



ISSN 2949-2483

Volume

2

Number

3

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2024

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 – Валиуллина Светлана Зиярковна

Редактор – Тарасова Гульнара Абдулахатовна

Технический редактор – Каримова Светлана Альфредовна

Художник-дизайнер – Загреддинова Гульнара Ильгизаровна

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

Специалист по продвижению журнала в сети Интернет –

Гуляева Полина Сергеевна

Адрес: 420111, Российская Федерация,

г. Казань, ул. Московская, 42

Телефон: +7 (843) 231-92-90

Факс: +7 (843) 292-61-59

E-mail: lawjournal@ieml.ru

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

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

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

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

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

Учредитель и издатель

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



© Казанский инновационный университет имени В. Г. Тимирязова, оформление и составление, 2024.

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

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

Важно!

16+

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

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

Дата подписания к публикации – 25 сентября 2024 г. Дата онлайн-размещения на сайте <https://www.lawjournal.digital> – 30 сентября 2024 г.

Международные редакторы

Феррейра Даниэл Брантес – доктор наук, профессор Университета АМБРА (Орландо, Соединенные Штаты Америки), исполнительный директор Центра альтернативного разрешения споров (Рио-де-Жанейро, Федеративная Республика Бразилия)

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)

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

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

Члены редакционной коллегии

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Талимончик Валентина Петровна – доктор юридических наук, доцент, профессор кафедры общетеоретических правовых дисциплин Северо-Западного филиала Российского государственного университета правосудия (Санкт-Петербург, 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)

Томашевский Кирилл Леонидович – доктор юридических наук, профессор, заместитель декана юридического факультета по научной работе, профессор кафедры гражданского и предпринимательского права Казанского инновационного университета имени В. Г. Тимирязова (Казань, Российская Федерация)

Харитоновна 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)

Ван Розалили Ван Росли – доктор наук, преподаватель факультета права Брэдфордского университета (Брэдфорд, Соединенное королевство Великобритании, Шотландии и Северной Ирландии)

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

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

Гозстоный 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 Тяша** – доктор наук, доцент кафедры гражданского, международного частного и сравнительного права Мариборского университета (Марибор, Республика Словения)
- Иоаннис Револидис** – доктор наук, преподаватель кафедры медиаправа и права технологий Мальтийского университета (Мсида, Республика Мальта)
- Йованич Татьяна** – доктор наук, доцент факультета права Белградского университета (Белград, Республика Сербия)
- Карим Ридоан** – доктор наук, профессор кафедры предпринимательского и налогового права Университета Монаша (Санвэй, Федерация Малайзия)
- Кастро Дуглас** – доктор наук, профессор международного права школы права Ланьчжоуского университета (Ланьчжоу, Китайская Народная Республика)
- Кера Решеф Дениза** – доктор наук, профессор Центра исследований технологий распределенного реестра Мальтийского университета (Мсида, Республика Мальта)
- Кипурас Павлос** – доктор наук, профессор Школы судебной графологии (Неаполь, Итальянская Республика)
- Мараньяо Альбукерке де Соуза Джулиано** – доктор наук, доцент факультета права Университета Сан-Паулу (Сан-Паулу, Федеративная Республика Бразилия)
- Мелипатаки Габор** – доктор наук, профессор кафедры аграрного и трудового права Университета Мишкольца (Мишкольц, Венгрия)
- Мехрдад Райеджиан Асли** – доктор наук, профессор Института исследований и развития в области гуманитарных наук, доцент кафедры ЮНЕСКО по правам человека, мира и демократии, заместитель декана по науке Университета имени Алламеха Табатабаи (Тегеран, Иран)
- Морина Менсур** – доктор наук, доцент, заместитель декана факультета права Университета бизнеса и технологий (Приштина, Республика Сербия)
- Мохсин Камшад** – доктор наук, доцент юридического факультета Международного университета Махариши (Махариши, Республика Индия)
- Муратаев Серикбек Алпамысович** – кандидат юридических наук, заведующий кафедрой теории государства и права Ташкентского государственного юридического университета (Ташкент, Республика Узбекистан)
- Нуреддин Мухамад** – доктор наук, старший преподаватель кафедры публичного права Университета Байеро (Кано, Федеративная Республика Нигерия)
- Праюди Юди** – доктор наук, профессор кафедры компьютерных наук и электроники Университета Гаджа Мада (Булаксурмур, 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)
- 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

Бегишев И. Р., Жарова А. К., Залоило М. В., Филипова И. А., Шутова А. А. Цифровые и природоподобные технологии: особенности регулирования правом	493
Залоило М. В. Правовые проблемы обеспечения технологического суверенитета	500
Троицкая А. А., Шарловский К. А. Редактирование генома человека: управление технологическими рисками правовыми средствами	521
Тошбоева Р. С. Цифровые технологии в национальной кадастровой системе Узбекистана: проблемы правового регулирования	544
Северино Ф., Спозини Л. Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн	565
Казанцев Д. А., Догнал П., Догнал – младший П. Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования	585
Новиков Д. А. Использование искусственного интеллекта при найме работников: проблемы и перспективы правового регулирования	611
Спайропулос Ф. Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии	636
Бабаева В. А. Новостная криминология в XXI веке: формирование общественного мнения в новых реалиях	657
Камиджани М. К. Нарушение воздушного пространства страны беспилотными летательными аппаратами (дронами) с точки зрения международного права	674
Талимончик В. П. Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений	690
Корнехо Я. Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии	711



От редакции

УДК 34:004

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

DOI: <https://doi.org/10.21202/jdtl.2024.25>

Цифровые и природоподобные технологии: особенности регулирования правом

Ильдар Рустамович Бегишев

Казанский инновационный университет имени В. Г. Тимирязова, Казань, Россия

Анна Константиновна Жарова

Национальный исследовательский университет «Высшая школа экономики», Москва, Россия

Максим Викторович Залоило

Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, Москва, Россия

Ирина Анатольевна Филипова

Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского, Нижний Новгород, Россия

Альбина Александровна Шутова

Казанский инновационный университет имени В. Г. Тимирязова, Казань, Россия

О растущем влиянии на современное общество цифровых технологий в научной литературе написано немало. К наиболее значимым цифровым технологиям относят, прежде всего, искусственный интеллект, робототехнику, беспроводную связь, блокчейн, виртуальную и дополненную реальность, интернет вещей, цифровые двойники, иные новые производственные технологии. Среди них вызывает повышенный интерес группа технологий искусственного интеллекта – в силу того, что по распространению на практике опережает остальные группы технологий. Сервисы на основе искусственного интеллекта, особенно генеративного искусственного интеллекта, становятся обыденностью, преобразуя рабочие процессы, трансформируя хобби людей и их быт.

Но не только цифровые технологии (и цифровые сервисы на их основе) в чистом виде меняют реальный (физический) мир, растет влияние и природоподобных технологий, позволяющих воспроизводить системы и процессы живой природы в виде технических систем и технологических процессов. К ним можно отнести, к примеру, биотехнологии (в том числе генную инженерию), нейротехнологии (нейропротезирование, нейроинтерфейсы и т. д.). Строго говоря, перечисленные технологии находятся на стыке цифровых и природоподобных, так как их развитие стало возможным

именно в связи с процессами цифровизации производства, бизнеса, исследований и коммуникаций. Обнаруживающая себя сегодня тенденция по нейроморфизации искусственного интеллекта также сближает его с природоподобными технологиями. Как известно, одним из подходов к созданию искусственного интеллекта является восходящий (биологический), связанный с построением нейронных сетей, которые искусственным образом моделируют процессы, подобные происходящим в мозге человека.

Если несколько лет назад постановка вопроса о регулировании касалась обычно лишь использования названных выше технологий, в настоящее время мнение о необходимости создания системы правового регулирования все чаще относится не только к применению данных технологий, но и к возможным путям их развития: слишком привлекателен потенциал использования этих технологий, одновременно с их развитием и распространением на практике значительно возрастают разнообразные риски. В парламентах разных стран и на уровне международных организаций обсуждается включение в правовую систему норм, регулирующих использование, а нередко и направления эволюционирования этих технологий.

Некоторые вопросы уже нашли отражение в действующем законодательстве и судебной практике. К примеру, принятый в 2024 г. Регламент Европейского союза об искусственном интеллекте регулирует применение технологий и продуктов на основе технологий искусственного интеллекта, при этом отдельное внимание в пятой главе Регламента уделено базовым моделям или моделям искусственного интеллекта общего назначения (*general-purpose AI models*). В статьях Регламента предусмотрены дополнительные обязанности, возлагаемые на поставщиков таких моделей, а если они входят в список моделей с системным риском, количество юридических обязанностей возрастает. Другим примером правового регулирования в данной области может служить «Положение об администрировании информационных служб Интернета Deep Synthesis», опубликованное Управлением киберпространства Китая 25 ноября 2022 г. (его нередко именуют «Правилами регулирования дипфейков»). Документ содержит ряд требований к предоставлению услуг глубокого синтеза при создании изображений, видео-, аудиоматериала и текстов. Генерируемый контент должен соответствовать правилам контроля за информацией и помечаться как синтетически созданный, а поставщики обязаны принимать меры для предотвращения неправильного использования сервиса и маркировать контент, созданный искусственным интеллектом.

Примером из судебной практики может служить решение Верховного суда Чили от 9 августа 2023 г., касающееся права на неприкосновенность частной жизни путем защиты работы человеческого мозга. Вопросы, которые затронуты решением, могут быть отнесены к персональным данным, нейроданным и нейроправам личности. Решение Верховного суда было вынесено в результате рассмотрения иска о конституционной защите, поданного против компании Emotiv Inc. (г. Сан-Франциско, США), коммерциализировавшей беспроводную гарнитуру с датчиками, собирающими нейроданные, т. е. информацию об электрической активности мозга. В решении указывается, что неприкосновенность частной жизни является важным аспектом человеческой целостности, достоинства человека и его прав, таких как когнитивная свобода, свобода мысли и идентичности. Подобное решение стало

возможным благодаря целенаправленной деятельности чилийских парламентариев по включению нейрорправ в законодательство этого государства.

На страницах данного номера журнала представлены результаты исследований авторов из разных стран, посвященных тематике использования и регулирования цифровых и природоподобных технологий, проблемам, которые связаны с расширяющимся использованием этих технологий и продуктов на их основе, а также предлагаемым вариантам решения проблем.

В первой статье номера – «Правовые проблемы обеспечения технологического суверенитета» (**Максим Залоило (Россия)**) – предложена теоретико-правовая модель обеспечения технологического суверенитета, рассмотрены концепции технологоцентризма, цифровой (технологической) солидарности, стратегические основы научно-технологического развития, поднимаются вопросы общего характера, касающиеся обеспечения технологической безопасности и определения научно обоснованных векторов их решениям, как следствие, повышения значимости сохранения независимости государства в сфере науки и технологий. Без этого становится невозможным эффективное развитие экономики и устойчивое функционирование критически важных для обеспечения жизнедеятельности людей государственных институтов. Технологический императив, лежащий в основе формирования современной техногенной цивилизации, стал важным фактором для начавшейся трансформации права. В свою очередь праву как универсальному регулятору общественных отношений приходится реагировать, решая непростую задачу защиты технологической безопасности страны.

Следующая статья номера – «Редактирование генома человека: управление технологическими рисками правовыми средствами» (**Александра Троицкая, Константин Шарловский (Россия)**) – посвящена проблемам правового регулирования использования генной инженерии как одной из наиболее востребованных сегодня биотехнологий, которая позволяет изменять ДНК, обеспечивающую передачу генетической программы следующим поколениям живых организмов. В статье представлены результаты исследования различных подходов к регулированию генетического редактирования в репродуктивных целях, определены условия и особенности применения возможных регуляторных механизмов и дается оценка действующему законодательству в данной сфере.

Вопросы правового регулирования цифровых технологий волнуют авторов из европейских стран, рассматривающих возникающие коллизии и риски между технологией блокчейн и законодательством по защите данных (**Фабио Северино, Людовико Спозини (Италия)**). Затрагиваются наиболее актуальные проблемы в этой области, обусловленные недостатками традиционных моделей блокчейна и «правом на забвение», закрепленным в действующем европейском праве. Особый интерес вызывает представленный в исследовании анализ материалов, посвященных гибриднему решению возникающих вопросов, позволяющих гарантировать права на удаление и модификацию персональных данных и устранить выявленную несовместимость между технологиями и действующим регулированием.

Интересно и изучение формируемых подходов к регулированию технологий в странах, опыт которых не столь часто транслируется в научной литературе, что позволяет шире взглянуть на проблему, обнаружив новые грани для

последующих исследований. Например, в одной из статей номера обозначены трудности, проявляющиеся на пути к регулированию использования цифровых технологий в национальной кадастровой системе Узбекистана (**Робия Тошбоева (Узбекистан)**). Применение технологий искусственного интеллекта позволяет улучшить осуществление кадастрового учета при условии, что будут сформированы качественные правовые рамки, а это представляется затруднительным без четкой регламентации правового режима искусственного интеллекта в национальном законодательстве.

Растущее использование технологий искусственного интеллекта в частном секторе влечет за собой изменение как собственно бизнес-процессов, так и отношений между работодателями и работниками, тем самым затрагиваются вопросы как предпринимательского, так и трудового права. Анализ проблем правового регулирования использования искусственного интеллекта для проведения конкурентных закупок позволил авторам другой статьи (**Дмитрий Казанцев (Россия), Павел Догнал (Чехия), Павел Догнал-младший (Дания)**) выделить наиболее перспективные направления по созданию правового регулирования соответствующих отношений, при этом в качестве экспериментальной модели рассматривается реальный пример проведения сложной закупки высокотехнологичного оборудования с прогнозированием использования искусственного интеллекта в закупках на будущее. Неменьший интерес представляет и тема формирования правового регулирования в сфере применения искусственного интеллекта при найме работников (**Денис Новиков (Россия)**). Проблемы, возникающие из-за внедрения сервисов на основе искусственного интеллекта в процедуру найма, многообразны. К ним следует отнести необходимость защиты персональных данных соискателя, риски дискриминации и необоснованного отказа в приеме на работу вследствие предвзятости алгоритмов, распределение ответственности за решение, к которому привела работа системы искусственного интеллекта. Чтобы избежать дополнительных ошибок, стоит обратиться к передовому иностранному опыту, что позволит учесть имеющиеся наработки и будет содействовать конструированию оптимального национального регулирования.

Еще две статьи, включенные в данный номер журнала, касаются уголовно-правовой сферы и криминологических интересов. Первая из них (**Фотиос Спирупулос (Кипр–Греция)**) посвящена новым подходам в криминологии, позволяющим обозначить и определить предмет цифровой криминологии, исследующей потенциальное использование новых технологий в преступных целях. Мир все больше становится «гибридным»: реальность и виртуальная среда будут переплетаться чем дальше, тем сильнее. Это отразится и на преступности, что заставляет задуматься об адаптации к новым явлениям действующего уголовного законодательства. Во второй статье (**Валентина Бабаева (Россия)**) затронуты функции новостной криминологии с учетом «перетекания» основной части медиаресурса в интернет-пространство и неуклонно растущего влияния социальных сетей, блогов и видеохостингов как альтернативных средств массовой информации на общественное мнение. В статье говорится о меняющихся возможностях взаимодействия средств массовой информации и правоохранительных органов и о новых рисках, возникающих в связи с освещением материалов о правоохранительных органах и преступности в таких медиа.

В следующих двух статьях номера отражены вопросы международно-правового характера. Рассматриваются беспилотные технологии, развитие и применение которых приводит к нарушениям воздушного пространства других государств, отмечается, что тема беспилотных летательных аппаратов (дронов) как автономного оружия обычно включает обсуждение того, каким нормам международного права должно подчиняться их использование и насколько нынешнее международное право способно реагировать на происходящие в результате цифровизации изменения в принципе (**Милад Каши Комижани (Иран)**). Другая статья связана с цифровыми технологиями, используемыми в международном правосудии, а именно в деятельности судов интеграционных объединений (**Валентина Талимончик (Россия)**). Ее автором ставится задача проанализировать компетенцию и процедуры рассмотрения дел судами интеграционных объединений, позволяющие им разрешать споры, связанные с цифровыми технологиями, определив в итоге перспективы по рассмотрению данной категории споров. По итогам комплексного анализа различных источников, в том числе научного характера, международных договоров и актов судебной практики, предложено ввести в научный оборот определение содержания споров, связанных с цифровыми технологиями, в отношении судов интеграционных объединений.

Научный обзор, завершающий данный номер журнала, представляет отдельный интерес, так как касается темы нейроправ и расширяющегося проникновения нейротехнологий из исследовательских лабораторий в обычную жизнь людей (**Ян Ан Корнехо (Эквадор)**). Развитие нейротехнологий открыло огромные возможности для понимания и улучшения функционирования человеческого мозга, но одновременно привело к серьезным проблемам, связанным с защитой прав человека, неприкосновенности частной жизни и психической автономии. Медицинские изделия на основе нейротехнологий сегодня позволяют значительно улучшить жизнь людей, имеющих определенные заболевания, но параллельно собирают данные об активности мозга и могут быть использованы для «взлома» сознания. Последнее обуславливает вынесение на обсуждение вопроса о закреплении правовых основ, гарантирующих ответственное развитие и использование нейротехнологий, через включение в законодательство прав на психическую неприкосновенность, нейротехнологическую недискриминацию (право на равное обращение независимо от нейробиологических особенностей человека), доступ к своим нейроданным, личностную идентичность и свободу воли как возможность самостоятельно принимать решения без внешнего вмешательства.

Представленные достижения правовой доктрины в области исследования вопросов, связанных с развитием цифровых и природоподобных технологий, показывают, что практика их использования в реальной жизни порождает множество сложных этических, социальных, юридических вопросов, находящихся на стыке права, науки и технологий. Право меняется вслед за изменениями в области науки и технологий, становится более динамичным. Затрагиваемые в настоящем номере журнала темы побуждают к дискуссии о новых глобальных вызовах и рисках, требующих выработки стратегического консенсуса в вопросах понимания новейших правовых явлений и процессов, поиска адекватных и научно обоснованных ответов, открывающих новые горизонты и перспективы, трансформирующих сложившиеся представления о праве.

Надеемся, что настоящий выпуск журнала будет интересен широкому кругу читателей, а увидевшие свет статьи послужат хорошим мотиватором для тех потенциальных авторов, которые хотели бы и готовы продемонстрировать свои перспективные научные результаты и разработки в области инноваций и права на страницах нашего периодического издания (рис. 1).



Рис. 1. География посетителей сайта журнала Journal of Digital Technologies and Law (160 стран по состоянию на 30 сентября 2024 г.)

Поскольку журнал имеет большую аудиторию российских читателей, в нем публикуется значительное число российских авторов (рис. 2), важным этапом в его научной деятельности в текущем году стала индексация в авторитетном источнике библиографической информации по национальной периодике – крупнейшей российской библиографической базе данных научного цитирования – РИНЦ, аккумулирующей не только труды ученых, но также информацию об их цитировании. Включение журнала в РИНЦ – важный шаг на пути к признанию высокого научного уровня журнала. Это открывает новые возможности для авторов и редакции, предоставляет пользователям системы, читателям и исследователям по всей России широкий доступ к трудам авторов, опубликовавших у нас результаты своего научного творчества. Интерес этой системы представляют ее аналитические возможности, позволяющие не только отслеживать публикации российских ученых в научных изданиях, их цитируемость в иных журналах, но также формировать на основе полученной информации различные наукометрические показатели самого журнала.

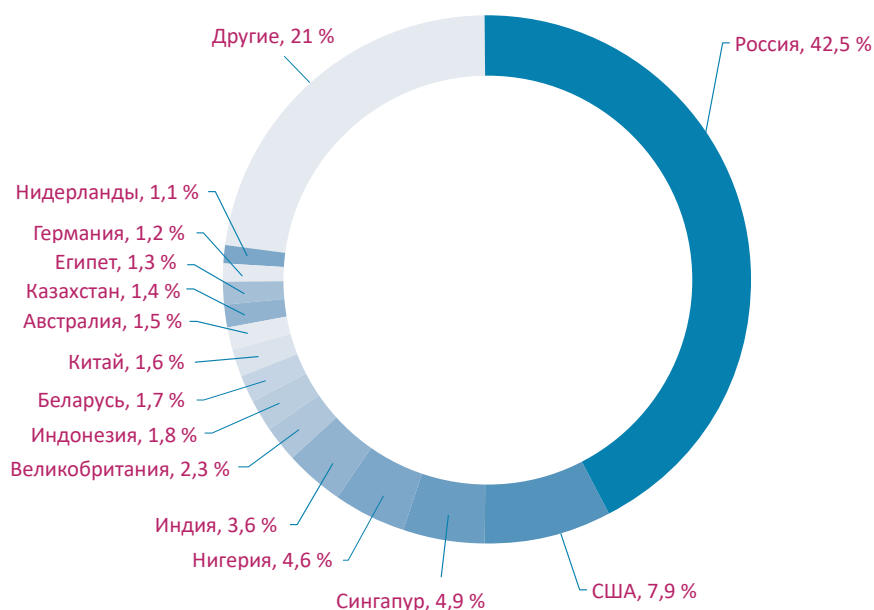


Рис. 2. Статистика посещаемости сайта журнала Journal of Digital Technologies and Law (по состоянию на 30 сентября 2024 г.)

В 2024 г. Journal of Digital Technologies and Law выступил генеральным информационным партнером крупнейшей в России и странах Содружества Независимых Государств III Международной научно-практической конференции «Цифровые технологии и право». Масштабное мероприятие ежегодно совместно организуют в рамках Международного форума Kazan Digital Week 2024 Казанский инновационный университет имени В. Г. Тимирязова и Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан при содействии Президента Академии наук Республики Татарстан, Председателя Совета Ассоциации содействия цифровому развитию Республики Татарстан Рифката Минниханова. Ежегодно конференция собирает тысячи участников из десятков стран мира.

