М., Бачило, И. Л., Бондуrowsкий, В. В. и др. (2017). Правовой вектор обеспечения информационной безопасности в модельном законодательстве СНГ. *Диалог: политика, право, экономика*, 2(5), 47–55. <https://elibrary.ru/yssbej>
- Bachilo, I. L. (2015). About the terms and definitions in information law. *Revista de Investigacoes Constitucionais*, 2(3), 207–222. EDN: <https://elibrary.ru/xxtfzr>. DOI: <https://doi.org/10.5380/rinc.v2i3.44535>
- Talapina, E. V., & Bachilo, I. L. (2012). Public governance in conditions of informatization. Russian experience. *Revue de l'Institut du monde et du développement*, 3, 111–120. <https://elibrary.ru/xtfqsl>

Сведения об авторах



Талапина Эльвира Владимировна – доктор юридических наук, главный науч-

ный сотрудник, Институт государства и права Российской академии наук

Адрес: 119019, Российская Федерация, г. Москва, ул. Знаменка, 10

E-mail: talapina@mail.ru

ORCID ID: <https://orcid.org/0000-0003-3395-3126>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/N-4960-2018>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=17347344300>

Google Scholar ID: <https://scholar.google.ru/citations?user=I1-RBQYAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=140000



Жарова Анна Константиновна – доктор юридических наук, доцент, старший

научный сотрудник, Институт государства и права Российской академии наук

Адрес: 420100, Российская Федерация, г. Москва, ул. Знаменка, 10

E-mail: anna_jarova@mail.ru

ORCID ID: <https://orcid.org/0000-0002-2981-3369>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/H-4012-2015>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56964137900>

Google Scholar ID: <https://scholar.google.com/citations?user=g8ij3BsAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=2240-1467

Вклад авторов

Авторы вложили равноценное участие и труд в написание данной статьи.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарности

Авторы благодарят Илларию Лаврентьевну Бачило за неоценимое участие во время совместной работы в секторе информационного права Института государства и права Российской академии наук.

История статьи

Дата поступления – 13 сентября 2022 г.

Дата одобрения после рецензирования – 2 октября 2022 г.

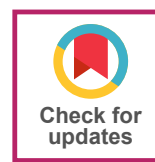
Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.12>



Illaria Lavrentyevna Bachilo – the Founder of Informational Law in Russia

Elvira V. Talapina  

Institute of State and Law of the Russian Academy of Sciences
Moscow, Russian Federation

Anna K. Zharova  

Institute of State and Law of the Russian Academy of Sciences
Moscow, Russian Federation

Keywords

Concept of the informational legislation development, Illaria Lavrentyevna Bachilo, Informational Code, informational law, Section of Informational Law

Abstract

Objective: to assess the scientific contribution of Illaria Lavrentyevna Bachilo into forming the science of informational law in Russia; the role and significance of I. L. Bachilo's scientific works for the Russian informational law.

Methods: the methods used in the work are: retrospective scientific and bibliographical analysis, analysis and synthesis, comparison and cross checking, bibliographical study of documents.

Results: a brief analysis of scientific activity of an outstanding researcher Illaria Lavrentyevna Bachilo was carried out; the most significant works were described, which, in the authors' opinion, appeared to be fundamental in the formation and development of the science of informational law.

Scientific novelty: the article presents the main stages and achievements of I. L. Bachilo's academic life and reflects the personal estimations and impressions of the authors, formed during mutual work with Illaria Lavrentyevna Bachilo.

Practical significance: the information presented in the article will allow scientists, especially young researchers, to get acquainted with the personality and activity of a prominent scientist, a deep and intelligent person, whose memory will always dwell with the hearts of the people working in the Section of Informational Law of the Institute of State and Law of the Russian Academy of Sciences.

 Corresponding author

© Talapina E. V., Zharova A. K., 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.

For citation

Talapina, E. V., & Zharova, A. K. (2023). Illaria Lavrentyevna Bachilo – the Founder of Informational Law in Russia. *Journal of Digital Technologies and Law*, 1(1), 296–307. <https://doi.org/10.21202/jdtl.2023.12>

References

- Bachilo, I. L. (1969). Functions of governance. Content and legal governance. *Soviet State and Law*, 12, 60. (In Russ.).
- Bachilo, I. L. (1972). Factors influencing the governance efficiency. *Sovetskoe Gosudarstvo i Pravo*, 2, 74. (In Russ.).
- Bachilo, I. L. (1976). *Functions of control bodies (legal issues of formatting and implementing)*. (In Russ.).
- Bachilo, I. L. (1980). Structures in the system of state governance. *Sovetskoe Gosudarstvo i Pravo*, 5, 51. (In Russ.).
- Bachilo, I. L. (1982). Competence and liability of the governance subjects. *Sovetskoe Gosudarstvo i Pravo*, 11, 22. (In Russ.).
- Bachilo, I. L. (1984). *Organization of Soviet state governance. Legal issues*. Moscow: Nauka. (In Russ.).
- Bachilo, I. L. (1987). Concepts of improving the system of state governance. *Sovetskoe Gosudarstvo i Pravo*, 6, 47. (In Russ.).
- Bachilo, I. L. (1992). Methodology of solving the legal problems in the sphere of informational security. *Informatika i Vychislitel'naya Tekhnika*, 2–3. (In Russ.).
- Bachilo, I. L. (1997). Information as an object of legal relations. *Scientific and Technical Information Processing. Ser. 1: Organization and methodology of informational work*, 9, 15–18. (In Russ.).
- Bachilo, I. L. (1999a). Global informatization and law. *Problemy Informatizatsii*, 3, 10–19. (In Russ.).
- Bachilo, I. L. (1999b). Informational resources as the object of law and the object of relations regulated by the Russian Civil Code. *Informatsionnye Resursy Rossii*, 1. (In Russ.).
- Bachilo, I. L. (2001a). Informational law. Role and position in the system of law of the Russian Federation, *State and Law*, 2, 5–14. (In Russ.).
- Bachilo, I. L. (2001b). *Informational law: basics of practical informatics: tutorial*. Moscow: Yurinformsistema. (In Russ.).
- Bachilo, I. L. (2002). The most important problems in the development of informational law. *State and Law*, 11, 8. (In Russ.).
- Bachilo, I. L. (2011). *Informational law: tutorial*. Moscow: Yurait. (In Russ.).
- Bachilo, I. L. (2012a). *State and law in the 21st century. The actual and the virtual*. Moscow: Yurkompani. (In Russ.).
- Bachilo, I. L. (2012b). The law as the event and the phenomenon of cognition and practice (information-communicative aspect). *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk*, 5, 175–190. (In Russ.).
- Bachilo, I. L. (2013a). Are the constitutional bases for developing informational society and informational law exhausted? *State and Law*, 12, 95–108. (In Russ.).
- Bachilo, I. L. (2013b). On the methodology of revealing the relations between the notions “jus” and “law” and the role of legal consciousness in this process. Approaching the problem through the prism of the informational law theory. *Voprosy Pravovedeniya*, 2(18), 46–60. (In Russ.).
- Bachilo, I. L. (2015a). About the terms and definitions in information law, *Revista de Investigacoes Constitucionais*, 2(3), 207–222. (In Russ.). <https://doi.org/10.5380/rinc.v2i3.44535>
- Bachilo, I. L. (2015b). On the methodology of identifying and classifying the conceptual framework in informational law. *Conceptual framework of informational law: a collection of scientific works*. Moscow, February, 2015. Moscow: Kanon+. (In Russ.).
- Bachilo, I. L. (2016a). *Informational law: tutorial*. Moscow: Yurait. (In Russ.).
- Bachilo, I. L. (2016b). The new stage of development of the information society and its institutions: legal aspect. *Voprosy Pravovedeniya*, 2(36), 133–141. (In Russ.).