С целью дальнейшего развития международного диалога мы готовы к взаимодействию с ведущими и молодыми специалистами, исследователями, экспертами, практикующими юристами для публикации их научных разработок по вопросам улучшения текущих подходов и создания новых методов в области этики, правового регулирования и охраны общественных отношений, связанных с цифровыми технологиями.

Выражаем благодарность авторам, рецензентам, членам редакционной коллегии, амбассадорам журнала за их сотрудничество и читателям – за растущий интерес к нашему изданию.



Научная статья

УДК 34:004:342.3:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.26>

Правовые проблемы обеспечения технологического суверенитета

Максим Викторович Залоило

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации, Москва, Россия

Ключевые слова

право,
стратегическая автономия,
стратегическое
планирование,
суверенизация правового
регулирования,
технологическая
безопасность,
технологический
суверенитет,
технологический уклад,
технологическое лидерство,
цифровая солидарность,
цифровые технологии

Аннотация

Цель: выявить правовые проблемы обеспечения технологического суверенитета и определить научно обоснованные векторы их решения.

Методы: в основе исследования лежат формально-юридический, историко-правовой, сравнительно-правовой методы, а также методология мягкой системности, юридического прогнозирования, правового моделирования.

Результаты: в статье представлен теоретико-правовой подход к пониманию и разграничению суверенитета на виды, где в современных условиях значительная роль отводится независимости и самостоятельности государства в технологической сфере. Рассмотрено соотношение цифрового и технологического суверенитета, а понятие последнего изложено с учетом набирающей популярность западной концепции цифровой (технологической) солидарности. Регулятивным фундаментом стратегической автономии государства служит правовое регулирование, в сфере которого в последние годы прочно закрепляется концепция технологоцентризма. Выявленная технологическая парадигма современных правовых регуляторов заключается в стратегировании научно-технологических новаций в документах стратегического планирования, суверенизации и циклизации правовой сферы, цифровой трансформации культуры правотворчества и правоприменения, технологизации юридического языка, расширении сферы законодательного регулирования и объема подзаконного правового массива. Проведенный анализ соотношения законодательного и подзаконного уровней технологического позиционирования Российской Федерации в стратегических областях позволил подчеркнуть важность системной взаимосвязи задействованных традиционных и инновационных инструментов правотворческого процесса в обеспечении технологического развития и выявить риски расширения правового экспериментирования в цифровой области общественных отношений, которое должно исключать возможность обхода таким образом установленных критически важных ограничений.

© Залоило М. В., 2024

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

Научная новизна: в работе сформирована теоретико-правовая модель обеспечения технологического суверенитета, имеющего стратегическое значение для сохранения суверенитета Российской Федерации в его классическом понимании как основного и важнейшего признака государства.

Практическая значимость: полученные результаты могут найти применение в правотворческой деятельности органов государственной власти по созданию правовых механизмов исследования, разработки и внедрения критических и сквозных технологий и основанному на них производству высокотехнологичной продукции в целях обеспечения национальной безопасности Российской Федерации.

Для цитирования

Залоило, М. В. (2024). Правовые проблемы обеспечения технологического суверенитета. *Journal of Digital Technologies and Law*, 2(3), 500–520. <https://doi.org/10.21202/jdtl.2024.26>

Содержание

Введение

1. Теоретико-правовой подход к пониманию суверенитета
2. Правовое регулирование как регулятивный фундамент стратегической автономии государства
3. Технологическая парадигма современных правовых регуляторов
4. Подзаконный уровень технологического позиционирования в стратегических областях

Заключение

Список литературы

Введение

Эпохальное всеобъемлющее изменение социальных и политических процессов в мире, цивилизационные вызовы современного миропорядка, усугубляющиеся усилением технологической конкуренции государств в условиях нарастающего санкционного противостояния и острого геополитического контекста, ставят на повестку дня юридической науки поиск новых подходов к защите основ национальной безопасности, надежности гарантий ее сохранения и стабильности существования общества и государства в целом. Одной из насущных задач в связи с этим является обеспечение технологической безопасности государства как важнейшей составляющей национальной безопасности, взаимообусловленной другими ее составляющими: экономической, социальной, информационной и пр.

Технологическая безопасность предполагает, прежде всего, устойчивое функционирование критически важных для обеспечения жизнедеятельности людей технологий, конкурентоспособное развитие экономики и организацию эффективного публичного управления технологиями (информационная инфраструктура, объекты энергетики, связи, транспорта, обороны, здравоохранения, продовольственного снабжения и др.), которые могут быть созданы, модернизированы, внедрены и успешно

поддерживаться в рабочем состоянии в автономном режиме вне зависимости от наличия или отсутствия политического, торгового и иного экономического взаимодействия с другими странами, а также невзирая на периодические внутренние и внешние потрясения.

Доминирующую функцию в концептуализации технологической безопасности выполняет технологический уклад, теория которого сложилась в отечественной доктрине для периодизации происходивших и будущих изменений в науке (Глазьев, Харитонов, 2009; Пашенцев и др., 2021). В настоящее время принято говорить о переходе к шестому технологическому укладу, ядро которого составляют нано-, био-, информационные технологии, срачиваемые с антропо- и техносредой (Глазьев, Косакян, 2024). Этот переход актуален в первую очередь для развитых стран, поскольку изменения технологических укладов происходят в разных государствах неодинаково, а нередко даже в одной и той же стране может существовать одновременно несколько технологических укладов (Тихомиров, 2023). Прогнозируются также седьмой и восьмой технологические уклады, новации которых должны найти отражение в модели соционормативного опережающего воздействия на них.

С утверждением техногенной цивилизации первостепенной становится потребность общества и государства в обеспечении устойчивости их организации и дальнейшего развития. При этом важнейшую роль в решении глобальных проблем человечества играют технологии, что, в частности, продемонстрировала пандемия коронавируса 2020–2021 гг. Аксиологический потенциал устойчивого развития для техногенной цивилизации был обозначен академиком В. С. Степиным еще несколько лет назад. Сейчас потребность в устойчивом развитии возведена в Российской Федерации на конституционный уровень и отражена в ст. 751 Конституции в рамках ее преобразований в 2020 г. В условиях турбулентности мирового порядка, санкционных противостояний и геополитических противоборств модель устойчивого развития Российской Федерации непосредственным образом сопряжена с уровнем реальной независимости страны в области науки, техники и технологий. Тесную связь понятие технологической безопасности обнаруживает с понятием технологического суверенитета¹, задача долгосрочного обеспечения которого имеет стратегическое значение для сохранения суверенитета Российской Федерации в его классическом понимании как основного и важнейшего признака государства².

Положенная в стратегическую основу обеспечения технологического суверенитета Российской Федерации, Стратегия научно-технологического развития³ выделяет большие вызовы научно-технологического развития страны, ответ на которые требует как получения новых знаний в рамках фундаментальной науки, создания

¹ Наличие в стране (под национальным контролем) критических и сквозных технологий, собственных линий разработки и условий производства продукции на их основе, что обеспечивает устойчивую возможность государства и общества достигать национальных целей развития.

² Кучеров, И. И., Нудель, С. Л., Семькина, О. И. (ред.) (2023). Уголовно-правовые гарантии суверенитета государства (сравнительно-правовое исследование): научно-практическое пособие. Москва: Проспект. <https://clck.ru/3EFbfw>

³ Указ Президента Российской Федерации № 145 от 28 февраля 2024 г. (2024). Собрание законодательства Российской Федерации, 10, ст. 1373.

научно-технологических платформ, осуществления комплекса организационно-координационных мероприятий, так и разработки и реализации широкого спектра правовых решений.

В сложных условиях смены векторов развития человечества при одновременном сохранении «традиционных» складывающихся на протяжении ряда лет угроз, создающих риски для стратегической безопасности страны и ее граждан, своевременность реагирования государственно-правовых механизмов, в том числе правотворчества, на требующие повседневного решения задачи управления обществом и государством становится одним из основных гарантов обеспечения жизнеспособности и нормального функционирования социальных и политических институтов. Поставленная на высоком государственном уровне задача обеспечения технологического суверенитета требует не только прорыва собственно в технологическом плане (Bergek et al., 2015; Luan et al., 2024; Ulmanen & Bergek, 2021), качественных изменений подходов к научному развитию (Лапаева, 2023; Acosta et al., 2020), но и масштабных новаций в правовой сфере, подлежащей трансформации под влиянием технологического императива. Поиску путей разрешения возникающих при этом правовых проблем посвящено настоящее исследование.

1. Теоретико-правовой подход к пониманию суверенитета

Суверенитет является одним из основных признаков государства. Согласно Конституции Российской Федерации, суверенитет Российской Федерации распространяется на всю ее территорию (ч. 1 ст. 4), а Российская Федерация обеспечивает защиту своего суверенитета и территориальной целостности (ч. 21 ст. 67). Суверенитет, исходя из правовой позиции Конституционного Суда Российской Федерации⁴, а также его общепринятого понимания в отечественной доктрине, предполагает верховенство, независимость и самостоятельность государственной власти, полноту законодательной, исполнительной и судебной власти государства на его территории и независимость в международном общении. Он выступает необходимым качественным признаком Российской Федерации как государства, характеризующим ее конституционно-правовой статус. В России суверенитет принадлежит Российской Федерации в целом, а суверенитет ее субъектов не допускается.

Со времен своего обоснования в трудах мыслителя Ж. Бодена в XVI в. понятие суверенитета претерпело некоторые изменения, наиболее заметные в современных условиях масштабных технологических новаций и цивилизационных вызовов человечеству. Отражением этих изменений стало разграничение суверенитета на виды – экономический, промышленный, энергетический, правовой, политический, сетевой и пр.

Пространственным пределом действия государственного суверенитета Российской Федерации является ее государственная граница. Вместе с тем в связи с развитием информационно-телекоммуникационных, цифровых технологий пространственные границы не являются единственным пределом распространения

⁴ Постановление Конституционного Суда Российской Федерации от 7 июня 2000 г. № 10-П «По делу о проверке конституционности отдельных положений Конституции Республики Алтай и Федерального закона «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации». (2000). Вестник Конституционного Суда Российской Федерации, 5.

независимой власти одного государства в отношении других стран, их граждан (подданных). В информационном (виртуальном, кибер-) пространстве, которое все больше становится альтернативной средой существования человека, отсутствуют территориальные границы, следовательно, усложняются как установление полного контроля над потоками информации, так и способность государства поддерживать свою суверенную власть. А в условиях ведения информационных и когнитивных войн, когда происходит борьба за сознание людей с использованием последних достижений информационных, цифровых, нейро- и прочих высоких технологий посредством деструктивного информационно-психологического воздействия, дезинформации и фейков, актуальным становится вопрос об информационном (цифровом) суверенитете государства, широко дискутируемый на полях юридической научной и научно-практической литературы (Степанов, 2024; Adams & Albakajai, 2016; Adonis, 2019; Floridi, 2020; Johnson & Post, 1996; Pizzul & Veneziano, 2023; Timmers, 2019).

В свете назревшей необходимости преодоления критического отставания страны от технологических лидеров на высоком государственном уровне получила оформление концепция технологического суверенитета (Maurer et al., 2015; Beltrán, 2016), обеспечение которого становится предметом ряда принятых в последнее время документов стратегического планирования. И хотя дробление суверенитета на виды подвергается критике как снижающее авторитет государства, в том числе и во внешней среде, принятые документы стратегического планирования ориентируют на понятие технологического суверенитета как государственного суверенитета в соответствующей сфере, предполагая создание дополнительных гарантий укрепления последнего.

В ряде зарубежных государств (страны Европейского союза, Великобритания, Канада, США) технологический суверенитет отождествляется с цифровым (Потапцева, Акбердина, 2023; Couture & Toupin, 2019; da Ponte et al., 2023). Встречается и иная точка зрения, согласно которой цифровой суверенитет поглощается технологическим (Hellmeie & Scherenberg, 2023). Настоящее исследование исходит из совместности этих понятий, которые соотносятся как часть и целое.

Используемая в контексте технологизации концепция суверенитета предполагает самостоятельное генерирование в государстве технологических и научных знаний или, в качестве альтернативы, минимально возможный уровень структурной зависимости от других стран (Dosi et al., 2006; Edler et al., 2023). Достижение достаточного уровня технологического суверенитета является предварительным условием обеспечения стратегической автономии государства (Broeders et al., 2023; Crespi et al., 2021).

Пристального внимания как со стороны государства, так и с позиций научного знания, в том числе юриспруденции, заслуживает противостоящая технологическому суверенитету концепция цифровой (технологической) солидарности, изложенная Государственным департаментом США в Стратегии международной политики Соединенных Штатов в области киберпространства и цифровых технологий (май 2024 г.) и представленная как инструмент ослабления технологического потенциала России, Китая, Ирана, КНДР и др.⁵

⁵ United States International Cyberspace & Digital Policy Strategy. <https://clck.ru/3EFd8R>

Согласно данному документу, цифровая солидарность понимается как «совместная работа по оказанию взаимной помощи жертвам злонамеренной киберактивности и другого цифрового вреда; оказание помощи партнерам, особенно странам с формирующейся рыночной экономикой, во внедрении безопасных, жизнестойких и устойчивых технологий для достижения их целей в области развития; построение сильной и инклюзивной инновационной экономики, которая может сформировать наше [США, их союзников. – Прим. М. З.] экономическое и технологическое будущее»⁶. Однако очевидным риском реализации концепта цифровой солидарности для государств, которые находятся или потенциально могут войти в сферу влияния США, может стать утрата собственного цифрового суверенитета, влекущая соответствующие последствия в виде усиления зависимости от «цифровых» лидеров, углубление цифрового неравенства народов и государств, нарушение кибербезопасности и киберустойчивости и т. д., что ставит под удар как технологический суверенитет, так и суверенитет государственной власти таких государств.

2. Правовое регулирование как регулятивный фундамент стратегической автономии государства

Обеспечение технологического суверенитета требует как интенсификации научного и производственного направлений, так и создания надлежащей нормативной основы. Вызовы техногенной цивилизации обуславливают тесную взаимосвязь и взаимовлияние правовой и технологической сфер. С одной стороны, технологии (прежде всего информационные, цифровые) прочно проникли в правовую среду, где уместно рассуждать об их применении на разных стадиях правового регулирования. Речь идет как о развитии генеративного искусственного интеллекта, способного взять на себя правотворческие, мониторинговые и экспертные функции, так и о сфере правореализации (Bex et al., 2017; Ermakova & Frolova, 2022; Pashentsev & Babaeva, 2024; Reiling, 2020), где актуальны автоматизация рутинных процедур, самоисполнимость договорных обязательств (смарт-контракты), машиночитаемость и машиноисполняемость права, медиатизация судебной власти, электронное правосудие и пр.⁷ В перспективе – внедрение в правовую сферу нейротехнологий (Филипова, 2021; Istace, 2024; Ligthart et al., 2023).

С другой стороны, право, в силу своей природы как мера опережающего отражения действительности, закономерно реагирует на динамику общественного развития, существенным пластом которого являются технологические новации. Трансформируются стадии конструирования правовой реальности, что находит отражение в законодательстве, правоприменительной практике, правовой культуре индивидов. Изменяющиеся под влиянием технологического императива индивидуальное и коллективное правосознание находят впоследствии свое отражение в праве. Таким образом, технологический императив становится определяющим в эволюции правовой сферы, где смещает достижения антропоцентризма в сторону технологоцентризма.

⁶ Там же.

⁷ Pietropaoli, I., Anastasiadou, I., Gauci, J.-P., & MacAlpine, H. Use of Artificial Intelligence in Legal Practice. British Imcstitute of International and Comparative Law. <https://clck.ru/3EFdGC>

Развитие правового регулирования отношений в сфере обеспечения технологического суверенитета происходит в направлениях:

- стратегирования будущих изменений науки, техники и технологий в программных актах;
- нарастающей суверенизации правового регулирования, которая выступает закономерным ответом на смену вектора глобализации в новых геополитических реалиях и задачу правового обеспечения стратегической автономии государства. В рамках конституционной реформы 2020 г. произошло укрепление конституционно-правового базиса российской науки, сопровождающееся последующей конкретизацией конституционных норм в документах стратегического планирования, нормативных правовых актах, регламентирующих государственную поддержку научной сферы. С обострением геополитической обстановки и нарастанием санкционных ограничений в правовой системе России продолжает ослабевать регулятивный потенциал международных и наднациональных регуляторов;
- циклизации нормативного правового массива, в рамках которой обретают системообразующее значение такие нетипичные правовые массивы, как цифровое право, начинается формирование технологического права, обеспечивающего нормативный фундамент технологической независимости страны;
- технологизации языка права и языка закона, которые приобретают междисциплинарный характер, унификации понятий и терминов цифрового (шире – технологического) правового массива;
- расширения сферы законодательного регулирования и закономерного увеличения объема подзаконного регулирования;
- распространения экспериментальных правовых режимов, в рамках которых осуществляется апробация юридических моделей новых или существенно изменяющихся под влиянием технологического императива общественных отношений;
- цифровой трансформации культуры правотворчества и законодательного процесса.

3. Технологическая парадигма современных правовых регуляторов

С точки зрения правового регулирования технологическое пространство характеризуется значительной содержательной сложностью и ввиду этого многообразием источников урегулирования соответствующих правоотношений – нормативных правовых актов как законодательного, так и подзаконного уровней регламентации общественных отношений.

Изменившиеся в процессе технологического развития потребности общества и государства неизбежно меняют систему, состав, сферу и пределы действия, а также количественное выражение источников права (Marchant & Allenby, 2017). Прогнозируется трансформация закона в более гибкий социальный регулятор (Пашенцев, 2019), замена законодательного регулирования мягким правом.

Вместе с тем в настоящее время и на ближайшую перспективу закон в современной правовой системе России продолжает оставаться главным и первичным регулятором наиболее важных и устойчивых общественных отношений, придавая ценностно-правовую направленность подзаконному регулированию. Подзаконные нормативные правовые акты соотносятся с положениями законов, в которых устанавливаются пределы подзаконного правотворчества (Абрамова, 2019).

Конкретизация законов осуществляется как по горизонтали – в других законодательных актах (первичных источниках), так и по вертикали – в принятых на их основе подзаконных нормативных правовых актах (документах вторичного свойства). При этом должна быть решена проблема определения пределов такой конкретизации:

- иерархических, предполагающих учет соподчиненности актов по юридической силе, что отражается в особенностях их издания и условиях, которые должны быть при этом соблюдены⁸;
- компетенционных (соблюдение правотворческих полномочий);
- пространственных (разграничение федеральных и региональных предметов ведения);
- содержательных, определяемых объемом и объектом правового регулирования.

Разные по форме и содержанию подзаконные акты имеют неодинаковую функциональную связь с законом. К примеру, указы Президента и постановления Правительства сами по себе могут выступать первичным источником регулирования тех или иных общественных отношений по вопросам, составляющим их исключительную компетенцию, когда эти отношения не являются предметом законодательного регулирования, но объективно нуждаются в правовой регламентации⁹.

Технологическая парадигма современных правовых регуляторов призвана решить проблему неоперативного реагирования закона на социальную и технологическую динамику. Базовый законодательный акт в этой области¹⁰ давно устарел, а неоднократно предпринимаемые попытки его модернизации (Габов и др., 2017) пока не увенчались успехом. Вынесенный в 2019 г. на общественное обсуждение новый законопроект «О научной и научно-технической деятельности» получил критические отклики со стороны научного и экспертного сообщества (Семенов и др., 2019). При этом в доктрине высказываются предложения о назревшей необходимости кодификации законодательства о науке и технологиях и закрепления всех правовых норм в этой сфере в едином акте, формирования отрасли научного права (Васильев, 2020; Лапаева, 2023). Остается нерешенным вопрос о кодификации законодательства, регулирующего отношения в сфере цифровизации. И хотя принятие Цифрового кодекса таит в себе ряд рисков (прежде всего возникновения коллизий и противоречий, а также сохранения фрагментарности правового регулирования соответствующих отношений), не подлежит сомнению необходимость упорядочения цифрового (а следом за ним в целом технологического) правового массива, например, в форме консолидации.

Объем законодательных норм, регулирующих общественные отношения, сопряженные с применением технологических решений, постоянно возрастает, в этой области принят комплекс законодательных актов различной отраслевой и предметной

⁸ Конституция Российской Федерации (ч. 3 ст. 90, ч. 1 ст. 115); Постановление Правительства Российской Федерации № 1009 от 13 августа 1997 г. (1997). Собрание законодательства Российской Федерации, 33, ст. 3895.

⁹ Так, к примеру, в результате конституционной реформы 2020 г. Правительство Российской Федерации было наделено полномочием по обеспечению государственной поддержки научно-технологического развития Российской Федерации, сохранения и развития ее научного потенциала (п. «в1» ч. 1 ст. 114 Конституции Российской Федерации).

¹⁰ О науке и государственной научно-технической политике. № 127-ФЗ от 23 августа 1996 г. (1996). Собрание законодательства Российской Федерации, 35, ст. 4137.

принадлежности (более 100 федеральных законов). Наряду с этим расширяется и число подзаконных нормативных правовых актов, устанавливающих механизмы реализации норм законов в сфере обеспечения технологического суверенитета.

Базовым направлением подзаконного регулирования отношений в сфере технологической безопасности в современных условиях является концептуализация модели технологического суверенитета и лидерства в документах стратегического планирования. Одним из основных актов здесь выступает Концепция технологического развития на период до 2030 г.¹¹ Этот документ, выделяя цели технологического развития¹², раскрывает механизмы их реализации. Комплексный подход к реализации целей технологического развития предполагает поддержку проектов технологического суверенитета, таксономия которых устанавливается на подзаконном уровне¹³.