- Bachilo, I. L. (2016c). Conceptual framework of informational law and the system of informational security provision. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk*, 3, 5–16. (In Russ.).
- Bachilo, I. L., Andryushchenko, E. A., Dem'yanets, M. V. et al. (2014). *Concept of the Informational Code of the Russian Federation*. Moscow: Institut gosudarstva i prava RAN – “Kanon+” ROOI “Reabilitatsiya”. (In Russ.).
- Bachilo, I. L., Antopol'skii, A. A., Belov, G. V. et al. (2005). Concept of informational legislation development in the Russian Federation. *State and Law*, 7, 47–61. (In Russ.).
- Bachilo, I. L., Brodskii, I. L., Vengerov, A. B., & Vishnyakov, V. G. (1979). *Organizational-legal issues of ACS*. Moscow. (In Russ.).
- Bachilo, I. L., Bukalero, L. A., Goloskokov, L. V. et al. (2019). *Topical issues of informational law*. Moscow: Kompaniya KnoRus. (In Russ.).
- Bachilo, I. L., Lopatin, V. N., & Fedotov, M. A. (2001). *Informational law: tutorial*. Saint Petersburg: Yurid. tsentr Press. (In Russ.).
- Bachilo, I. L., Volokitin, A. V., Kopylov, V. A. et al. (1995). On the issues of legislation in the sphere of information, informatization and informational security. *Problemy Informatizatsii*, 1, 3–5. (In Russ.).
- Executive power in the Russian Federation. Problems of development* (1998). Moscow, Yurist. (In Russ.).
- Informational resources of development of the Russian Federation: legal issues*. (2003). Moscow, Nauka. (In Russ.).
- Medvedev, V. N., Grishkovets, A. A., Al'khimenko, V. V. et al. (2013). *Twenty years of the Constitution of the Russian Federation: legal science and practice*. Moscow, Institut gosudarstva i prava RAN. (In Russ.).
- Talapina, E. V., & Bachilo, I. L. (2012). Public governance in conditions of informatization. Russian experience. *Revue de l'Institut du monde et du développement*, 3, 111–120. (In Russ.).
- Yusupov, R. M., Bachilo, I. L., Bondurovskii, V. V. et al. (2017). Legal vector of providing informational security in the model legislation of CIS. *Dialog: Politika, Pravo, Ekonomika*, 2(5), 47–55. (In Russ.).

Authors information



Elvira V. Talapina – Doctor of Law, Chief Researcher of Institute of State and Law of the Russian Academy of Sciences

Address: 10 Znamenkey Str, 119019, Moscow, Russian Federation

E-mail: talapina@mail.ru

ORCID ID: <https://orcid.org/0000-0003-3395-3126>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/N-4960-2018>

ScopusAuthorID:<https://www.scopus.com/authid/detail.uri?authorId=17347344300>

Google Scholar ID: <https://scholar.google.ru/citations?user=l1-RBQYAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=140000



Anna K. Zharova – Doctor of Law, Associate Professor, Senior Researcher of Institute of State and Law of the Russian Academy of Sciences

Address: 10 Znamenkey Str, 119019, Moscow, Russian Federation

E-mail: anna_jarova@mail.ru

ORCID ID: <https://orcid.org/0000-0002-2981-3369>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/H-4012-2015>

ScopusAuthorID:<https://www.scopus.com/authid/detail.uri?authorId=56964137900>

Google Scholar ID: <https://scholar.google.com/citations?user=g8ij3BsAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=2240-1467

Authors' contributions

The authors contributed equally into writing this article.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgments

The authors thank Illaria Lavrentyevna Bachilo for invaluable contribution during the collaborative work in the Section of Informational Law of the Institute of State and Law of the Russian Academy of Sciences.

Article history

Date of receipt – September 13, 2022

Date of approval – October 2, 2022

Date of acceptance – March 3, 2023

Date of online placement – March 10, 2023