Президентом Российской Федерации в числе национальных целей развития страны определены технологическое лидерство, а также цифровая трансформация, достижение которых характеризуется выполнением ряда целевых показателей, включая обеспечение технологической независимости и формирование рынков по направлениям биоэкономики, средств производства и автоматизации, цифровой трансформации, искусственного интеллекта, перспективных космических и энергетических технологий, увеличение доли отечественных высокотехнологичных товаров и услуг, созданных на основе собственных линий разработки, рост инвестиций в отечественные решения в сфере информационных технологий, обеспечение сетевого суверенитета и информационной безопасности в сети Интернет и др.¹⁴ Немаловажная роль отводится научной сфере, призванной создать фундамент развития соответствующих технологий, наращивать объем научных исследований и разработок, в том числе посредством увеличения внутренних затрат государства на соответствующие исследования и разработки, а также прироста частных инвестиций на эти цели.

Основными характеристиками подзаконных нормативных правовых актов являются оперативность их принятия и расширение диапазона действия. Эти характеристики актуализируются в условиях кризисных ситуаций (пандемия коронавируса, санкционное давление, угрозы технологической деградации), когда полномочия по принятию экономических и социальных мер концентрируются на подзаконном уровне, изменяется соотношение законодательного и подзаконного регулирования, повышается удельный вес оперативного подзаконного правотворчества в общем массиве принятых актов (как на федеральном, так и на региональном уровнях) (Тихомиров, 2022). Вместе с тем и в таких ситуациях положительные последствия оперативного правового реагирования могут столкнуться с негативными результатами нарушения законности. Во избежание опережающего

¹¹ Распоряжение Правительства Российской Федерации № 1315-р от 20 мая 2023 г. (2023). Собрание законодательства Российской Федерации, 22, ст. 3964.

¹² Обеспечение национального контроля над воспроизводством критических и сквозных технологий; переход к инновационно ориентированному экономическому росту, усиление роли технологий как фактора экономического и социального развития; технологическое обеспечение устойчивого функционирования и развития производственных систем.

¹³ Постановление Правительства Российской Федерации № 603 от 15 апреля 2023 г. (2023). Собрание законодательства Российской Федерации, 17, ст. 3141.

¹⁴ Указ Президента Российской Федерации № 309 от 7 мая 2024 г. (2024). Собрание законодательства Российской Федерации, 20, ст. 2584.

подзаконного регулирования тех общественных отношений, которые являются предметом законодательной регламентации, умаления роли закона в системе права и механизме правового регулирования необходимо, чтобы подзаконный акт не вступал в противоречие с законом и соответствовал ему (Абрамова, 2019).

В доктрине справедливо подчеркивается, что слабая действенность многих законов обусловлена отставанием разработки и применения подзаконных актов (Баранов, 2022). В этом контексте важным является обеспечение прямого действия законов и избежание необоснованного включения в проектируемые законодательные акты избыточного числа отсылочных норм, предполагающих дальнейшую подзаконную конкретизацию. Ориентиром оптимальной подзаконной детализации норм закона служит «достижение необходимого эффекта правовой регламентации в соответствующей сфере общественных отношений, ее полнота с точки зрения потребностей социального развития» (Абрамова, 2019).

Сохраняется проблема обеспечения соответствия и оперативной разработки подзаконных норм, обусловленных принятием соответствующих законодательных актов. Ее решением служит как одновременная разработка законодательных и конкретизирующих их подзаконных правовых норм, так и отлагательный срок вступления закона в силу, соответствующий срокам разработки конкретизирующих его положения подзаконных нормативных правовых актов.

Одновременно для Российской Федерации принятие в недружественных государствах концепции цифровой солидарности заставляет усилить правовые, институциональные и организационные шаги по обеспечению национальной безопасности и технологического суверенитета. Эти вопросы относятся не только к внешним проявлениям суверенитета государственной власти, но напрямую затрагивают внутренний суверенитет государства, под которым понимается независимость государства от любой другой политической силы внутри страны, построение национальной правовой системы на основе сложившихся правовых ценностей, правовых традиций и потребностей страны. Развитие концепции цифровой солидарности требует либо внесения изменений в действующие программно-стратегические акты, либо разработки новых для учета новых угроз в киберпространстве. Речь идет, в частности, о таком документе, как Доктрина информационной безопасности, которая была утверждена еще в далеком 2016 г.¹⁵, тогда как развитие информационно-телекоммуникационных, цифровых и прочих высоких технологий требует создания опережающего регулирования. Стратегические документы, в правовой форме определяющие направления и перспективы развития государства, имеют в условиях непрекращающихся и ускоряющихся технологических трансформаций важнейшее значение. Именно они создают правовой фундамент инновационного развития, определяя основы государственной политики. Определенными перспективами обладает идея разработки Стратегии информационной безопасности, которая как система формально-определенных положений, закрепляющих стратегическую цель, задачи и направления деятельности органов государственной власти по ее достижению, средства и ресурсы, которые могут быть на это затрачены, существенно отличается от такого документа стратегического планирования, как доктрина. Стратегия должна описывать комплексный системный подход к реализации указанных цели и задач,

¹⁵ Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. (2016). Собрание законодательства Российской Федерации, 50, ст. 7074.

согласованные и взаимосвязанные действия и мероприятия, которые базировались бы на целевых индикаторах и показателях на каждом этапе реализации.

О значительном числе до сих пор не устраненных правовых барьеров для развития технологий и обеспечения технологического лидерства страны свидетельствует пусть и позитивная, но распространяющаяся практика применения экспериментальных правовых режимов на основании Закона об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации¹⁶. С другой стороны, сохраняются риски использования экспериментальных правовых режимов в неправомерных целях обхода критически важных ограничений. В этой связи целесообразно обеспечение системной взаимосвязи инструментов правотворческого процесса для развития технологий (оценка регулирующего воздействия, «регуляторная гильотина», нормативные дорожные карты устранения барьеров Национальной технологической инициативы¹⁷).

4. Подзаконный уровень технологического позиционирования в стратегических областях

Подзаконное регулирование отношений в сфере обеспечения технологического суверенитета представляет собой наиболее значительный правовой массив среди всего многообразия принятых актов, основные особенности которого заключаются в следующем:

- стратегическая важность качественного и оптимального с учетом складывающихся внешних и внутренних условий подзаконного регулирования, вытекающая из стратегического значения самой сферы технологической безопасности, устойчивое и бесперебойное функционирование которой является необходимым условием обеспечения нормальной жизнедеятельности и гарантом защиты основных интересов общества и государства;
- предметное разнообразие и сложная система подзаконных нормативных правовых актов;
- уникальность подзаконного регулирования в сфере обеспечения технологического суверенитета (содержание подзаконных нормативных правовых актов в значительной мере специфично и усложнено за счет использования специальной терминологии, особых правовых конструкций механизмов, применимых в отношении деятельности по обеспечению технологического суверенитета);
- особая практическая (экономическая) ценность подзаконных нормативных правовых актов для эффективного развития затрагиваемых ими сфер экономики (посредством создания условий максимального благоприятствования для развития в соответствующих сферах современных технологий);
- стремительность разработки и принятия подзаконных нормативных правовых актов в случае выявления потребности в соответствующем регулировании ввиду того, что такая потребность имеет стратегическое значение для безопасности страны в целом.

¹⁶ Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации. № 258-ФЗ от 31 июля 2020 г. (2020). Собрание законодательства Российской Федерации, 31 (ч. I), ст. 5017.

¹⁷ Постановление Правительства Российской Федерации № 317 от 18 апреля 2016 г. (2016). Собрание законодательства Российской Федерации, 17, ст. 2413.

Кроме того, особенности подзаконного регулирования отношений, возникающих и развивающихся под влиянием технологического императива, выражаются в необходимости одновременной реализации как законодательно установленных основ регулирования соответствующих правоотношений¹⁸, так и определенных на высшем уровне государственного управления системных стратегических направлений развития и обеспечения приоритетной защиты указанной сферы. Зачастую задачи развития сферы технологической безопасности (которые должны решаться в том числе на уровне подзаконного нормативного правового регулирования) определяются именно в документах стратегического характера¹⁹.

С учетом указанных выше и иных законодательно установленных и определенных документами стратегического планирования приоритетных направлений развития сферы технологической безопасности можно выделить несколько блоков задач, решаемых на уровне подзаконного нормативного регулирования, в числе которых обеспечение информационной, промышленной, энергетической, транспортной безопасности, технологической независимости оборонно-промышленного комплекса.

Выше приведены только некоторые отдельные примеры аспектов технологической безопасности и подзаконных нормативных правовых актов, направленных на их урегулирование. Сама сфера технологической безопасности является обширной и охватывающей все возможные случаи применения различного рода технологий для многообразных потребностей человека.

Подзаконное нормативное правовое регулирование в рассматриваемой области представляет собой обширный массив действующих нормативных предписаний, обеспечивающих решение широкого спектра практических задач обеспечения технологического суверенитета в развитие соответствующих законодательно и политически определенных приоритетов. Оно является необходимым звеном системы правового регулирования рассматриваемых отношений, без которого невозможно обеспечить реализацию действенных механизмов защиты и совершенствования сферы технологической безопасности государства.

Заключение

По отношению к сфере обеспечения технологического суверенитета право выполняет ряд функций:

- регулятивную (создание нормативного каркаса функционирования и развития науки и технологий),
- стимулирующую (внедрение технологий в различные сферы жизнедеятельности),
- ограничительную (направленную на недопущение технологической и законотворческой сингулярности).

¹⁸ О безопасности критической информационной инфраструктуры Российской Федерации. № 187-ФЗ от 26 июля 2017 г. (2017). Собрание законодательства Российской Федерации, 31 (ч. I), ст. 4736; О безопасности объектов топливно-энергетического комплекса. № 256-ФЗ от 21 июля 2011 г. (2011). Собрание законодательства Российской Федерации, 30 (ч. 1), ст. 4604; О транспортной безопасности. № 16-ФЗ от 9 февраля 2007 г. (2007). Собрание законодательства Российской Федерации, 7, ст. 837; и др.

¹⁹ Указ Президента Российской Федерации № 400 от 2 июля 2021 г. (2021). Собрание законодательства Российской Федерации, 27 (ч. II), ст. 5351.

Обеспечение технологического суверенитета предполагает доктринальное обоснование и решение назревших и потенциальных правовых задач, среди которых:

- юридическая идентификация стратегических технологий;
- создание обновленного правового стандарта научной и научно-технологической деятельности;
- упорядочение нормативного массива в сфере технологической безопасности;
- унификация понятий и терминов технологического правового массива;
- корреляция принимаемых нормативных правовых актов с моделью технологического суверенитета, концептуализированной в действующих документах стратегического планирования;
- обеспечение прямого действия закона;
- соблюдение пределов горизонтальной и вертикальной конкретизации норм закона;
- обеспечение соответствия и оперативной разработки подзаконных норм, обусловленных принятием соответствующих законодательных актов.

Список литературы

- Абрамова, А. И. (2019). Подзаконное правотворчество в современном понимании: реалии и перспективы. *Журнал российского права*, 8, 25–35. <https://doi.org/10.12737/jrl.2019.8.3>
- Баранов, В. М. (2022). Ссылки (отсылки) в актах правотворчества: технико-юридические дефекты и пути преодоления их вредных последствий. *Журнал российского права*, 3, 5–21. <https://doi.org/10.12737/jrl.2022.025>
- Васильев, А. А. (2020). Научное право как отрасль российского права. *Управление наукой: теория и практика*, 2(4), 52–70. EDN: <https://elibrary.ru/xjobbj>. DOI: <https://doi.org/10.19181/smtp.2020.2.4.3>
- Габов, А. В., Путило, Н. В., Гутников, О. В. (2017). Проект федерального закона о науке – новый формат правового регулирования научной и инновационной деятельности. *Вестник Пермского университета. Юридические науки*, 38, 385–399. <https://doi.org/10.17072/1995-4190-2017-38-385-399>
- Глазьев, С. Ю., Косакян, Д. Л. (2024). Состояние и перспективы формирования 6-го технологического уклада в Российской экономике. *Экономика науки*, 10(2), 11–29. <https://doi.org/10.22394/2410-132X-2024-10-2-11-29>
- Глазьев, С. Ю., Харитонов, В. В. (ред.) (2009). *Нанотехнологии как ключевой фактор нового технологического уклада в экономике*: монография. Москва: Тривант. <https://elibrary.ru/quaadz>
- Лапаева, В. В. (2023). Технологический суверенитет России: правовые проблемы. *Научоведческие исследования*, 2, 60–72. EDN: <https://elibrary.ru/mntsbs>. DOI: <https://doi.org/10.31249/scis/2023.02.04>
- Пашенцев, Д. А. (ред.) (2019). *Цифровизация правотворчества: поиск новых решений*: монография. Москва: ИЗиСП: ИНФРА-М. <https://elibrary.ru/qrnijy>
- Пашенцев, Д. А., Залоило, М. В., Дорская, А. А. (2021). *Смена технологических укладов и правовое развитие России*: монография. Москва: ИЗиСП: Норма: ИНФРА-М. <https://elibrary.ru/tqiyan>
- Потапцева, Е. В., Акбердина, В. В. (2023). Технологический суверенитет: понятие, содержание и формы реализации. *Вестник Волгоградского государственного университета. Экономика*, 25(3), 5–16. EDN: <https://elibrary.ru/vdglxr>. DOI: <https://doi.org/10.15688/ek.jvolsu.2023.3.1>
- Семенов Е. В., Гутников О. В., Путило Н. В., Постников А. Е., Андриченко Л. В., Егеров С. В., Тамбовцев В. Л., Дементьев А. Н., Лапаева В. В., Боринская С. А., Салицкая Е. А., Ваганов А. Г. (2019). Проект федерального закона «О научной и научно-технической деятельности». *Управление наукой: теория и практика*, 1, 13–50. <https://elibrary.ru/tzhvio>
- Степанов, П. В. (2024). Подходы к пониманию цифрового суверенитета России. *Журнал российского права*, 28(4), 37–51. <https://doi.org/10.61205/jrp.2024.4.1>
- Тихомиров, Ю. А. (ред.) (2022). *Правовое управление в кризисных ситуациях*: монография. Москва: Проспект. <https://elibrary.ru/medwfm>
- Тихомиров, Ю. А. (ред.) (2023). *Интересы в механизме публичной власти: проблемы теории и практики*: монография. Москва: Проспект. <https://elibrary.ru/gryaci>

- Филипова, И. А. (2021). Нейротехнологии: развитие, применение на практике и правовое регулирование. *Вестник Санкт-Петербургского университета. Право*, 3, 502–521. <https://doi.org/10.21638/spbu14.2021.302>
- Acosta, M., Coronado, D., León, M., & Moreno, P. (2020). The Production of Academic Technological Knowledge: an Exploration at the Research Group Level. *Journal of the Knowledge Economy*, 11, 1003–1025. <https://doi.org/10.1007/s13132-019-0586-9>
- Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, 4(6), 256–265. <https://doi.org/10.17265/2328-2185/2016.06.003>
- Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, 21(2), 262–282. <https://doi.org/10.7454/global.v21i2.412>
- Beltrán, N. C. (2016). Technological Sovereignty: What Chances for Alternative Practices to Emerge in Daily IT Use? *Hybrid [Online]*, 3. <https://doi.org/10.4000/hybrid.987>
- Bergek, A., Hekkert, M., Jacobsson, S., Markard, J., Sandén, B., & Truffer, B. (2015). Technological innovation systems in contexts: Conceptualizing contextual structures and interaction dynamics. *Environmental Innovation and Societal Transitions*, 16, 51–64. <https://doi.org/10.1016/j.eist.2015.07.003>
- Bex, F., Prakken, H., van Engers, T., & Verheij, B. (2017). Introduction to the special issue on Artificial Intelligence for Justice (AI4J). *Artificial Intelligence and Law*, 25, 1–3. <https://doi.org/10.1007/s10506-017-9198-5>
- Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, 61, 1261–1280. <https://doi.org/10.1111/jcms.13462>
- Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Crespi, F., Caravella, S., Menghini, M., & Salvatori, C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*, 56(6), 348–354. <https://doi.org/10.1007/s10272-021-1013-6>
- da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological Sovereignty of the EU in Advanced 5G Mobile Communications: An Empirical Approach. *Telecommunications Policy*, 47(1), 102459. <https://doi.org/10.1016/j.telpol.2022.102459>
- Dosi, G., Llerena, P., & Labini, M. S. (2006). The relationships between science, technologies and their industrial exploitation: An illustration through the myths and realities of the so-called ‘European Paradox’. *Research Policy*, 35, 1450–1464. <https://doi.org/10.1016/J.RESPOL.2006.09.012>
- Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, 52(6). <https://doi.org/10.1016/j.respol.2023.104765>
- Ermakova, E. P., & Frolova, E. E. (2022). Using Artificial Intelligence in Dispute Resolution. In A. O. Inshakova, E. E. Frolova. (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (Vol. 254). Springer. https://doi.org/10.1007/978-981-16-4621-8_11
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It IS, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Hellmeier, M., & Scherenberg, F. V. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. In *European Conference on Information Systems 2023 Research Papers*, Kristiansand. https://aisel.aisnet.org/ecis2023_rp/306
- Istace, T. (2024). Human rights law: an incomplete but flexible framework to protect the human mind against neurotechnological intrusions. *Law, Innovation and Technology*, 16, 309–340. <https://doi.org/10.1080/17579961.2024.2313796>
- Johnson, D. R. & Post, D. G. (1996). Law and Borders – the Rise of Law in Cyberspace. *Stanford Law Review*, 48, 1367–1402. <https://dx.doi.org/10.2139/ssrn.535>
- Ligthart, S., Ienca, M., Meynen, G., Molnár-Gábor, F., Andorno, R., Bublitz, C., Catley, P., Claydon, L., Douglas, T., Fins, J. J., Goering, S., Haselager, W. F., Jotterand, F., Lavazza, A., McCay, A., Paz, A. W., Rainey, S., Ryberg, J., & Kellmeyer, P. (2023). Minding rights: Mapping ethical and legal foundations of ‘neurorights’. *Cambridge quarterly of healthcare ethics*, 32(4), 461–481. <https://doi.org/10.1017/S0963180123000245>
- Luan, C., Deng, S., Porter, A. L., & Song, B. (2024). An Approach to Construct Technological Convergence Networks Across Different IPC Hierarchies and Identify Key Technology Fields. In *IEEE Transactions on Engineering Management*, 71, 346–358. <https://doi.org/10.1109/TEM.2021.3120709>
- Marchant, G. E., & Allenby, B. R. (2017). Soft law: New tools for governing emerging technologies. *Bulletin of the Atomic Scientists*, 73, 108–114. <https://doi.org/10.1080/00963402.2017.1288447>
- Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. <https://doi.org/10.1109/CYCON.2015.7158468>

- Pashentsev, D. A., & Babaeva, Y. G. (2024). Artificial intelligence in law-making and law enforcement: Risks and new opportunities. *Вестник Санкт-Петербургского университета. Право*, 15(2), 516–526. <https://doi.org/10.21638/spbu14.2024.214>
- Pizzul, D., & Veneziano, M. (2023). Digital sovereignty or sovereignism? Investigating the political discourse on digital contact tracing apps in France. *Information, Communication & Society*, 27(5), 1008–1024. <https://doi.org/10.1080/1369118X.2023.2232840>
- Reiling, A. D. (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, 11(2), 8. <https://doi.org/10.36745/ijca.343>
- Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, 29(4), 635–645. <https://doi.org/10.1007/s11023-019-09508-4>
- Ulmanen, J., & Bergek, A. (2021). Influences of technological and sectoral contexts on technological innovation systems. *Environmental innovation and societal transitions*, 40, 20–39. <https://doi.org/10.1016/j.eist.2021.04.007>

Сведения об авторе



Залоило Максим Викторович – кандидат юридических наук, ведущий научный сотрудник отдела теории права и междисциплинарных исследований законодательства, Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации

Адрес: 117218, Россия, г. Москва, ул. Большая Черемушkinsкая, 34

E-mail: z-lo@mail.ru

ORCID ID: <https://orcid.org/0000-0003-4247-5242>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57215428686>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/S-4168-2018>

Google Scholar ID: https://scholar.google.ru/citations?hl=ru&user=_5-4AjwAAAAJ

РИНЦ Author ID: https://www.elibrary.ru/author_profile.asp?id=595876

Конфликт интересов

Автор является заместителем главного редактора журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование проведено в рамках государственного задания Института законодательства и сравнительного правоведения при Правительстве Российской Федерации на 2024 год

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс

Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 8 июня 2024 г.

Дата одобрения после рецензирования – 16 июня 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:342.3:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.26>

Legal Issues of Ensuring Technological Sovereignty

Maksim V. Zaloilo

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

Keywords

digital solidarity,
digital technologies,
law,
sovereignization of legal
regulation,
strategic autonomy,
strategic planning,
technological leadership,
technological mode,
technological security,
technological sovereignty

Abstract

Objective: to identify the legal issues of ensuring technological sovereignty and to determine scientifically grounded vectors of their solution.

Methods: the study is based on formal-legal, historical-legal, comparative-legal methods, as well as the methodology of soft systematicity, legal forecasting, and legal modeling.

Results: the article presents a theoretical and legal approach to understanding sovereignty and differentiating its types. Under modern conditions, a significant role is given to the independence and autonomy of the state in the technological sphere. The correlation of digital and technological sovereignty is considered; the latter notion is outlined taking into account the gaining popularity of the Western concept of digital (technological) solidarity. The regulatory foundation of the state strategic autonomy is legal regulation, in which the concept of technology-centrism has been firmly established in recent years. The technological paradigm of modern legal regulations was identified. It consists in strategizing the scientific and technological innovations in strategic planning documents, as well as in sovereignization and cyclization of the legal sphere, digital transformation of the culture of lawmaking and law enforcement, technologization of the legal language, expansion of the scope of legislative regulation and the volume of subordinate legislation. The analysis of the correlation between the legislative and subordinate law levels of technological positioning of the Russian Federation in strategic areas has allowed to emphasize the important systemic interrelation of the involved traditional and innovative law-making tools as they ensure technological development. The author also identifies the risks of expanding legal experimentation in the digital area of public relations, which should exclude the possibility of circumventing the established critical limitations.

© Zaloilo M. V., 2024

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 work forms a theoretical and legal model of ensuring technological sovereignty, which is of strategic importance for the preservation of the Russian Federation sovereignty in its classical understanding as the main and most important feature of the state.

Practical significance: the results can be used in law-making activities of public authorities to create legal mechanisms for research, development and implementation of critical and end-to-end technologies and the production of high-tech products based on them in order to ensure national security of the Russian Federation.

For citation

Zaloilo, M. V. (2024). Legal Issues of Ensuring Technological Sovereignty. *Journal of Digital Technologies and Law*, 2(3), 500–520. <https://doi.org/10.21202/jdtl.2024.26>

References

- Abramova, A. I. (2019). By-law-making in the Modern Understanding: Realities and Prospects. *Journal of Russian Law*, 8, 25–35. (In Russ.). <https://doi.org/10.12737/jrl.2019.8.3>
- Acosta, M., Coronado, D., León, M., & Moreno, P. (2020). The Production of Academic Technological Knowledge: an Exploration at the Research Group Level. *Journal of the Knowledge Economy*, 11, 1003–1025. <https://doi.org/10.1007/s13132-019-0586-9>
- Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, 4(6), 256–265. <https://doi.org/10.17265/2328-2185/2016.06.003>
- Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, 21(2), 262–282. <https://doi.org/10.7454/global.v21i2.412>
- Baranov, V. M. (2022). References in Law-Making Acts: Technical and Legal Defects and Ways to Overcome Their Harmful Consequences. *Journal of Russian Law*, 26(3), 5–21. (In Russ.). <https://doi.org/10.12737/jrl.2022.025>
- Beltrán, N. C. (2016). Technological Sovereignty: What Chances for Alternative Practices to Emerge in Daily IT Use? *Hybrid [Online]*, 3. <https://doi.org/10.4000/hybrid.987>
- Bergek, A., Hekkert, M., Jacobsson, S., Markard, J., Sandén, B., & Truffer, B. (2015). Technological innovation systems in contexts: Conceptualizing contextual structures and interaction dynamics. *Environmental Innovation and Societal Transitions*, 16, 51–64. <https://doi.org/10.1016/j.eist.2015.07.003>
- Bex, F., Prakken, H., van Engers, T., & Verheij, B. (2017). Introduction to the special issue on Artificial Intelligence for Justice (AI4J). *Artificial Intelligence and Law*, 25, 1–3. <https://doi.org/10.1007/s10506-017-9198-5>
- Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, 61, 1261–1280. <https://doi.org/10.1111/jcms.13462>
- Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Crespi, F., Caravella, S., Menghini, M., & Salvatori, C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*, 56(6), 348–354. <https://doi.org/10.1007/s10272-021-1013-6>
- da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological Sovereignty of the EU in Advanced 5G Mobile Communications: An Empirical Approach. *Telecommunications Policy*, 47(1). <https://doi.org/10.1016/j.telpol.2022.102459>
- Dosi, G., Llerena, P., & Labini, M. S. (2006). The relationships between science, technologies and their industrial exploitation: An illustration through the myths and realities of the so-called ‘European Paradox’. *Research Policy*, 35, 1450–1464. <https://doi.org/10.1016/J.RESPOL.2006.09.012>
- Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, 52(6). <https://doi.org/10.1016/j.respol.2023.104765>

- Ermakova, E. P., & Frolova, E. E. (2022). Using Artificial Intelligence in Dispute Resolution. In A. O. Inshakova, E. E. Frolova. (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (Vol. 254). Springer. https://doi.org/10.1007/978-981-16-4621-8_11
- Filipova, I. A. (2021). Neurotechnologies: Development, practical application and regulation. *Vestnik of Saint Petersburg University. Law*, 3, 502–521. (In Russ.). <https://doi.org/10.21638/spbu14.2021.302>
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It IS, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Gabov, A. V., Putilo, N. V., & Gutnikov, O. V. (2017). The Draft Federal Law on Science – a New Format of Legal Regulation of Scientific and Innovation Activities. *Perm University Herald. Juridical Sciences*, 38, 385–399. (In Russ.). <https://doi.org/10.17072/1995-4190-2017-38-385-399>
- Glazyev, S. Yu., & Kharitonov, V. V. (Eds.) (2009). *Nanotechnology as a key factor of the new technological mode in the economy: monograph*. Moscow: Trovant. (In Russ.).
- Glazyev, S. Yu., & Kosakyan, D. L. (2024). State and Prospects of 6th Technological Mode in Russian Economy. *Economics of Science*, 10(2), 11–29. (In Russ.). <https://doi.org/10.22394/2410-132X-2024-10-2-11-29>
- Hellmeier, M., & Scherenberg, F. V. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. In *European Conference on Information Systems 2023 Research Papers*, Kristiansand. https://aisel.aisnet.org/ecis2023_rp/306
- Istace, T. (2024). Human rights law: an incomplete but flexible framework to protect the human mind against neurotechnological intrusions. *Law, Innovation and Technology*, 16, 309–340. <https://doi.org/10.1080/17579961.2024.2313796>
- Johnson, D. R. & Post, D. G. (1996). Law and Borders – the Rise of Law in Cyberspace. *Stanford Law Review*, 48, 1367–1402. <https://dx.doi.org/10.2139/ssrn.535>
- Lapaeva, V. V. (2023). Technological sovereignty of Russia: legal issues. *Science Studies*, 2, 60–72. (In Russ.).
- Lighthart, S., Ienca, M., Meynen, G., Molnár-Gábor, F., Andorno, R., Bublitz, C., Catley, P., Claydon, L., Douglas, T., Fins, J. J., Goering, S., Haselager, W. F., Jotterand, F., Lavazza, A., McCay, A., Paz, A. W., Rainey, S., Ryberg, J., & Kellmeyer, P. (2023). Minding rights: Mapping ethical and legal foundations of ‘neurorights’. *Cambridge quarterly of healthcare ethics*, 32(4), 461–481. <https://doi.org/10.1017/S0963180123000245>
- Luan, C., Deng, S., Porter, A. L., & Song, B. (2024). An Approach to Construct Technological Convergence Networks Across Different IPC Hierarchies and Identify Key Technology Fields. In *IEEE Transactions on Engineering Management*, 71, 346–358. <https://doi.org/10.1109/TEM.2021.3120709>
- Marchant, G. E., & Allenby, B. R. (2017). Soft law: New tools for governing emerging technologies. *Bulletin of the Atomic Scientists*, 73, 108–114. <https://doi.org/10.1080/00963402.2017.1288447>
- Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. <https://doi.org/10.1109/CYCON.2015.7158468>
- Pashentsev, D. A. (Ed.) (2019). *Digitalization of Law-Making: the Research for New Solutions*: monograph. Moscow: ILCL: INFRA-M. (In Russ.).
- Pashentsev, D. A., & Babaeva, Y. G. (2024). Artificial intelligence in law-making and law enforcement: Risks and new opportunities. *Vestnik of Saint Petersburg University. Law*, 15(2), 516–526. <https://doi.org/10.21638/spbu14.2024.214>
- Pashentsev, D. A., Zaloilo, M. V., & Dorskaya, A. A. (2021). *Changing of Technological Orders and Legal Development of Russia*: monograph. Moscow: ILCL: Norma: INFRA-M. (In Russ.).
- Pizzul, D., & Veneziano, M. (2023). Digital sovereignty or sovereignism? Investigating the political discourse on digital contact tracing apps in France. *Information, Communication & Society*, 27(5), 1008–1024. <https://doi.org/10.1080/1369118X.2023.2232840>
- Potapitseva, E. V., Akberdina, V. V. (2023). Technological Sovereignty: Concept, Content, and Forms of Implementation. *Journal of Volgograd State University. Economics*, 25(3), 5–16. (In Russ.). <https://doi.org/10.15688/ek.jvolsu.2023.3.1>
- Reiling, A. D. (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, 11(2), 8. <https://doi.org/10.36745/ijca.343>
- Semenov, E. V., Gutnikov, O. V., Putilo, N. V., Postnikov, A. E., Andrichenko, L. V., Egerev, S. V., Tambovtsev, V. L., Dementiev, A. N., Lapaeva, V. V., Borinskaya, S. A., Salitskaya, E. A., & Vaganov, A. G. (2019). Draft Federal Law “On scientific and scientific-technical activity”. *Upravlenie naukoj: teoriya i praktika*, 1, 13–50. (In Russ.).
- Stepanov, P. V. (2024). Approaches to Understanding Russia’s Digital Sovereignty. *Journal of Russian Law*, 28(4), 37–51. (In Russ.). <https://doi.org/10.61205/jrp.2024.4.1>

- Tikhomirov, Yu. A. (Ed.) (2022). *Legal Management in Crisis Situations*: monograph. Moscow: Prospect. (In Russ)
- Tikhomirov, Yu. A. (Ed.) (2023). *Interests in the mechanism of public power: issues of theory and practice*: monograph. Moscow: Prospect. (In Russ.).
- Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, 29(4), 635–645. <https://doi.org/10.1007/s11023-019-09508-4>
- Ulmanen, J., & Bergek, A. (2021). Influences of technological and sectoral contexts on technological innovation systems. *Environmental innovation and societal transitions*, 40, 20–39. <https://doi.org/10.1016/j.eist.2021.04.007>
- Vasiliev, A. A. (2020). Scientific law as a branch of Russian law. *Science Management: Theory and Practice*, 2(4), 52–70. (In Russ.). <https://doi.org/10.19181/smtp.2020.2.4.3>

Author information



Maksim V. Zaloilo – Cand. Sci. (Law), Leading Researcher of the Department of Theory of Law and Interdisciplinary Research of Legislation, Institute of Legislation and Comparative Law under the Government of the Russian Federation

Address: 34 Bolshaya Cheremushkinskaya Str., 117218 Moscow, Russia

E-mail: z-lo@mail.ru

ORCID ID: <https://orcid.org/0000-0003-4247-5242>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57215428686>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/S-4168-2018>

Google Scholar ID: https://scholar.google.ru/citations?hl=ru&user=_5-4AjwAAAAJ

РИНЦ Author ID: https://www.elibrary.ru/author_profile.asp?id=595876

Conflict of interests

The author is the Deputy Editor-in-Chief of the Journal; the article was reviewed on general terms.

Financial disclosure

The research was performed within the framework of the 2024 state assignment of the Institute of Legislation and Comparative Law under the Government of the Russian Federation.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – June 8, 2024

Date of approval – June 16, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:342.721:612.6

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

DOI: <https://doi.org/10.21202/jdtl.2024.27>

Редактирование генома человека: управление технологическими рисками правовыми средствами

Александра Алексеевна Троицкая ✉

Московский государственный университет имени М. В. Ломоносова, Москва, Россия

Константин Александрович Шарловский

Пепеляев Групп, Москва, Россия

Ключевые слова

генетические технологии,
генетическое
редактирование,
геном человека,
законодательство,
право,
репродуктивные технологии,
рискориентированный
подход,
технологический риск,
цифровые технологии,
юридическая
ответственность

Аннотация

Цель: определить теоретические подходы к правовому регулированию репрогенетического редактирования с учетом рискориентированного подхода и практики регулирования такого рода прорывных технологий в различных юрисдикциях, а также наметить дальнейшие нормативные и управленческие шаги, которые должны быть предприняты для развития технологии.

Методы: общенаучные методы анализа и синтеза, классификация, системный и функциональный подходы; частнонаучные методы – формально-юридический, сравнительно-правовой, историко-правовой.

Результаты: проведенное исследование показывает возможные варианты подходов к регулированию генетического редактирования в репродуктивных целях. Рассмотренные варианты оценены с точки зрения рискориентированного подхода, определены условия и особенности применения различных регуляторных механизмов, а также дана оценка текущему отечественному регулированию в этой сфере. По итогам анализа возможно заключить, что запрет или существенное ограничение развивающейся технологии репрогенетического редактирования не имеет под собой неопровержимых оснований, более того, может привести скорее к обратным результатам, нежели те, которые декларируются сторонниками такого подхода. В этой связи необходимо развивать дискуссию в конструктивном итеративном ключе, вовлекая в нее всех стейкхолдеров, в том числе научное сообщество.

✉ Контактное лицо

© Троицкая А. А., Шарловский К. А., 2024

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: обобщение и концептуальное осмысление опыта правового регулирования репрогенетических технологий на международном уровне, в рамках различных юрисдикций, а также анализ естественно-научных доводов в контексте оценки эффективности внедряемого регулирования позволяют не только системно рассмотреть существующие и гипотетически возможные риски развития и использования генетических технологий, но дают возможность использовать рискориентированный подход к анализу проблем правового регулирования технологий редактирования генома человека. Это позволяет сделать следующий шаг в осмыслении феномена генетического редактирования.

Практическая значимость: результаты настоящего исследования могут быть использованы для целей выстраивания дальнейшего конструктивного диалога по поводу применения правовых механизмов к вопросам редактирования генома человека. Исследование также возможно рассматривать в качестве основы для использования итеративного подхода в рамках дальнейшей дискуссии.

Для цитирования

Троицкая, А. А., Шарловский, К. А. (2024). Редактирование генома человека: управление технологическими рисками правовыми средствами. *Journal of Digital Technologies and Law*, 2(3), 521–543. <https://doi.org/10.21202/jdtl.2024.27>

Содержание

Введение

1. Редактирование генома человека: текущее положение вещей в России

1.1. Биомедицинская составляющая

1.2. Правовая составляющая

2. Потенциальные механизмы регулирования

2.1. Принципиальные установки

2.2. Нормативная правовая база

2.3. Управление и контроль

Заключение

Список литературы

Введение

Редактирование генома – одна из технологий, которая заметным образом прогрессировала благодаря достижениям не только молекулярной биологии, но и цифрового инструментария (Atimango et al., 2024; Pombo, 2011; Wilson, 2023; Tan et al., 2023; Sharif et al., 2023). Именно благодаря этому инструментарии в генетике могли быть обработаны большие данные о последовательностях нуклеотидов, генетической экспрессии, взаимосвязях генов на выстраиваемые аминокислоты и т. д. (Балашенко, 2016). Это же относится и к результатам применения для редактирования генома CRISPR-технологий.

Существуют различные виды редактирования генома человека. Не только с биомедицинской, но и с правовой точки зрения значение имеет разница между

редактированием в медицинских и немедицинских целях, а также редактированием соматических клеток, затрагивающим только конкретного пациента, и зародышевой линии, изменение которой может проявить себя и в будущих поколениях (Yu et al., 2012).

В России сохраняется неопределенность правового регулирования наследуемого редактирования генома человека в каких бы то ни было целях при нерешенности ряда этических вопросов в этой сфере. Фактически наследуемое редактирование осуществляется на уровне фундаментальных исследований (хотя и при нехватке контроля за ними) и не проводится в целях репродукции. Между тем есть ощущение, что развитие данной биомедицинской сферы, причем развитие максимально безопасное как для отдельных участников происходящего (доноров генетического материала, потенциальных родителей и детей, а также собственно исследователей), так и для популяции в целом требует понятных правовых рамок, обеспечивающих не только предсказуемость, но и программируемое совершенствование технологии, процедур и результатов ее применения.

Статья построена следующим образом. Вначале в ней будет представлено текущее положение дел в России с редактированием генома человека, при этом акцент будет сделан на рисках, обычно ассоциируемых с технологией, и существующих (в действительности, скорее, несуществующих) правовых нормах, относящихся к ней. Далее будут рассмотрены возможные конкретные механизмы регулирования, которые могли бы обеспечить адекватное сочетание генетических и репродуктивных технологий строго в медицинских целях на практике, при надлежащем контроле со стороны органов государственной власти и научного сообщества. На этой основе будут сделаны выводы относительно перспектив правового регулирования технологии в России.

1. Редактирование генома человека: текущее положение вещей в России

1.1. Биомедицинская составляющая

По своей сути редактирование генома означает целенаправленное внесение изменений в ДНК организма путем добавления, устранения или перемещения генетического материала. Как таковое оно может быть применено к самым разным организмам и потому реально или потенциально востребовано в различных областях – от сельского хозяйства и промышленности до здравоохранения и биобезопасности (Asquer & Morrison, 2022). Самые серьезные ожидания были связаны с технологией редактирования CRISPR-Cas9, по некоторым описаниям претендовавшей на сравнительную (по отношению к другим методам, таким как вирусные векторы, нуклеазы «цинковые пальцы» (ZFN), или TALENs) точность, эффективность и дешевизну в использовании (Barnett, 2017), хотя нельзя было не заметить, что в действительности жизнерадостная оценка несколько опровергалась данными о реально проведенных экспериментах с очень небольшим процентом успеха на выходе (Liang et al., 2015; Ma H. et al., 2017; Ledford, 2017). Именно этот способ был заявлен в нашумевшей истории китайского исследователя Хэ Дзянькуя, не только подвергнувшего корректировке ген, кодирующий белок, используя который в организм проникает ВИЧ, но и пересадившего (вопреки существующему в КНР законодательному запрету) измененные таким образом

эмбрионы в полость матки, что окончилось рождением двух девочек (и уголовным наказанием для самого исследователя)¹.

В Российской Федерации фундаментальные исследования, вовлекающие изменение генома эмбрионов, также предпринимаются. Известность получила деятельность группы Д. В. Ребрикова, особенно после многочисленных публикаций в СМИ о готовности исследователя использовать технологию, вслед за китайским ученым, в репродуктивных целях². Нужно уточнить, что со временем фокус внимания группы был смещен с ситуаций, связанных с создаваемой невосприимчивостью к некоторым вариантам ВИЧ (что хотя и имело явные медицинские цели, но все же означало не излечение уже имеющегося заболевания как такового, а скорее, обретение «суперспособности» избегать инфицирования³), на наследственную тугоухость. Аутосомно-рецессивный тип наследования заболевания, на первый взгляд, не требует таких радикальных мер, как генетическое редактирование, – болезнь проявляется только в гомозиготном состоянии, т. е. тогда, когда обе копии гена, расположенные на гомологичных аутосомах, являются поврежденными. Даже если оба родителя являются носителями заболевания, по законам Менделя вероятность рождения больного ребенка равна 25 % и может быть нивелирована применением таких технологий, как экстракорпоральное оплодотворение и преимплантационное генетическое тестирование с целью отбора эмбрионов, которые не столкнутся с манифестацией заболевания⁴. На самом же деле картина заметно меняется, если принять во внимание еще и социокультурную сторону вопроса. Если семьи создаются внутри сообщества людей с наследственной тугоухостью (а часто так и происходит), то ни одного эмбриона, не получившего этого заболевания, у пары может не оказаться. В таком случае редактирование выглядит как противодействие именно заболеванию будущего потомства и вдобавок в ситуации без отчетливых альтернатив.

Тем не менее на сегодняшний день от органов публичной власти в России не было получено явно выраженного одобрения на проведение редактирования в репродуктивных целях⁵. В отсутствие такого одобрения, насколько можно судить, редак-

¹ См., например: Cyranoski, D. (2018, November 28). CRISPR-Baby Scientist Fails to Satisfy Critics. *Nature*. <https://clck.ru/3DrtT2>

² См., например: В России создают детей с измененной ДНК. Чем это грозит стране. (2019, 14 июня). РИА Новости. <https://clck.ru/3DrtV2>

³ И тем самым в дополнение ко всем другим критическим замечаниям в адрес Хэ Дзянькуя продуцировало дополнительные упреки в движении в сторону немедицинских целей создания потомства с заданными характеристиками (проблема так называемых дизайнерских детей). См., например: Chinese scientist who produced genetically altered babies sentenced to 3 years in jail. (2019, December 30). *Science*. <https://clck.ru/3DrtWp>

⁴ Конструкция, безусловно, сама по себе не свободная от нареканий, в первую очередь этического характера (Henaghan, 2006), однако вполне легально применимая на практике, в том числе в России. См.: Приказ Министерства здравоохранения РФ № 803н от 31.07.2020, п. 10 которого прямо предусматривает в числе показаний для Вспомогательной репродуктивной технологии (далее – ВРТ) «наследственные заболевания, для предупреждения которых необходимо преимплантационное генетическое тестирование (далее – ПГТ), независимо от статуса фертильности».

⁵ В 2019 г. министерство отказало в выдаче такого разрешения, ссылаясь на неизученность возможных осложнений в кратко- и долгосрочной перспективах, а также на позицию ВОЗ. См.: Минздрав заявил, что выдавать разрешение на изменение генома человека пока преждевременно. (2019, 6 октября). ТАСС. <https://clck.ru/3Drtgc>

рование не выходит за пределы стадии фундаментальных исследований, чему способствует в том числе и неопределенность в вопросе о правовых последствиях для российских ученых в том случае, если они решат двинуться по стопам китайского коллеги.

1.2. Правовая составляющая

Правовая составляющая развития и применения обсуждаемой технологии в России действительно остается неопределенной. Нельзя сказать, что нормативная база в сфере геной инженерии вовсе отсутствует, но именно по вопросу о внесении в геном человека наследуемых изменений нормативных положений, которые можно было бы назвать достаточно четкими, не просматривается.

В частности, Федеральный закон от 5 июля 1996 г. № 86-ФЗ «О государственном регулировании в области генно-инженерной деятельности»⁶ (с последующими изменениями) в первой же статье уточняет, что «порядок осуществления генно-инженерной деятельности и применения ее методов к человеку, тканям и клеткам в составе его организма, за исключением генодиагностики и геной терапии (генотерапии), не является предметом»⁷ его регулирования. При этом в соответствии со ст. 2 геной терапия (генотерапия) понимается как «совокупность генно-инженерных (биотехнологических) и медицинских методов, направленных на внесение изменений в генетический аппарат соматических клеток человека в целях лечения заболеваний»⁸; поскольку речь явным образом идет только о соматических клетках, то внесение изменений в зародышевую линию (собственно, наследуемых изменений) данным законом столь же явным образом не регулируется.

Отдельного внимания заслуживает вопрос о том, откуда могут или не могут браться эмбрионы для фундаментальных исследований. В этом контексте часто цитируют Конвенцию Совета Европы о защите прав и достоинства человека в связи с применением достижений биологии и медицины 1997 г., согласно ст. 18 которой «создание эмбрионов человека в исследовательских целях запрещается»⁹. Эта норма выглядит вполне однозначной, причем в двух аспектах: она запрещает специально под исследования создавать эмбрионы и не запрещает использовать те, что остались от применения вспомогательных репродуктивных технологий. В данной статье мы сознательно не заостряем внимание на обсуждении рисков, в том числе этических, возникающих в этом вопросе, потому что этому посвящена другая детальная публикация (Троицкая, 2022), но нетрудно заметить, что если эмбрионы разрешено создавать *in vitro* и проводить их тестирование, а признанные непригодными или не востребовавшие для пересадки не запрещено утилизировать (а так и обстоит дело в России), то по сравнению с этим этический вызов проведения на таких

⁶ Федеральный закон от 5 июля 1996 г. № 86-ФЗ «О государственном регулировании в области генно-инженерной деятельности» // Собрание законодательства РФ. 1996. № 28. Ст. 3348.

⁷ Там же.

⁸ Там же.

⁹ Конвенция Совета Европы о защите прав и достоинства человека в связи с применением достижений биологии и медицины 1997 г. <https://clck.ru/3EBHyX>

эмбрионах исследований (опять же с последующей утилизацией¹⁰) не выглядит как более устрашающий.

Однако российское государство не является участником данной Конвенции, и ситуация для него должна быть уточнена в соответствии с этим. В правовом пространстве России не только не запрещено использовать неостребованные в рамках ВРТ эмбрионы, но и явного запрета на их создание специально для исследований не присутствует. Федеральный закон от 23 июня 2016 г. № 180-ФЗ «О биомедицинских клеточных продуктах» запрещает создавать эмбрионы человека в целях производства таких продуктов, а также использовать в этих целях биологический материал, полученный путем прерывания процесса развития эмбриона или плода человека или нарушения такого процесса. При этом определение, содержащееся в этом же законе, заставляет задуматься, является ли отредактированный эмбрион биомедицинским клеточным продуктом. По определению, биомедицинский клеточный продукт – комплекс, состоящий из клеточной линии (клеточных линий) и вспомогательных веществ либо из клеточной линии (клеточных линий) и вспомогательных веществ в сочетании с прошедшими государственную регистрацию лекарственными препаратами для медицинского применения, и (или) фармацевтическими субстанциями, включенными в государственный реестр лекарственных средств, и (или) медицинскими изделиями. Эмбрион хоть и может быть источником клеточной линии, сам ею, судя по имеющимся определениям¹¹, не является. Также полагаем, что в случае с отредактированными эмбрионами не соблюдается второй критерий отнесения продукта к биомедицинским клеточным продуктам, а именно – эмбрион не включает в себя вспомогательные вещества и/или лекарственные средства, фармацевтические субстанции, медицинские изделия. Кроме того, в законе специально уточняется, что он не применим при использовании половых клеток человека в целях применения вспомогательных репродуктивных технологий, а также к отношениям, возникающим при обращении клеток и тканей человека в научных и образовательных целях. Соответственно, приведенный

¹⁰ Как еще будет показано далее, правовой порядок, который допускает эксперименты с эмбрионами, но не разрешает пересадку измененных эмбрионов в полость матки, имеет такой инструмент, как запрет развития эмбрионов *in vitro* более определенного срока, например, 14 дней. Этот срок был результатом консенсуса, достигнутого еще в 1979 г. по предложению США. Логика при этом была следующая: до этого момента эмбрион еще может поделиться на два (в результате чего появляются одноплодные близнецы) или быть поглощенным другим эмбрионом (в случае многоплодной беременности), и, соответственно, о появлении конкретной личности до 14 дней еще говорить не приходится. Однако в последнее время можно заметить оживление дискуссии, допускающей изменение этого консенсуса и продления срока существования эмбрионов до 21 или даже 28 дней. Насколько можно понять аргументы сторонников увеличения срока, в центре их заботы находится не какое-то принципиально новое понимание эмбриогенеза; речь идет в основном о том, чтобы иметь время (и развивающийся объект исследования) и лучше изучить последствия вносимых в геном корректив, увидеть чуть более отдаленные последствия редактирования для клеток и тканей эмбриона и в перспективе надежнее контролировать движение к здоровому потомству у людей. См. (McCully, 2021).

¹¹ В самом Федеральном законе под клеточной линией понимается стандартизованная популяция клеток одного типа с воспроизводимым клеточным составом, полученная путем изъятия из организма человека биологического материала с последующим культивированием клеток вне организма человека. В научной литературе встречаются также иные определения, например: клеточная линия – «совокупность клеток, полученная из первичной культуры путем увеличения количества клеток после нескольких генераций с преобладанием клеток или линий дифференцировки с высоким темпом роста и высокой однородностью клеточной популяции» (Черкасова, Брилкина, 2015).

запрет создания эмбрионов для получения биомедицинских клеточных продуктов не затрагивает интересующие нас в данном случае исследования.

Уже упоминавшийся Приказ Минздрава № 803н указывает на возможность диагностики и хранения гамет и эмбрионов, но не регулирует вопрос об их редактировании и тем более вопрос о создании эмбрионов в целях развития соответствующих технологий, что как раз неудивительно, поскольку его предметом являются вспомогательные репродуктивные технологии, а не фундаментальные исследования.

Похоже, что в такой ситуации определение источников появления эмбрионов для исследований остается на усмотрение конкретного научного коллектива, а сами изыскания следуют логике, определяемой его руководителем.

Что же касается ответственности в случае, если отредактированные эмбрионы будут пересажены в полость матки (допустим, согласной на это) женщины, то и она остается не вполне определенной. Статья 235 УК РФ предусматривает наказания за осуществление медицинской деятельности лицом, не имеющим лицензии на данный вид деятельности, при условии, что такая лицензия обязательна, если это повлекло по неосторожности причинение вреда здоровью человека или (отдельный состав) смерть человека. Данная статья может быть применима в том случае, когда редактирование и пересадка отредактированного эмбриона осуществлялись вне стен медицинской организации, имеющей необходимую лицензию. В рамках редактирования генома, по-видимому, речь идет о лицензии на осуществление медицинской деятельности, предусматривающей выполнение работ (услуг) по генетике и лабораторной генетике.

В объективную сторону описанного преступления, помимо осуществления деятельности без лицензии, входит также обязательное причинение вреда здоровью. По-видимому, эта статья не будет применима в ситуации, если редактирование прошло по задуманному плану, избавило будущего ребенка от заболевания и не причинило ему вреда. Редактирование может быть недостаточно точным и/или эффективным, но как именно можно доказать, что конкретные мутации – это именно побочный эффект редактирования? Кроме того, в некоторых случаях проявить себя они смогут на более поздней стадии, уже после пересадки эмбриона, в ходе пренатальной диагностики. На ком будет лежать ответственность, если в случае выявившихся проблем женщина примет решение пролонгировать беременность и родит в итоге ребенка, который не будет вполне здоров? Список таких вопросов может быть продолжен. И это не говоря о том, что даже вполне четко зафиксированный запрет на пересадку отредактированных эмбрионов в полость матки может быть сравнительно легко обойден на практике, если по соглашению врача и родителей факт редактирования будет скрыт, а генетический вариант, не ожидаемый теоретически, но появившийся в итоге будет объяснен случайной чудесной мутацией; в сущности, кто и как смог бы это опровергнуть?

Уголовным кодексом также определена ответственность за оказание услуг, в том числе медицинских, не отвечающих требованиям безопасности (ст. 238 УК РФ). Объективную сторону преступления составляет оказание услуг, не отвечающих требованиям безопасности жизни или здоровья потребителей; при этом состав является формальным, т. е. наличие ущерба здоровью конкретного потребителя (пациента) не входит в предмет доказывания (за исключением специальных составов, установленных ч. 2 и 3 ст. 238 УК РФ). Можно предположить, что оказание любой медицинской услуги будет признаваться не отвечающим требованиям безопасности в случае, если оказание такой услуги не предусмотрено стандартами и порядками оказания

медицинской помощи и не проводится в рамках клинического исследования или клинической апробации (ст. 36.1 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»). Например, описанный случай редактирования генома эмбриона для целей последующей пересадки в полость матки предполагает практическое применение разработанных и ранее не применявшихся методов профилактики, диагностики, лечения и реабилитации при оказании медицинской помощи для подтверждения доказательств их эффективности, которые должны осуществляться исключительно в порядке клинической апробации, в том числе необходимо получение одобрения этического комитета на применение способа, разрешения Минздрава на саму клиническую апробацию, в котором должно быть указано, в каких медицинских организациях, на каком количестве пациентов и в каком порядке такая апробация будет осуществляться. Очевидно, что данный разрешительный порядок введен в целях обеспечения безопасности пациентов при применении инновационных схем/способов лечения, при этом несоблюдение разрешительного порядка и осуществление редактирования генома без такого разрешения само по себе может свидетельствовать о том, что услуга не отвечает требованиям безопасности (либо как минимум позволяет презюмировать, что требования безопасности не обеспечены).

Не сильно иначе обстоит дело на принципиальном уровне, если оценивать нормы КоАП РФ. Существуют общие нормы, которые касаются осуществления деятельности без лицензии (ст. 14.1 КоАП РФ), оказания услуг ненадлежащего качества (ст. 14.4 КоАП РФ), при этом под качеством именно медицинских услуг понимается соблюдение в том числе соответствующих порядков оказания медицинской помощи и клинических рекомендаций (см. ч. 2 ст. 64 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации») и т. д. Есть и специальная норма, предусматривающая ответственность за правонарушения, совершенные в области генно-инженерной деятельности, – ст. 6.3.1 раскрывает состав как «использование генно-инженерно-модифицированных организмов и (или) продукции, полученной с применением таких организмов или содержащей такие организмы, которые не прошли государственную регистрацию в случае, если государственная регистрация предусмотрена указанным законодательством [и, похоже, имеется в виду Федеральный закон «О государственном регулировании в области генно-инженерной деятельности», который, как уже отмечалось выше, к редактированию эмбрионов не относится], или срок действия свидетельства о государственной регистрации которых истек, либо в использовании генно-инженерно-модифицированных организмов не в соответствии с целями, для которых они зарегистрированы, либо в нарушении специальных условий использования генно-инженерно-модифицированных организмов, в том числе при производстве конкретного вида продукции»¹². Едва ли создатели этой нормы имели в виду обсуждаемую нами ситуацию редактирования эмбриона в репродуктивных целях, а никакой другой специальной нормы для этой ситуации в Кодексе просто нет.

Отдельные вопросы возникают в сфере цивилистики. Каков может быть коммерческий потенциал развития (с перспективами применения на практике) технологии генетического редактирования, если ст. 1349 Гражданского кодекса РФ

¹² Кодекс об административных правонарушениях Российской Федерации. <https://clck.ru/3EBJCC>

устанавливает, что «способы модификации генетической целостности клеток зародышевой линии человека»¹³ не могут быть объектами патентных прав (хотя понятно, что разработку самих этих способов никакой акт не запрещает)¹⁴

В итоге в РФ существует ситуация, в рамках которой наследуемое редактирование эмбрионов не запрещено на уровне фундаментальных исследований, хотя процедуры контроля за появлением для этих целей эмбрионов не являются сколько-нибудь отчетливыми, а коммерческая составляющая потенциальных инвестиций в эту сферу остается «завешенной»; что же касается наследуемого редактирования в репродуктивных целях, то оно остается полностью неопределенным с точки зрения правовых последствий для его «авторов».

Однако представляется, что имеющиеся технологические продвижения, а также опасения различной степени интенсивности этического, социального и биологического характера требуют от права не сохранения сумеречной зоны, а подходов, более близких к тому, чтобы способствовать контролируемому развитию в рассматриваемой области. Не претендуя на абсолютизацию каких-либо идей, представим возможные ходы в этом направлении.

2. Потенциальные механизмы регулирования

Представляя инструменты управления, мы будем ориентироваться на опубликованные в 2021 г. Всемирной организацией здравоохранения Рамочные положения для управления в сфере редактирования генома человека¹⁵, которые наряду с другими сценариями (пренатального и постнатального редактирования соматических клеток) содержат и сценарии, касающиеся наследуемых изменений, а также на известный зарубежный опыт тех стран, для которых по их уровню технологического развития вопрос о наследуемом редактировании в принципе актуален и которые имеют некоторый опыт регламентирования этой сферы. В связи с этим следует особенно подчеркнуть, что прогресс других правовых порядков в отношении технологии редактирования ДНК человека далеко не так скромнен, как иногда считается¹⁶.

¹³ Гражданский кодекс Российской Федерации. <https://clck.ru/3EBJ6X>

¹⁴ В литературе можно встретить грамотный анализ возражений, выдвигаемых против патентования генов (негативные последствия патентной охраны таких объектов для здравоохранения и научных исследований; особая природа гена как части человеческого тела и общего наследия человечества; отсутствие качества патентоспособности). См. (Ворожевич, 2020). Отметим, однако, что в ряде случаев обсуждается патентование не видоизмененного гена как такового, а именно способов изменить его (см., например: Решение Суда по интеллектуальным правам от 15.06.2020 по делу № СИП-960/2019). В этом случае, особенно если (как указывается ниже) в этих отношениях будет участвовать государство, все или как минимум часть обозначенных возражений окажутся сняты.

¹⁵ WHO. (2021, July 12). Human Genome Editing: a Framework for Governance. <https://clck.ru/3DrtyJ>

¹⁶ Детальный обзор см.: (Baylis et al., 2020). Этим исследованием были охвачены 106 стран. Как демонстрируют авторы, в 96 из них есть документы (законодательство, акты исполнительной власти, руководящие принципы, кодексы или международные договоры), относящиеся к редактированию генома ранних эмбрионов или гамет. Некоторые страны запрещают лабораторное исследование редактирования зародышевой линии (Австрия, Германия, Хорватия и др.), некоторые разрешают (Ирландия, Норвегия, Соединенное Королевство, США, Япония и др.). Использование наследуемого редактирования в репродуктивных целях не разрешено, по утверждению авторов статьи, ни в одном из исследованных государств, хотя в отношении некоторых из них допущена формула «запрет с исключениями» (Бельгия, Италия и др.), что, конечно, особенно впечатляет.

При этом мы будем полагать само собой разумеющимся, что к приоритетному целеполаганию в этом вопросе относится развитие представлений о роли генов (а также их комплиментарного действия, эффектах эпигенетических факторов и т. д.), наряду с перспективами улучшения здоровья конкретных пациентов и будущих поколений людей с полным уважением их достоинства, а движение к этой цели требует понимания и учета рисков (действующих в том числе в условиях неопределенности), которые могут стоять за конкретными технологиями. В каком-то смысле эти идеи можно считать «вынесенными за скобки», т. е. осознаваемыми и способными быть применимыми ко всему сказанному ниже, хотя уже и не повторяемыми каждый раз специально.

2.1. Принципиальные установки

В ситуации, когда процесс создания адекватных имеющимся вызовам правовых норм и так буксует, волей-неволей возникает стремление проскочить стадию обсуждения ключевых ценностей, которые послужили бы ориентиром для будущего регулирования и управления в сфере редактирования генома человека. Тем не менее именно этой стадии и должно быть уделено внимание в первую очередь. Здесь можно было бы акцентировать следующие стартовые точки:

- необходимость развития фундаментальной науки в области генетики и смежных областях, понимания того, как функционирует человеческий геном, даже в отсутствие немедленных заранее понятных прикладных следствий этого знания;

- осознание связи между развитием науки и обеспечением достоинства личности, из которой вытекают как стремление к улучшению качества жизни людей, так и уважительное отношение к их автономии, на практике требующего понять, что именно понимается под их автономией в сфере генетического наследия (по понятным причинам, общего для популяции) и о каком именно улучшении качества жизни может идти речь, хотя уже и сейчас очевидно, что медицинские цели (даже те, которые связаны с получением способности противостоять каким-либо заболеваниям, а не только с излечением уже имеющихся) представляют собой меньший вызов, нежели «дизайн» людей с заданными характеристиками, не сцепленными с медицинскими соображениями;

- потребность в биологической безопасности, которая, однако, должна находиться в связке с представлениями о том, что технология генетического редактирования появляется не в вакууме, а в условиях действия на практике самых разных факторов, которые и без редактирования влияют на геном (включая давнее применение медицинских достижений, позволяющих сохранять в популяции самые разные комбинации генов, в том числе приводящие к манифестации заболеваний; техногенные катастрофы; изменения в системе экологических отношений; новые виды вооружений и т. д.);

Этот список может быть продолжен, в том числе идеями, вытекающими из уже озвученных, и в первую очередь это касается идеологии прозрачных, подотчетных и ответственных (причем как со стороны исследователей, так и со стороны органов публичной власти) действий, которую продвигает ВОЗ¹⁷. И, надо сказать, в ее формулировках это действительно коррелирует с ожиданиями адекватных ресурсов и создаваемых для ученых и общественности возможностей технологического прогресса¹⁸.

¹⁷ См.: Human Genome Editing: a Framework for Governance. § 14.

¹⁸ См.: Там же. § 19.

2.2. Нормативная правовая база

Зарубежный опыт показывает, что с назревшей потребностью в регулировании законодательной власти удается создать комплексный акт, охватывающий в том числе и отношения, связанные с редактированием генома. Тут можно увидеть два заметно отличающихся примера. Британский закон о фертильности и эмбриологии человека 1990 г. с последующими изменениями¹⁹ и с уточнениями, добавляемыми на уровне вторичного нормотворчества²⁰, имеет самостоятельный и ясно очерченный предмет регулирования – он содержит нормы об эмбрионах человека и любого последующего развития таких эмбрионов; запрете определенных действий в отношении эмбрионов и гамет; создании специального органа – Управления по фертильности и эмбриологии человека. Этот акт связан с иными актами, в том числе о суррогатном материнстве, но и сам выстроен полно и последовательно по своему предмету. Французский закон о биоэтике 2021 г.²¹, представляющий собой куда более непростое чтение, по сути своей является массивным перечнем вносимых изменений в другие акты, прежде всего в Кодекс общественного здравоохранения, хотя и несет с собою явно сформулированное стремление решить целый ряд биоэтических вопросов, в том числе относящихся к сфере осуществления репродуктивных прав.

Очевидно, что при движении без малого с нуля в вопросе наследуемого редактирования генома человека оба пути (создание нового самостоятельного акта или внесение дополнений в существующий в РФ Федеральный закон 2011 г. «Об основах охраны здоровья граждан в Российской Федерации») возможны. Возможен также и путь, по которому до сих пор шло регулирование вспомогательных репродуктивных технологий – актом уровня приказа Министерства здравоохранения при самых базовых установках в этом федеральном законе. Больше того, есть ощущение, что этот путь может оказаться даже в каком-то смысле²² более продуктивным для достижения в первую очередь профессионального консенсуса по ряду вопросов. В конце концов и британский, и французский законы, допуская манипуляции на эмбрионах, одинаково запрещают пересадку эмбриона с измененными ядерными генами²³ в репродуктивных целях. Можно предположить, что и в России внести ясность в этот вопрос можно нормами разного уровня, особенно если эти нормы сами по себе будут нести определенность, а также будут соотнесены с нормами Уголовного кодекса и Кодекса об административных правонарушениях.

¹⁹ Human Fertilisation and Embryology Act 1990. <https://clck.ru/3DruCm>; особенно обратим внимание на изменения 2022 г., произведенные Законом о здравоохранении и уходе (Health and Care Act 2022). <https://clck.ru/3DruDn>

²⁰ Human Fertilisation and Embryology (Research Purposes) Regulations, 2001.

²¹ Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique. <https://clck.ru/3DruFq>

²² Однако следует иметь в виду и обратную сторону монеты при использовании такого подхода: внедрение общих правил актами органа исполнительной власти имплицитно содержит в себе вероятность единовременной отмены или изменения таких правил, что делает ситуацию плохо прогнозируемой, в том числе с точки зрения как потенциальных инвесторов, так и научных коллективов/медицинских организаций.

²³ В отношении британского законодательства нужно оговориться, что использование в репродуктивных технологиях донорской митохондрии (и содержащегося в ней сравнительно небольшого числа генов) допускается. Тем не менее использование донорской органеллы, хотя и позволяет говорить о создании «генно-модифицированных» детей, не является по биомедицинской сути тем же самым, что редактирование генома.

Поэтому в действительности более сложные вопросы лежат в плоскости не столько формы, сколько содержания – определения, в каких пределах, на основе каких процедур и ресурсов могут происходить фундаментальные исследования в области редактирования генома эмбрионов или гамет. Назовем предметно:

- конституционно и законодательно значимые цели таких исследований;
- перечень (вероятно, закрытый) показаний для редактирования;
- ожидаемая фундаментальная или практическая польза для общества (в сопоставлении с предметно обозначенными рисками);
- процедуры привлечения частных или государственных средств на них;
- источники собственно материала, который вовлекается в исследования, особенно когда речь идет об эмбрионах;
- возможные на практике, нужные для исследования и при этом допустимые с этической точки зрения предельные сроки развития отредактированного эмбриона;
- меры контроля за порядком проведения и качеством результата исследования (публикации, возможность верификации результатов, а также иные меры *ex ante* (напр., разрешительный порядок, лицензирование и пр.) и *ex post* контроля и т. д.);
- степень открытости подлинных результатов для окружающих и возможность их компетентного обсуждения, в том числе научной проверки и критики;
- особенности защиты интеллектуальных прав исследователей для последующего коммерческого применения результатов их научного труда;
- степень учета имеющихся международных стандартов и зарубежных практик.

Это те вопросы, которые могли бы быть «стартовой решеткой» для разработки даже самой лаконичной, а тем более развернутой системы регулирования в вопросе наследуемого регулирования.

2.3. Управление и контроль

Судя по имеющимся сообщениям, коллектив Д. В. Ребрикова при попытках просчитать «пределы возможного» взаимодействовал с Министерством здравоохранения РФ²⁴. В структуре Минздрава имеется Департамент науки и инновационного развития здравоохранения, способный, в свою очередь, взаимодействовать с другим ведомством – Министерством науки и образования. В соответствии с приказом Минздрава РФ от 30 декабря 2020 г. № 1416, к ведению именно данного Департамента относится реализация мероприятий, направленных на инновационное развитие здравоохранения и отдельных приоритетных направлений медицинской науки, включая вопросы биомедицинских и генетических технологий. Таким образом, в принципе, в системе исполнительной власти в интересующей нас сфере мы не наблюдаем такого вакуума, какой существует в части законодательства. Тем не менее как именно должны выглядеть процедуры организации фундаментальных исследований наследуемого редактирования генома человека (за исключением порядка выделения грантовых

²⁴ Чего хочет Ребриков? (2019, 22 октября). PCR.news. <https://clck.ru/3EBKYs>

средств некоторых фондов), контроль и оценка их результатов – из ведомственных актов пока не просматривается.

Опять же по зарубежному опыту можно видеть различные возможности организации управления и контроля. Так, в Великобритании лицензию на фундаментальные исследования уполномочено выдавать Управление по фертильности и эмбриологии человека. Получаемое научным коллективом заключение признанной и независимой этической комиссии – обязательное условие обращения за такой лицензией. Заявку Управление направляет на экспертную оценку, а само тем временем организует проверку помещений и оборудования заявителя. Заявка, заключение этической комиссии, экспертные оценки заявки, отчет о проверке условий для выполнения исследований передаются в Лицензионный комитет, который и принимает решение о выдаче лицензии и при необходимости сопровождает ее дополнительными условиями (Lawford, 2020). Осуществление манипуляций с зародышевой линией без лицензии или без соблюдения ее условий – это преступное деяние, наказание за которое варьируется от штрафа до лишения свободы сроком до двух лет. Подчеркивая цели исключительно фундаментального исследования, Управление выдавало лицензии на редактирование эмбрионов человека с помощью CRISPR-технологии с 2016 г. Лицензированная указанным образом исследовательская деятельность требует также письменного информированного согласия доноров гамет или эмбрионов на то, что донорский материал будет использован именно в рамках такой деятельности. Публичное финансирование подобных исследований в Великобритании возможно и осуществляется на практике. Насколько можно судить, такой порядок взаимодействия позволяет обеспечивать проведение контролируемых исследований, но без эксцессов вроде китайского казуса.

В свою очередь, именно опыт Китая как раз и позволяет понять, какой вариант организации контроля дал осечку и каким образом органы публичной власти отреагировали на нее. До заявления о рождении двух девочек, чьи ДНК были искусственно изменены, основой регулирования генетического редактирования в КНР выступали Этические руководящие принципы исследования человеческих эмбриональных клеток, датированные 2003 г. Статья 6 этого документа запрещала как исследования человеческих эмбрионов через 14 дней после оплодотворения, так и всякие генетические манипуляции с гаметам, зиготам и эмбрионами человека в репродуктивных целях. Манипуляции в исследовательских целях требовали получения согласия этического комитета какого-либо из уполномоченных на это медицинских учреждений. На практике Хэ Дзянькуй получил такое согласие от частной медицинской компании, про которую известно не только то, что она контролирует около 80 % всех частных госпиталей в КНР, но и то, что она попадает в большое количество скандалов, обнаруживающих ее приверженность исключительно «коммерческому этосу». Такое развитие событий продемонстрировало со всею наглядностью, что полагаться на одни только этические принципы в столь деликатной сфере, как генетическое редактирование едва ли может быть отнесено к блестящим идеям.

Справедливости ради следует указать, что подобный вывод был поддержан центральным представительным органом КНР. В 2020 г. Всекитайское собрание народных представителей включило в Гражданский кодекс положения, детализирующие конституционное право на достоинство и регулирующие биомедицинские (в том числе генетические) исследования. В соответствии со ст. 1008 любое клиническое испытание в этой сфере требует этического одобрения и информированного

согласия затрагиваемых субъектов при раскрытии цели, задач и потенциальных рисков такого испытания. В ст. 1009 указывается, что «любая медицинская исследовательская деятельность, связанная с человеческим геном и человеческим эмбрионом, должна осуществляться согласно соответствующим законам, административным положениям и национальному регулированию, не должна наносить ущерб отдельным лицам и нарушать этическую мораль и общественные интересы»²⁵.

Естественно, одни только эти изменения еще не могли заблокировать варианты, подобные тем, что осуществил Хэ Дзянькуй. Однако ими дело и не закончилось.

Одновременно был разработан проект изменения Уголовного кодекса, в соответствии с которым специализированные составы преступлений, связанных с незаконной практикой редактирования генов человека, клонированием человеческого эмбриона и с серьезной угрозой безопасности генетических ресурсов человека, предусматривали санкции в виде штрафов и лишением свободы теперь уже до 7 лет²⁶.

Вместе с тем ключевая линия обороны проходит по полю исполнительной власти КНР. В части создания административных установлений прослеживается разграничение полномочий Министерства науки и технологии (разработка регулирования фундаментальных исследований) и Комитета национального здравоохранения (разработка регулирования клинических исследований) при последующем принятии соответствующих актов Государственным советом КНР. В 2019 г. был принят регламент в отношении фундаментальных исследований. Он предусматривает, что сбор, хранение и использование генетической информации подлежат либо лицензированию, либо административной регистрации. Санкции за нарушение этого требования – штрафы в размере до 5 млн юаней либо в 10-кратном размере незаконной прибыли (при вступлении в силу поправок в Уголовный кодекс должны действовать санкции за преступление, связанное с серьезной угрозой безопасности генетических ресурсов человека). В том же году был разработан проект регламента клинических исследований, предусматривающий принципиальное изменение схемы их согласования. Комитет национального здравоохранения заявил, что все клинические исследования, связанные с инновационными биомедицинскими технологиями, потребуют административного одобрения. Регламент, предлагаемый Комитетом, классифицирует клинические исследования по редактированию генов на два уровня: (1) высокого и (2) низкого и среднего риска. При этом технология редактирования генов и сопутствующие ей вспомогательные репродуктивные технологии отнесены к зоне высокого риска и в будущем должны быть одобрены самим Комитетом после рассмотрения научных и этических аспектов проекта²⁷. То есть все клинические исследования инновационных биомедицинских технологий должны теперь проходить двойную проверку: внутреннюю, проводимую медицинским учреждением, и внешнюю, за который отвечают административные органы государства. Регламент предусмотрел и требования к медицинским учреждениям, претендующим на проведение кли-

²⁵ Гражданский кодекс Китайской Народной Республики. <https://clck.ru/3EBLAD>

²⁶ Для сравнения, французский Уголовный кодекс, рассматривающий евгенические практики и репродуктивное клонирование как преступления против человечности, допускает за них лишение свободы до 30 лет и штрафы до 7 500 000 евро (ст. 214-1 и 214-2).

²⁷ Клинические исследования с низким и средним риском потребуют административного разрешения от департамента здравоохранения уровня провинции.

нических исследований и (что выглядит психологически значимым) санкции для их руководителей, а не только для лидера научной группы, как это было с Хэ Дзянькуем, на случай нарушения требований регламента. В дополнение к этому в КНР обсуждаются планы создания Национального этического контрольного комитета по науке и технологии, специально для контроля за исследованиями, вызывающими значительные этические споры, такими как проекты, связанные с технологией редактирования генов (Song & Joly, 2021).

По приведенным примерам выкристаллизовывается подход, в рамках которого административный контроль сочетается с профессиональной этической экспертизой планируемых исследований и их результатов. Несмотря на кажущуюся громоздкость этого сочетания, именно оно, вероятно (при соответствующих правилах формирования этических комитетов), и призвано обеспечить, с одной стороны, развитие науки в стратегически важной по ряду причин области при участии в принятии решений компетентных специалистов, а с другой – управляемое и относительно безопасное развитие. При этом выстраивание процедур согласования порядка проведения исследований и отчетности по ним возможно не только для целей распределения публичного финансирования, но и для частных инициатив²⁸.

К этому необходимо добавить еще один деликатный момент, связанный с проблемой верификации получаемых результатов (требуемой в том числе, если иметь в виду возможный когда-то переход от фундаментальных исследований к клиническим испытаниям и внесению наследуемых изменений в геном человека в рамках применения репродуктивных технологий), а именно внимание к тому, что в настоящий момент в России только один коллектив позиционирует себя как имеющий достаточно серьезные продвижения. На первый взгляд, юридическая наука может не беспокоиться о том, что относится к существующему порядку вещей. Но вместе с тем в этой точке начинают ощущаться некоторые издержки, хотя вербализовать их не так просто. Эти ощущения связаны с затруднительностью при таком положении вещей получить полную картину имеющихся достижений и оценить перспективу дальнейшего развития. Насколько, в сущности, точна и эффективна технология редактирования? Могут ли конкретные результаты быть уверенно повторены? Какие именно сложности возникают при редактировании, что именно отделяет нас от того, чтобы перестать опасаться появления реальных детей с отредактированной ДНК? Какой именно эффект имеют существующие финансовые вложения в эту область и каковы преимущества и издержки дальнейшего финансирования конкретных областей науки? Список этих вопросов может быть продолжен, но есть серьезное подозрение, что в отсутствие научной конкуренции или сотрудничества нескольких коллективов (либо же обстоятельной сверки результатов с зарубежными коллегами) ответы на эти вопросы будут оставаться расплывчатыми, что не будет способствовать выведению данных исследований из той отчасти маргинализованной тени, где они сейчас, как кажется, оказались.

²⁸ Как отмечает ВОЗ, правила, регулирующие финансирование частных и государственных исследований, могут налагать ряд условий, которые функционируют как инструмент управления. Например, это могут быть: условия об источнике гамет или эмбрионов (особенно об оплате и согласии их поставщиков); ограничения на продолжительность времени, в течение которого эмбрионы могут поддерживаться *in vitro*; правила создания гибридных эмбрионов; права владения и распоряжения гаметам и эмбрионами; нормы об интеллектуальных правах и обмене данными и материалами. См.: Human Genome Editing: a Framework for Governance. § 70.

В то же время проблема обмена информацией как раз и поднимает еще два важных вопроса в контексте попыток понять, как именно должна выстраиваться схема управления. Один из них – это функционирование информационной базы о проведенных генетических коррекциях и исследованиях в части редактирования генома человека²⁹. Судя по сайту Центра высокоточного редактирования и генетических технологий для биомедицины³⁰, имеется впечатляющий задел, но все же информация далека от полной. Проблема недоступности детальной информации о проведенных исследованиях характерна не только для рассматриваемой сферы генетических исследований, но также и для «классической» фармацевтики – и предлагаемые актуальным регулированием варианты ее решения, как кажется, далеки от идеальных³¹.

А второй связанный с этим вопрос – это патентоспособность результатов фундаментальных исследований. В литературе уже прозвучала критика слишком жестких подходов к (не)предоставлению патентно-правовой охраны результатов интеллектуальной деятельности в сфере редактирования генома эмбрионов человека³², и думается, что действительно требуется понять, не находится ли здесь одна из возможных точек роста не просто для уже имеющихся коллективов, но для более масштабного стимулирования научных исследований, однако в несколько другом аспекте. В частности, в науке обсуждаются такие известные способы управления результатами научного труда, как право на участие в изобретениях, созданных за счет публичного финансирования, государственные лицензии, предметные ограничения и другое, – все они предусмотрены для случаев, когда правительство либо заинтересовано в технологии, чтобы применять ее от своего имени в определенных границах, либо вынуждает владельца патента разрешить другому использовать ее так, как правительство сочтет нужным (Scheinerman & Sherkow, 2021).

Из изложенного видно, что и управление сферой генетического редактирования требует комплексных решений, где ожидания по одним вопросам явным образом влияют на ответы по другим.

²⁹ См.: Постановление Правительства РФ № 479 от 22.04.2019. (2019). Гарант.ру. <https://clck.ru/3DruV4>

³⁰ Центр высокоточного редактирования и генетических технологий для биомедицины. <https://clck.ru/3DruWd>

³¹ Например, в РФ действует открытый реестр клинических исследований лекарственных препаратов (<https://clck.ru/3DruYb>), однако его наполнение таково, что невозможно определить, как проводилось исследование, чем оно закончилось и т. д. Более того, Федеральным законом от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» (ч. 18, 21 ст. 18) в отечественный правовой порядок имплементирован так называемый институт «эксклюзивности данных», который с учетом сформировавшейся судебной практики (см. например: Определение Верховного Суда РФ от 26.05.2016 № 305-ЭС16-2399 по делу № А40-188378/14) стимулирует фармацевтические компании сохранять результаты и детали даже успешно проведенных клинических исследований в тайне как минимум на период действия эксклюзивности данных (до шести лет с даты регистрации препарата на основании проведенных исследований). При этом с учетом динамичного развития науки и значимости результатов исследований как для научных коллективов, так и в конечном итоге для общества, для конкретных пациентов можно констатировать, что сокрытие такой информации и ее защита в режиме коммерческой тайны (i) противоречат общественным интересам, (ii) могут тормозить развитие науки, (iii) не позволяют добросовестным компаниям, публикующим данные исследований, пользоваться защитой в рамках периода эксклюзивности, (iv) неясно, какую пользу реализация такого стимула приносит государству, и в частности, государственной системе здравоохранения.

³² См. (Бородин, Крюкова, 2021). Более сдержанные позиции в науке также представлены в (Panagopoulos & Sideri, 2021).

Заключение

Наследуемое редактирование человеческого генома – технология, которая так или иначе уже существует. Для этого уже создана, если можно так выразиться, материальная часть. Исследования в этом направлении ведутся в России, при этом важно, что не только в ней. Известно, что управление развитием и применением технологии – это всегда процесс. В данном случае регулирование генетического редактирования и соответствующие практики можно сравнить с живым организмом, который уже пора произвести на свет, хотя бы и с тем, чтобы он мог развиваться в дальнейшем.

Дополнительный интерес ситуации придает тот факт, что в данном случае практически любое продвижение в правовом поле требует компетентного обсуждения с основными стейкхолдерами, которое с очевидностью должно строиться по итеративному принципу. Даже принципиальные основы, стартовые точки должны быть сверены с участниками происходящего. Тем более это касается дальнейшего, более детального механизма взаимодействия органов публичной власти, представителей юридической и этической наук, медицинских организаций, осуществляющих ключевой научный функционал в сфере редактирования, пациентов (пациентских организаций) и т. д. Создание и сохранение горизонта обсуждения позволяет, с одной стороны, умерить азарт первооткрывателей, а с другой – не консервировать ситуацию до полного отказа от действий.

Как представляется, такое положение требует функционирования специальных площадок для междисциплинарного обсуждения того, какие именно нормативные и управленческие шаги должны быть предприняты в России для развития технологии; для этих целей мы и представили здесь ряд предложений.

Список литературы

- Балашенко, Н. А. (2016). Информационные технологии в генетике. *Информатизация образования*, 1, 84–94. <https://elibrary.ru/ywwhqo>
- Бородин, С. С., Крюкова, Е. С. (2021). Правовая регламентация стимулирования внедрения генетических технологий в экономический оборот. В кн. А. А. Мохов, О. В. Сушкова (ред.), *Генетические технологии и медицина* (с. 23–24). Москва: Проспект. <https://elibrary.ru/nmxhrw>
- Ворожевич, А. С. (2020). Патентные права на результаты генетических исследований: условия предоставления, допустимые изъятия и ограничения. *Вестник гражданского права*, 2, 176–216. <https://elibrary.ru/gcgapa>
- Троицкая, А. (2022). Правовые ответы на вопросы о редактировании генома человека (с учетом технологии CRISPR-CAS9). *Сравнительное конституционное обозрение*, 5, 11–41. <https://doi.org/10.21128/1812-7126-2022-5-11-41>
- Черкасова, Е. И., Брилкина, А. А. (2015). *Работа с культурами клеток*. Нижний Новгород: ННГУ им. Н. И. Лобачевского.
- Asquer, A., & Morrison, M. (2022). Editorial: Regulation and governance of gene editing technologies (CRISPR, etc.). *Frontiers in Political Sciences*, 4, 1027410. <https://doi.org/10.3389/fpos.2022.1027410>
- Atimango, A. O., Wesana, J., Kalule, S. W., Verbeke, W., & De Steur, H. (2024). Genome editing in food and agriculture: from regulations to consumer perspectives. *Current Opinion in Biotechnology*, 87, 103127. <https://doi.org/10.1016/j.copbio.2024.103127>
- Barnett, S. A. (2017). Regulating Human Germline Modification in Light of CRISPR. *University of Richmond Law Review*, 51, 553–591.
- Baylis, F., Darnovsky, M., Hasson, K., & Krahn, T. M. (2020). Human Germline and Heritable Genome Editing: the Global Policy Landscape. *The CRISPR Journal*, 3(5), 365–377. <https://doi.org/10.1089/crispr.2020.0082>
- Henaghan, M. (2006). *Choosing Genes for Future Children: Regulating Preimplantation Genetic Diagnosis*. Dunedin, N.Z.: Human Genome Research Project.

- Lawford, D. J. (2020). The Regulation of Human Germline Genome Modification in the United Kingdom. In A. Boggio, C. P. R. Romano, J. Almqvist (Eds.), *Human Germline Genome Modification and the Right to Science. A Comparative Study of National Laws and Policies* (pp. 217–240). Cambridge University Press.
- Liang, P., Xu, Y., Zhang, X., Ding C., Huang R., Zhang Z., Lv J., Xie X., Chen Y., Li Y., Sun Y., Bai Y., Songyang Zh., Ma W., Zhou C., Huang J. (2015). CRISPR/Cas9-Mediated Gene Editing in Human Triprenuclear Zygotes. *Protein Cell*, 5(6), 363–372. <https://doi.org/10.1007/s13238-015-0153-5>
- Ledford, H. (2017). CRISPR fixes disease gene in viable human embryos. *Nature*, 548, 13–14. <https://doi.org/10.1038/nature.2017.22382>
- Ma, H., Marti-Gutierrez, N., Park, S. W., ... Mitalipov, Sh. (2017). Correction of a pathogenic gene mutation in human embryos. *Nature*, 548, 413–419. <https://doi.org/10.1038/nature23305>
- McCully, S. (2021). The Time has Come to Extend the 14-Day Limit. *Journal of Medical Ethics*, 7. <https://doi.org/10.1136/medethics-2020-106406>
- Panagopoulos, A., & Sideri, K. (2021). Prospect patents and CRISPR; rivalry and ethical licensing in a semi-commons environment. *Journal of Law and the Biosciences*, 8(2), Isab031. <https://doi.org/10.1093/jlb/Isab031>
- Pombo, M. L. (2011). Biotechnological products in Pan American Health Organization (PAHO): Regional efforts towards harmonization of regulation. *Biologicals*, 39(5), 348. <https://doi.org/10.1016/j.biologicals.2011.06.010>
- Scheinerman, N., & Sherkow, J. (2021). Governance Choices of Genome Editing Patents. *Frontiers in Political Sciences*, 3, 745898. <https://doi.org/10.3389/fpos.2021.745898>
- Sharif, J., Koseki, H., & Parrish, N. F. (2023). Bridging multiple dimensions: roles of transposable elements in higher-order genome regulation. *Current Opinion in Genetics & Development*, 80, 102035. <https://doi.org/10.1016/j.gde.2023.102035>
- Song, L., & Joly, Y. (2021). After He Jianku: China's Biotechnology Regulation Reforms. *Medical Law International*, 21(2). <https://doi.org/10.1177/0968533221993504>
- Tan, J., Shen, M., Chai, N., Liu, Q., Liu, Y., & Zhu, Q. (2023). Genome editing for plant synthetic metabolic engineering and developmental regulation. *Journal of Plant Physiology*, 291, 154141. <https://doi.org/10.1016/j.jplph.2023.154141>
- Wilson, L. (2023). Regulation of biological agents and biotechnology. In *Encyclopedia of Forensic Sciences* (Vol. 4, 3rd Ed., pp. 376–386). Elsevier eBooks. <https://doi.org/10.1016/b978-0-12-823677-2.00232-4>
- Yu, H., Taduri, S., Kesan, J., Lau, G., & Law, K. H. (2012). Mining information across multiple domains: A case study of application to patent laws and regulations in biotechnology. *Government Information Quarterly*, 29, S11–S21. <https://doi.org/10.1016/j.giq.2011.08.013>

Сведения об авторах



Троицкая Александра Алексеевна – доктор юридических наук, доцент, профессор кафедры конституционного и муниципального права, Московский государственный университет имени М. В. Ломоносова

Адрес: 119991, Россия, г. Москва, Ленинские горы, 1, стр. 13

E-mail: stephany@mail.ru

ORCID ID: <https://orcid.org/0000-0002-5025-9905>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=15045938900>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/O-5879-2017>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=629760



Шарловский Константин Александрович – партнер, руководитель практики «Фармацевтика и здравоохранение», ООО «Пепеляев Групп»

Адрес: 125047, Россия, г. Москва, ул. 3-я Тверская-Ямская, 39, стр. 1

E-mail: K.Sharlovskiy@pgplaw.ru

ORCID ID: <https://orcid.org/0000-0003-1091-5338>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/AAH-5173-2019>

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс

Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 2 июня 2024 г.

Дата одобрения после рецензирования – 18 июня 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:342.721:612.6

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

DOI: <https://doi.org/10.21202/jdtl.2024.27>

Human Genome Editing: Managing Technological Risks through Legal Means

Aleksandra A. Troitskaya ✉

Lomonosov Moscow State University, Moscow, Russia

Konstantin A. Sharlovskiy

Pepelyayev Group LLC, Moscow, Russia

Keywords

digital technologies,
genetic editing,
genetic technologies,
human genome,
law,
legal liability,
legislation,
reproductive technologies,
risk-based approach,
technological risk

Abstract

Objective: to determine theoretical approaches to the legal regulation of reprogrammed editing, taking into account the risk-oriented approach and the practice of regulation of such breakthrough technologies in different jurisdictions; to outline further regulatory and managerial steps to be taken for the technology development.

Methods: general scientific methods of analysis and synthesis, classification, system and functional approaches; specific scientific methods: formal-legal, comparative-legal, and historical-legal.

Results: the research shows the possible approaches to the regulation of genetic editing for reproductive purposes. The considered variants are evaluated from the viewpoint of risk-oriented approach; conditions and peculiarities of various regulatory mechanisms' application are determined; the current Russian regulation in this sphere is assessed. The analysis allows concluding that the prohibition or significant restriction of the developing technology of reprogrammed editing has no irrefutable grounds. Moreover, it may lead to the results opposite to those declared by its proponents. In this regard, it is necessary to develop the discussion in a constructive and iterative way and involve all stakeholders in it, including the scientific community.

✉ Corresponding author

© Troitskaya A. A. Sharlovskiy K. A., 2024

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 international practice of legal regulation of reprogenetic technologies within different jurisdictions was generalized and conceptually interpreted; the natural scientific arguments in assessing the implemented regulation effectiveness were analyzed. This not only allows systematically considering the current and hypothetical risks of genetic technologies' development and use, but also provides an opportunity to use a risk-oriented approach to the analysis of legal regulation of genome editing technologies. The next step in comprehending the phenomenon of genetic editing becomes possible.

Practical significance: the study results can be used for building further constructive dialog on applying legal mechanisms to human genome editing. The study can also be a basis for iterative approach in the future discussion.

For citation

Troitskaya, A. A., & Sharlovskiy, K. A. (2024). Human Genome Editing: Managing Technological Risks through Legal Means. *Journal of Digital Technologies and Law*, 2(3), 521–543. <https://doi.org/10.21202/jdtl.2024.27>

References

- Asquer, A., & Morrison, M. (2022). Editorial: Regulation and governance of gene editing technologies (CRISPR, etc.). *Frontiers in Political Sciences*, 4, 1027410. <https://doi.org/10.3389/fpos.2022.1027410>
- Atimango, A. O., Wesana, J., Kalule, S. W., Verbeke, W., & De Steur, H. (2024). Genome editing in food and agriculture: from regulations to consumer perspectives. *Current Opinion in Biotechnology*, 87, 103127. <https://doi.org/10.1016/j.copbio.2024.103127>
- Balashenko, N. A. (2016). Information Technologies in Genetics. *Informatization of Education*, 1, 84–94. (In Russ.).
- Barnett, S. A. (2017). Regulating Human Germline Modification in Light of CRISP. *University of Richmond Law Review*, 51, 553–591.
- Baylis, F., Darnovsky, M., Hasson, K., & Krahn, T. M. (2020). Human Germline and Heritable Genome Editing: the Global Policy Landscape. *The CRISPR Journal*, 3(5), 365–377. <https://doi.org/10.1089/crispr.2020.0082>
- Borodin, S. S., Kryukova, E. S. (2021). Legal regulation of stimulating the introduction of genetic technologies into economic circulation. In A. A. Mokhov, O. V. Sushkova (Eds.), *Genetic research and medicine* (pp. 23–24). Moscow: Prospect. (In Russ.).
- Cherkasova, E. I., Brilkina, A. A. (2015). *Working with cell cultures*. Nizhny Novgorod. (In Russ.).
- Henaghan, M. (2006). *Choosing Genes for Future Children: Regulating Preimplantation Genetic Diagnosis*. Dunedin, N.Z.: Human Genome Research Project.
- Lawford, D. J. (2020). The Regulation of Human Germline Genome Modification in the United Kingdom. In A. Boggio, C. P. R. Romano, J. Almqvist (Eds.), *Human Germline Genome Modification and the Right to Science. A Comparative Study of National Laws and Policies* (pp. 217–240). Cambridge University Press.
- Ledford, H. (2017). CRISPR fixes disease gene in viable human embryos. *Nature*, 548, 13–14. <https://doi.org/10.1038/nature.2017.22382>
- Liang, P., Xu, Y., Zhang, X., Ding C., Huang R., Zhang Z., Lv J., Xie X., Chen Y., Li Y., Sun Y., Bai Y., Songyang Zh., Ma W., Zhou C., Huang J. (2015). CRISPR/Cas9-Mediated Gene Editing in Human Triprounuclear Zygotes. *Protein Cell*, 5(6), 363–372. <https://doi.org/10.1007/s13238-015-0153-5>
- Ma, H., Marti-Gutierrez, N., Park, S. W., ... Mitalipov, Sh. (2017). Correction of a pathogenic gene mutation in human embryos. *Nature*, 548, 413–419. <https://doi.org/10.1038/nature23305>
- McCully, S. (2021). The Time has Come to Extend the 14-Day Limit. *Journal of Medical Ethics*, 7. <https://doi.org/10.1136/medethics-2020-106406>

- Panagopoulos, A., & Sideri, K. (2021). Prospect patents and CRISPR; rivalry and ethical licensing in a semi-commons environment. *Journal of Law and the Biosciences*, 8(2), Isab031. <https://doi.org/10.1093/jlb/Isab031>
- Pombo, M. L. (2011). Biotechnological products in Pan American Health Organization (PAHO): Regional efforts towards harmonization of regulation. *Biologicals*, 39(5), 348. <https://doi.org/10.1016/j.biologicals.2011.06.010>
- Scheinerman, N., & Sherkow, J. (2021). Governance Choices of Genome Editing Patents. *Frontiers in Political Sciences*, 3, 745898. <https://doi.org/10.3389/fpos.2021.745898>
- Sharif, J., Koseki, H., & Parrish, N. F. (2023). Bridging multiple dimensions: roles of transposable elements in higher-order genome regulation. *Current Opinion in Genetics & Development*, 80, 102035. <https://doi.org/10.1016/j.gde.2023.102035>
- Song, L., & Joly, Y. (2021). After He Jianku: China's Biotechnology Regulation Reforms. *Medical Law International*, 21(2). <https://doi.org/10.1177/0968533221993504>
- Tan, J., Shen, M., Chai, N., Liu, Q., Liu, Y., & Zhu, Q. (2023). Genome editing for plant synthetic metabolic engineering and developmental regulation. *Journal of Plant Physiology*, 291, 154141. <https://doi.org/10.1016/j.jplph.2023.154141>
- Troitskaya, A. (2022). Legal answers to questions about editing the human genome (considering CRISPR-Cas9 technology). *Comparative Constitutional Review*, 31(5), 11–41. (In Russ.).
- Vorozhevich, A. S. (2020). Patent rights to the results of genetic research: terms and conditions of acceptance. *Civil Law Review*, 2, 176–216.
- Wilson, L. (2023). Regulation of biological agents and biotechnology. In *Encyclopedia of Forensic Sciences* (Vol. 4, 3rd Ed., pp. 376–386). Elsevier eBooks. <https://doi.org/10.1016/b978-0-12-823677-2.00232-4>
- Yu, H., Taduri, S., Kesan, J., Lau, G., & Law, K. H. (2012). Mining information across multiple domains: A case study of application to patent laws and regulations in biotechnology. *Government Information Quarterly*, 29, S11–S21. <https://doi.org/10.1016/j.giq.2011.08.013>

Authors information



Aleksandra A. Troitskaya – Dr. Sci. (Law), Associate Professor, Professor of the Department of Constitutional and Municipal Law, Lomonosov Moscow State University
Address: 1 Leninskiye Gory, building 13, 119991 Moscow, Russia
E-mail: stephany@mail.ru
ORCID ID: <https://orcid.org/0000-0002-5025-9905>
Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=15045938900>
WoS Researcher ID: <https://www.webofscience.com/wos/author/record/O-5879-2017>
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=629760



Konstantin A. Sharlovskiy – Partner, Head of Life Sciences Practice, Pepelyaev Group LLC
Address: 39 3rd Tverskaya-Yamskaya Str., building 1, 125047 Moscow, Russia
E-mail: K.Sharlovskiy@pgplaw.ru
ORCID ID: <https://orcid.org/0000-0003-1091-5338>
WoS Researcher ID: <https://www.webofscience.com/wos/author/record/AAH-5173-2019>

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – June 2, 2024

Date of approval – June 18, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:349.4:004.8:528

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

DOI: <https://doi.org/10.21202/jdtl.2024.28>

Цифровые технологии в национальной кадастровой системе Узбекистана: проблемы правового регулирования

Робия Собировна Тошбоева

Ташкентский государственный юридический университет, Ташкент, Узбекистан

Ключевые слова

государственный кадастр, искусственный интеллект, кадастровая информация, национальное законодательство, право, правовое регулирование, специальный правовой режим, Узбекистан, цифровые технологии, этика

Аннотация

Цель: проведение критического анализа состояния национального законодательства Узбекистана на предмет правового регулирования цифровизации и использования искусственного интеллекта в кадастровой сфере.

Методы: основу проведенного исследования составляют такие методы научного познания, как формально-юридический и сравнительно-правовой анализ, индукция и дедукция.

Результаты: проанализированы положения, которые регламентируют цифровизацию и применение искусственного интеллекта в кадастровой сфере, выявлены правовые пробелы. Определено, что практическое применение технологий искусственного интеллекта опережает его правовое регулирование. Отмечаются недостатки правового регулирования в указанной сфере (отсутствие легальной дефиниции и определения правового статуса искусственного интеллекта в национальном законодательстве, регламентация участия субъектов предпринимательской деятельности в управлении искусственным интеллектом и др.), что затягивает процесс его полноценного применения и уравнивания наряду с традиционными источниками кадастровой информации. Обоснована необходимость всеобщей оцифровки национального кадастра. Спрогнозирована возможность более широкого применения искусственного интеллекта в природно-ресурсной кадастровой системе. Утверждается, что существующая система в ее текущем состоянии в последующем будет приводить к принятию неправильных решений и появлению кадастровых ошибок, в связи с чем необходимо совершенствование правового регулирования в сфере кадастра.

Научная новизна: впервые представлена оценка итогов оцифровки национального кадастра и даны прогнозы о возможности применения искусственного интеллекта в данной сфере при условии дальнейшего совершенствования правового регулирования, которое имеет принципиальное значение для реформирования кадастровой системы, поскольку технологическая основа указанной системы не в полной мере отвечает потребностям цифровой экономики.

© Тошбоева Р. С., 2024

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 правовой регламентации понятия и правового статуса искусственного интеллекта в национальном законодательстве, а также единого подхода к цифровизации кадастровой системы. Современные технологии активно применяются на практике, однако не имеют под собой достаточной правовой основы. Основные выводы, предложения и рекомендации по теме исследования могут служить основой для дальнейшего совершенствования нормативно-правовой базы Узбекистана в части применения технологий искусственного интеллекта.

Для цитирования

Тошбоева, Р. С. (2024). Цифровые технологии в национальной кадастровой системе Узбекистана: проблемы правового регулирования. *Journal of Digital Technologies and Law*, 2(3), 544–564. <https://doi.org/10.21202/jdtl.2024.28>

Содержание

Введение

1. Состояние правового регулирования
 - 1.1. Состояние национального законодательства
 - 1.2. Международные нормы и их имплементация в законодательство
 - 1.3. Передовая зарубежная практика
2. Узбекский опыт применения искусственного интеллекта
 - 2.1. Нормативно-правовая основа
 - 2.2. Обзор литературы

Заключение

Список литературы

Введение

Кадастровая система Узбекистана включает в себя более 20 видов государственных кадастров, объектами которых являются как природные ресурсы, так и объекты неприродного характера. Данная система содержит огромную базу данных, от достоверности которой зависит ход экономических реформ. Поэтому применение возможностей искусственного интеллекта (далее – ИИ) в работе с кадастровой информацией является одной из актуальных тем отечественной экологической и кадастровой практики.

Анализ международного рейтинга Government Artificial Intelligence Readiness Index («Индекс готовности правительства к искусственному интеллекту»), проводимый Oxford Insights, показывает, что Узбекистан прилагает большие усилия в сфере внедрения технологий искусственного интеллекта. Так, если в 2019 г. среди 160 стран мира Узбекистан занимал 158-е место, то в 2020 г. – 95-е, в 2021 г. – 93-е и в 2022 г. – 79-е место¹. Таким образом, позиция страны в сфере применения искусственного интеллекта за пять лет улучшилась почти в два раза. В большей степени это обусловлено и началом применения искусственного интеллекта в сфере кадастра.

¹ Цифровизация: Узбекистан поднимается вверх в международных рейтингах. (2022, 29 декабря). UZA. <https://click.ru/3CsERN>

Опубликование ЮНЕСКО Рекомендаций об этических аспектах применения искусственного интеллекта в 2021 г., а также принятие Евросоюзом первого в мире Закона «Об искусственном интеллекте» в конце 2023 г. стало импульсом для Узбекистана в дальнейшем совершенствовании нормативно-правовой базы применения технологий искусственного интеллекта (Podshivalov, 2022; Sladić et al., 2020).

Применение искусственного интеллекта в национальном кадастре пока носит фрагментарный характер, что говорит о его латентном уровне. Практическое применение технологий искусственного интеллекта опережает его правовое регулирование и выражается в форме 3D, 4D и 5D компьютерных моделирований.

В плане практических результатов реализации 3D-моделей следует отметить создание 3D-моделей по отдельным видам полезных ископаемых, предусмотренное еще в 2020 г. в рамках кадастра месторождений, проявлений полезных ископаемых и техногенных минеральных образований. Широко практикуется создание 3D-моделей зданий и сооружений (Przewięźlikowska, 2020; Ameyaw & De Vries, 2023).

На основе Административного регламента по оказанию государственной услуги по предоставлению информации об истории недвижимости можно получить справку об истории недвижимости (здания) непосредственно в Центре государственных услуг, либо через Единый портал интерактивных государственных услуг, либо на сайте davreestr.uz, что является первым опытом 4D-кадастра.

Успешно применяется и 5D-моделирование в отношении таких объектов, как промышленные предприятия, котельные, логистические центры, торговые центры и другие сложные имущественные комплексы. В частности, на официальном сайте Агентства по кадастру <https://kadastr.uz/ru/kadastr-qiymatini-hisoblash> предоставляется услуга по вычислению стоимости зданий на основе BIM-модели здания.

Но искусственный интеллект не охватывает все виды государственных кадастров, и его практическое применение не подкреплено правовой регламентацией.

1. Состояние правового регулирования

1.1. Состояние национального законодательства

Вопрос правового регулирования применения искусственного интеллекта в кадастре связан с вопросом регламентации правового статуса искусственного интеллекта в целом.

Что касается общих вопросов правового регулирования применения искусственного интеллекта, то в табл. 1–3 дается анализ основополагающих направлений законодательства. Финансирование национальных проектов с применением искусственного интеллекта осуществляется за счет средств МФО, грантов, средств исполнителей, международных грантов, средств ИПФО и совместных альянсов.

Таблица 1. Состояние нормотворческой деятельности в сфере применения искусственного интеллекта

№	Нормативный акт	Наличие
1	Закон «Об искусственном интеллекте»	Отсутствует
2	Стратегия развития искусственного интеллекта	Отсутствует
3	Государственные стандарты в сфере применения искусственного интеллекта	Отсутствует
4	Кодекс этики использования искусственного интеллекта	Отсутствует
5	Специальный режим использования технологий ИИ	Есть

Таблица 2. Состояние образования в сфере искусственного интеллекта

Высшее специальное образование		Послевузовское обучение	
специальное	юридическое	специальное	юридическое
231 квота для бакалавриата, 14 квот для магистратуры по направлению «Искусственный интеллект» в шести вузах страны	Отсутствует	5 квот для докторантуры и самостоятельных исследователей по направлению «Цифровые технологии и искусственный интеллект»	Отсутствует

Таблица 3. Информация о природных ресурсах, предоставляемая в открытом доступе для реализации проектов в области искусственного интеллекта

Информация	Есть (+) / Нет (-)
О климате и погодных условиях	+
Об объектах растительного мира	-
О водных ресурсах	+
Об объектах животного мира	-
О земельных ресурсах	+
О лесных ресурсах	-
Об охраняемых природных территориях	-
О полезных ископаемых	-

Отмеченное позволяет констатировать, что фундаментальные и концептуальные акты правового регулирования в сфере ИИ еще не приняты, а специальный режим поддержки технологий ИИ имеет временные рамки использования и распространяется лишь на резидентов IT-парков, что, на наш взгляд, ограничивает возможности других субъектов, занимающихся данной сферой.

Организационный аспект управления ограничивается лишь функционированием государственного административного органа и консультационной структурой, при этом участие частного сектора в сфере управления ИИ отсутствует. Если учесть тот факт, что во всем мире основными разработчиками ИИ являются крупнейшие частные компании², то будущее сферы применения ИИ в Узбекистане также будет сосредоточено в руках субъектов предпринимательской деятельности. Следовательно, их участие в управлении ИИ также должно быть регламентировано.

Отсутствует регламентирование преподавания правовых знаний в рамках формирования специальных знаний в сфере ИИ. Несмотря на то, что Ташкентский государственный юридический университет входит в список вузов, в которых внедряются учебные курсы и предметы по прикладному применению технологий искусственного интеллекта в системе государственного управления, целевые показатели по подготовке кадров (бакалавриат, магистратура и докторантура) в сфере применения ИИ не разработаны. Недостаточное внимание развитию общей научной деятельности резко проявляется на фоне практического отсутствия правовой научной деятельности.

² По статистическим данным за 2023 г., крупнейшими IT-компаниями мира стали Google, OpenAI, Microsoft, Huawei, «Яндекс» и др.

Финансирование проектов с ИИ осуществляется преимущественно за счет внебюджетных средств, при этом государственное финансирование присутствует лишь в новом институте – Альянсе, который представляет собой объединение финансов государственных органов и субъектов предпринимательской деятельности.

Ограничен и состав данных о природных ресурсах, которые могут быть использованы в качестве алгоритма данных. Открытые кадастровые данные о земельных и водных ресурсах пока используются в проектах с применением ИИ, тогда как данные о других природных ресурсах отсутствуют.

Анализ общих норм законодательства показывает, что в нем отсутствует регламентация таких понятий, как «3D-участок», «3D-собственность». Вся имеющаяся кадастровая информация связана с 2D-кадастром. Земельный кодекс Республики Узбекистан гласит, что «земельный участок – это часть земельного фонда, имеющая фиксированную границу, площадь, местоположение, правовой режим и другие характеристики, отражаемые в государственном земельном кадастре», при этом понятие «земельный фонд» не определяется, а приводятся лишь его составные части³. Закон «О государственном земельном кадастре» не дает определения земельного участка⁴. Закон «О недрах» определяет недра как часть земной коры, расположенной ниже почвенного слоя, а при его отсутствии – ниже земной поверхности или дна водных объектов, простирающаяся до глубин, доступных для геологического изучения и освоения, а горный отвод – как участок недр, ограниченный по площади и глубине⁵. Такие объекты, как мосты, подземные помещения, стадионы, инженерная коммуникация, туннели, частично урегулированы и являются объектами отдельных кадастров. Гражданский кодекс Республики Узбекистан под недвижимым имуществом подразумевает участки земли, недра, здания, сооружения, многолетние насаждения и иное имущество, прочно связанное с землей, т. е. объекты, перемещение которых без несоразмерного ущерба их назначению невозможно⁶. Но понятие «вертикальная недвижимость» не регламентируется ни в Гражданском, ни в Градостроительном кодексах Республики Узбекистан⁷.

1.2. Международные нормы и их имплементация в законодательство

Основной международной нормой, имплементацию которой в национальное законодательство считаем целесообразной, являются Рекомендации об этических аспектах искусственного интеллекта (далее – Рекомендации), в которых даны основные критерии использования ИИ на сегодняшний день. Разработка этого документа началась еще в 2019 г. и была принята лишь в ноябре 2021 г. Генеральной конференцией ООН по вопросам образования, науки и культуры (ЮНЕСКО). Целью принятия данного документа является урегулирование применения ИИ в мирных целях, направление его для служения во благо человека, общества и окружающей среды (табл. 4).

³ Земельный кодекс Республики Узбекистан. <https://clck.ru/3CsFj2>

⁴ Закон Республики Узбекистан «О государственном земельном кадастре». <https://clck.ru/3CsFjX>

⁵ Закон Республики Узбекистан «О недрах». <https://clck.ru/3CsFkX>

⁶ Гражданский кодекс Республики Узбекистан. <https://clck.ru/3CsFm9>

⁷ Градостроительный кодекс Республики Узбекистан. <https://clck.ru/3CsFms>

Таблица 4. Этические ценности и принципы деятельности искусственного интеллекта, закрепленные в Рекомендациях об этических аспектах ИИ

Ценностные установки	Принципы деятельности
– Уважение, защита и поощрение прав человека и основных свобод и человеческого достоинства; – благополучие окружающей среды и экосистем; – обеспечение разнообразия и инклюзивности; – жизнь в мирных, справедливых и взаимосвязанных обществах	– Соразмерность и непричинение вреда; – безопасность и защищенность; – справедливость и отказ от дискриминации; – устойчивость; – право на неприкосновенность частной жизни и защита данных; – подконтрольность и подчинение человеку; – прозрачность и объяснимость; – ответственность и подотчетность; – осведомленность и грамотность; – многостороннее и адаптивное управление и взаимодействие

Приведенные установки и принципы в целом соответствуют основополагающим принципам национального кадастрового законодательства.

Несмотря на то, что данный акт называется Рекомендациями об этических аспектах искусственного интеллекта, в нем содержатся и юридические рекомендации, которые до принятия отдельного закона могут заменить правовые нормы регулирования использования ИИ в странах, имплементировавших его.

В частности, рекомендации относительно юридической ответственности, выделение сфер, в которых можно и нельзя применять искусственный интеллект, обязательная подконтрольность искусственного интеллекта человеку и др.

Использование ИИ в сфере окружающей среды и экосистем, составной частью которой являются кадастры природных ресурсов, относится к области, требующей принятия стратегических мер по применению искусственного интеллекта, рекомендуемой ООН.

Нормы, непосредственно регулирующие применение ИИ в сфере кадастра, в национальном законодательстве отсутствуют.

Сопоставляя вышеприведенные нормы с положениями Рекомендаций, мы выявили, что в них отсутствуют некоторые фундаментальные требования (табл. 5).

Таблица 5. Последствия, связанные с недостатками правового регулирования

Отсутствующие нормы	Чем чревато
Не регламентируются понятия «искусственный интеллект» и «жизненный цикл искусственного интеллекта»	Отождествление искусственного интеллекта с традиционными объектами правоотношений
Минимизация возможных негативных последствий применения ИИ	Полученный положительный результат обесценивается, создается угроза для окружающих
Контроль деятельности ИИ на протяжении всего жизненного цикла, в том числе и общественный контроль	Тотальное господство машин над человеком
Пределы ответственности человека при применении ИИ	Нарушение прав и интересов человека при использовании ИИ останется ненаказуемым
Гарантия интересов маргинализированных групп населения, исходя из цифрового неравенства на внутригосударственном уровне	Создаст ограниченный круг субъектов пользования ИИ
Механизм возмещения вреда, причиненного применением ИИ-технологий	Право на возмещение материального и морального ущерба не будет реализовано
Система мягкого управления в сфере применения ИИ	Отсутствие единых требований при регламентировании деятельности разработчиков ИИ
ИИ не могут иметь статус юридического лица	Предъявление претензий к ИИ как самостоятельному субъекту права в качестве субъекта частного и публичного права

Итак, приведенный анализ показывает, что основополагающие принципы и установки в сфере применения технологий ИИ в кадастровом законодательстве Узбекистана на сегодняшний день регламентированы частично. Следует отметить, что некоторые положения Рекомендаций уже действуют в изучаемой сфере законодательства.

В частности, установление прозрачной системы согласования с частными юридическими лицами, имеющими общественно значимую информацию. Такая система есть в Законе «Об экологическом аудите»⁸, согласно которому выводы по экологическому аудиту не разглашаются без согласия заказчика.

1.3. Передовая зарубежная практика

Исходя из зарубежной практики правового регулирования применения искусственного интеллекта в кадастре, можно выделить следующие тенденции использования 3D-кадастра:

- наличие отдельного закона, регулирующего применение 3D-кадастра. Например, в Китае действует отдельный закон о 3D-кадастре, который наряду с земельными участками, находящимися в исключительной государственной собственности, регистрирует здания и сооружения;

- отсутствие отдельного закона, при этом внесение в действующее законодательство изменений и дополнений, регулирующих правовой статус 3D-кадастров. К таким странам относятся Австралия (Квисленд), Венгрия, Швеция, Нидерланды, Польша, Турция и др. Эта система является очень гибкой, так как в ее основе лежит использование границ земельных участков в рамках двухмерного кадастра для формирования информации по объекту 3D-кадастра. Вместе с тем есть и свои недостатки этой системы. Так, при формировании информации об одном объекте в рамках 3D-кадастра используется информация о нескольких земельных участках в рамках 2D-кадастра. Данная практика может дать сбой в будущем, когда встанет вопрос юридического признания 3D-кадастров;

- недопуск к использованию 3D-кадастра нормами действующего законодательства, несмотря на широкое применение на практике. В Греции и на Кипре применение 3D-кадастра противоречит Гражданскому кодексу.

Родиной внедрения искусственного интеллекта в сфере кадастра является Австралия. В 1997 г. она одной из первых в мире внедрила 3D-моделирование в сфере кадастра недвижимости. Поэтому информация 3D-кадастра имеют равную силу наравне с 2D- и 4D-кадастровыми информациями. Бумажная кадастровая информация действует параллельно с электронной, при этом первая отличается слишком большим объемом деталей, тогда как 3D представляет собой простое графическое изображение. Таким образом, бумажная и цифровая кадастровая информация как бы дополняют друг друга. Все виды прав собственности можно зарегистрировать как в 3D-, так и в 2D-кадастрах. Кроме того, отдельно выделяют объекты трехмерного моделирования: мосты, подземные помещения, парковки, сервитуты, договоры аренды, инженерные сети, трубопроводы, стадионы и др. 3D-участок может быть

⁸ Закон Республики Узбекистан «Об экологическом аудите». <https://clck.ru/3CsGZk>

объектом залога, как и обычный участок, несмотря на то, что 3D-кадастровая информация не является последней истиной в кадастре.

Законодательство Аргентины не регламентирует правовой статус 3D-кадастра, несмотря на его широкое применение в практике. В Австрии при всем стремлении полностью перейти на 3D-кадастр цифровизация кадастра полностью не выполнена. В Болгарии наблюдается частичное применение 3D-моделирования, так, если в Софии трехмерный кадастр считается необходимым, в других городах страны он не является основным источником информации. При этом в законодательстве не регламентируется его правовой статус. Канадский кадастр отличается ежедневным обновлением кадастровых карт, книг, отчетов, хотя по сути является многоцелевым кадастром, при этом нет отдельного закона о 3D-кадастре, но объекты трехмерного кадастра отдельно регламентированы.

2. Узбекский опыт применения искусственного интеллекта

2.1. Нормативно-правовая основа

Отсутствие закона об использовании искусственного интеллекта в Узбекистане восполняется ограниченным правовым регулированием – Специальным режимом поддержки технологий искусственного интеллекта и порядка его деятельности, под которым подразумевается порядок правового регулирования осуществления испытательных работ, основанных на технологии искусственного интеллекта, создание организационно-правовых условий для юридических лиц и научных организаций, создание благоприятных условий в правовых отношениях в ходе осуществления деятельности, связанной с разработкой программных обеспечений и оказания услуг, проведения апробации программных обеспечений и их внедрения в рамках «умного» регулирования⁹. Данный режим является отдельным звеном Технологического парка программных продуктов и информационных технологий.

Рабочим органом Специального режима является Министерство развития информационных технологий и коммуникаций Республики Узбекистан. К задачам рабочего органа относятся следующие:

- утверждает форму заявления и перечень необходимых сведений, представляемых претендентами на получение статуса участника специального режима, и организует прием заявлений;
- утверждает устав Экспертного совета специального режима, а также форму соглашения об условиях деятельности, заключаемого с его участниками;
- формирует и утверждает состав Экспертного совета специального режима совместно с заинтересованными министерствами и ведомствами;
- вносит на рассмотрение Координационной комиссии предложения о включении и исключении преступников из специального режима;
- привлекает сотрудников научно-исследовательского института развития цифровых технологий и искусственного интеллекта для контроля за научной деятельностью участников особого режима;
- обеспечивает организационную, юридическую и консультативную поддержку в период реализации пилотных проектов участников особого режима;

⁹ Жилищный кодекс Республики Узбекистан. <https://clck.ru/3CsGch>

- на основании заключения Координационной комиссии принимает решение о предоставлении, отказе в предоставлении или лишении инициаторов проекта статуса участника особого режима;

- представляет ежегодный официальный отчет соответствующим министерствам и ведомствам об успешно реализованных участниками особого режима проектах.

В Узбекистане ведется специальный Единый реестр участников специального режима, в котором содержится общедоступная и открытая информация о юридических лицах и научных организациях, являющихся участниками специального режима, – резидентах IT-парков. Чтобы стать участником специального режима, следует подать заявку в Координационную комиссию.

Правовой статус участников специального режима весьма специфичен, так как Положением регулируются лишь их обязанности. А права участников закрепляются в двустороннем договоре между Координационной комиссией и участником. Положением предоставлены большие преференции и льготы участникам специального режима. В частности, компенсируются средства, потраченные на повышение квалификации и переподготовку кадров, предоставлено право получать информацию и документы, необходимые для реализации пилотных проектов (за исключением сведений, содержащих государственную тайну и иную охраняемую законом конфиденциальную информацию), а также персональную информацию от министерств, ведомств и организаций, перечень документов, необходимых для получения соответствующих документов разрешительного характера, сокращается соответствующим уполномоченным государственным органом, а также размер платы, установленной за получение соответствующих документов разрешительного характера, снижается в два раза, устанавливается минимум требований и условий осуществления деятельности со стороны компетентного государственного органа.

Вместе с тем Положение закрепляет семь оснований лишения статуса участника специального режима (например, невыполнение договорных отношений с рабочим органом, признание юридического лица банкротом, предоставление недостоверной информации, несоответствие деятельности участника особого режима видам деятельности, указанным в проекте). При этом данный перечень не исчерпывающий, законодатель оставляет и иные основания, предусмотренные законом.

Вместе с тем данный документ нельзя назвать идеальным, так как он содержит ряд положений, противоречащих законодательству:

- во-первых, отказ в регистрации участника специального режима в случае наличия налогов и других обязательных платежей противоречит законодательству о предпринимательской деятельности;

- во-вторых, отсутствие окончательного перечня оснований лишения статуса участника специального режима порождает фундамент для коррупции;

- в-третьих, функционирование режима выдачи заключений по вопросу о получении статуса участника специального режима является непрозрачным.

2.2. Обзор литературы

В научной литературе отсутствует единый подход к определению ИИ. Так, ученые С. Гулямов, И. Рустамбеков определяют ИИ как большое направление научных и прикладных исследований¹⁰.

Андреас Каплан и Майкл Хенлейн пишут, что искусственный интеллект – это «способность системы правильно интерпретировать внешние данные, извлекать уроки из таких данных и использовать полученные знания для достижения конкретных целей и задач при помощи гибкой адаптации» (Kaplan & Haenlein, 2019).

Элейн Рич и Кевин Кнайт определяют ИИ как вид науки, которая учит компьютеры выполнять функции людей, дающие им превосходство над ними (Rich & Knight, 1991). Ронал Чандра и Йога Прихастомо выделяют ИИ как вид интеллектуальных компьютерных программ (Chandra & Prihastomo, 2012).

Важной частью вопроса использования искусственного интеллекта является проблема ответственности. В этом отношении интересным представляется позиция отечественного исследователя С. С. Бозарова, который, рассмотрев такие подходы к установлению юридической ответственности в отношении искусственного интеллекта, как приравнивание объектов искусственного интеллекта к юридическим лицам либо объектам повышенной общественной опасности, в качестве решения предлагает необходимость установления вещных (ограниченных) прав на ИИ¹¹.

Учеными стран ЕС вопросы применения искусственного интеллекта в 3D- и 4D-кадастрах изучены достаточно всесторонне. В частности, И. Вильямсон обосновал необходимость перехода к трехмерному кадастру (Williamson, 1997), С. Хендрайтингсин с соавторами предлагают гибридный вариант трехмерного кадастра, сочетающего основные положения двухмерного кадастра с трехмерным моделированием (Hendriatiningsih et al., 2007), Мохамед Эл-Мекей с соавторами выделяют основные преимущества 3D-кадастра (El Mekawy et al., 2014) и др.

Отдельным вопросом является изучение правового регулирования использования данных 3D-кадастра как объекта искусственного интеллекта. Учитывая наличие разной практики, единого подхода в этом вопросе нет до сих пор.

В частности, первая группа ученых предлагает урегулировать использование ИИ в форме концепции объекта 3D-кадастра, отдельного нормативного акта, а также в форме систематизации норм, связанных с применением ИИ (Stoter & Zevenbergen, 2001; Karki et al., 2011).

Вторая группа выдвигает идею ограничительного регулирования (Sandberg, 2001; Stoter & Ploeger, 2003; Tan & Hussin, 2012), четвертая группа ученых рассматривает правовой статус 3D-кадастра как результат взаимодействия публичного и частного права (Navratil, 2012), пятая группа ученых выдвигает позицию общего права собственности (Paulsson, 2012) и др.

Самые яркие сторонники правового регулирования использования 3D-кадастра – П. Ван Остером, Ж. Стотер, Х. Пложер, Р. Томпсон и С. Карки – обосновывают предложение о необходимости признания 3D-кадастра в виде

¹⁰ Гулямов, С., Рустамбеков, И. (2021, 2 марта). Искусственный интеллект – современное требование в развитии общества и государства. Правда Востока, 43(29547).

¹¹ Бозаров, С. С. (2023). Правовая ответственность в рамках искусственного интеллекта: автореф. дис. ... д-ра филос. наук. Ташкент: ТГЮУ.

самостоятельного правомочия наравне с такими правомочиями, как владеть, пользоваться и распоряжаться (Van Oosterom et al., 2011).

Фатих Донер с соавторами рассматривают проблемы регистрации инженерных сетей в кадастре в четырехмерном измерении на примере законодательства трех стран с точки зрения правовых, организационных и технических кадастровых требований на основе прототипа из Нидерландов и обосновывают его перспективность (Doñnera et al., 2011).

Петер Ван Остероом с соавторами, обосновывая преимущества 4D-кадастра на австралийском и нидерландском опыте, анализируют юридические аспекты регистрации временных прав собственности на землю в рамках *Eigendom*, *droit de propriété* а также гарантии их безопасности, последствия продажи недвижимости одновременно нескольким лицам, действия временной шкалы объекта кадастра таймшеров на основе требований Кодекса Квисленда (Van Oosterom et al., 2006).

Преимущества искусственного интеллекта перед традиционными технологиями в сфере кадастра не требуют доказательств, они налицо.

Современный этап экономических реформ диктует необходимость перехода к использованию более сложных систем ИИ (например, нейронных сетей) в национальном кадастре по той причине, что функционируемая отечественная 2D кадастровая модель не отвечает потребностям цифровой зеленой экономики, которая формируется в Узбекистане.

К факторам, способствующим использованию искусственного интеллекта в кадастрах, относятся:

- современные национальные кадастры природных ресурсов – представляют собой географические информационные системы благодаря полноценному применению ГИС-технологий. На их основе создана электронная карта земельных участков;

- в 2017 г. Узбекистан перешел на международные стандарты в сфере геодезии – Единую систему пространственных данных (WGS-84), которая представляет собой привязанную к Земле глобальную опорную систему, включая модель Земли, и определяется набором основных и вспомогательных параметров. Ранее Узбекистан использовал Систему координат 1942 г. (СК-42), доставшуюся нам от социалистической системы хозяйствования, которая позволяет получать данные об объектах с погрешностью в 2 см;

- в стране идет интенсивный рост урбанизации, включающий расширение городских территорий со сложной инфраструктурой, строительством высотных зданий и подземных объектов (туннелей, подземных сетей и объектов инфраструктуры), плотными застройками со сложными структурами и точечными застройками. Все это происходит на фоне ограниченности земель населенных пунктов и роста демографических процессов, усиливающих спрос на недвижимость. частности, ст. 42 Жилищного кодекса Республики Узбекистан установила социальную норму жилья на одного человека не ниже 16 кв. метров, а для инвалидов на креслах-колясках – не менее 23 кв. метров¹². По прогнозам, население страны до 2030 г. вырастет до 40 млн¹³, тогда как в настоящее время этот показатель составляет около

¹² В ближайшие годы численность населения Узбекистана достигнет 40 млн человек. (2023, 9 ноября). Daryo. <https://clck.ru/3CsGsn>

¹³ Определены задачи по эффективному использованию земельных ресурсов. (2023, 21 ноября). Официальный сайт Президента Республики Узбекистан. <https://clck.ru/3CsGxD>

37 млн человек. Это означает, что потребность в жилье будет расти, следовательно, будут задействованы земельные участки других категорий путем их изменения, что в свою очередь будет влиять на достоверность всего земельного фонда.

Вместе с тем можно выделить ряд факторов, которые значительно тормозят внедрение технологий искусственного интеллекта. Остановимся на некоторых из них.

Во-первых, неполное формирование кадастров природных ресурсов. В частности, в 2023 г. не определен правовой статус 460 тысяч гектаров земель, более 900 тысяч гектаров земель сельскохозяйственного назначения, а также земель вдоль каналов и коллекторов, у естественных озер и рек, которые не вошли в кадастр¹⁴. Учитывая, что искусственный интеллект обрабатывает те алгоритмы данных, которые были заданы человеком, при неполных алгоритмах подготовленный контент тоже будет неполным. Следовательно, результат, представленный искусственным интеллектом, будет недостоверным. Возникает вопрос целесообразности применения искусственного интеллекта в таких условиях. Именно поэтому полнота кадастра должна быть основным условием применения искусственного интеллекта.

Во-вторых, старая технологическая база, не отвечающая потребностям цифровой экономики. В то время как по всему миру идет тенденция отказа от кадастрового картографирования, мы все еще используем такие технологии сбора кадастровой информации, как топографико-геодезические, картографические, почвоведческие, агрохимические и геоботанические исследования. Узбекистан до сих пор не имеет свой спутник космического наблюдения, а ограничивается арендой иностранных. Основные сдвиги в этом направлении начались в 2023 г., в частности, были закуплены дроны Matrice 600, различное программное обеспечение, а также выделены средства на обновление имеющихся дронов, куплены самолеты для аэрофотосъемок, а в текущем году запланирована покупка 80 станций спутникового наблюдения. Но этого недостаточно для формирования полного и достоверного кадастра.

В-третьих, Узбекистан не участвовал в кадастровом проекте Cadastr-2014 и не участвует в проекте Cadastr-2034, в которых напрямую предусмотрено применение искусственного интеллекта ИИ в сфере кадастра в форме 3D- и 4D-кадастра.

В-четвертых, неурегулированность механизма формирования правовых знаний в сфере технологий искусственного интеллекта. На сегодняшний день в пяти высших учебных заведениях страны (Ташкентском университете информационных технологий имени Мухаммада ал-Хоразми, Национальном университете Узбекистана имени Мирзо Улугбека, Ташкентском государственном техническом университете имени Ислама Каримова, Самаркандском государственном университете имени Шарафа Рашидова, Научно-исследовательском институте развития цифровых технологий и искусственного интеллекта) готовят специалистов по направлению «Искусственный интеллект», но вопрос подготовки специалистов в сфере правового регулирования применения искусственного интеллекта пока не рассматривается. При этом Ташкентский государственный юридический университет, являющийся базовым в сфере юриспруденции учебным заведением, входит в перечень заведений, в которых преподаются дисциплины в сфере применения

¹⁴ Постановление Президента Республики Узбекистан № ПП-4996 от 17.02. 2021. <https://clck.ru/3CsGzX>

искусственного интеллекта ИИ в сфере государственного управления¹⁵, при этом подготовка специалистов в сфере правового регулирования применения искусственного интеллекта еще не налажена.

В-пятых, неудовлетворительное состояние научной деятельности. На сегодняшний день в стране нет научного исследования в сфере правового регулирования деятельности с использованием ИИ в кадастровой сфере. Узбекистан на сегодняшний день не относится к странам с высоким уровнем развития технологий искусственного интеллекта, вместе с тем применение искусственного интеллекта довольно востребовано в сфере кадастра. Это, в свою очередь, требует активного и глубокого исследования правовых проблем регулирования применения ИИ в кадастре параллельно с подготовкой специалистов.

В-шестых, пассивное участие государства в финансировании проектов в сфере применения ИИ. На сегодняшний день финансирование проектов с ИИ осуществляется в основном за счет негосударственных средств (средств разработчика), либо в форме объединения капитала крупных государственных субъектов предпринимательской деятельности с бизнесом (Альянс).

В-седьмых, отсутствие имплементации международных стандартов в сферу. Основополагающий акт – Рекомендации ЮНЕСКО об этических аспектах применения искусственного интеллекта, принятые в 2021 г. – до сих пор не имплементирован.

На наш взгляд, использование искусственного интеллекта в сфере кадастра поможет решить ряд накопившихся проблем.

Во-первых, позволит поднять национальный кадастр на международный уровень. Во всех развитых, а также во многих развивающихся странах кадастр является основным источником информации при обеспечении неприкосновенности частной собственности.

Во-вторых, повысит престиж кадастра как основного достоверного юридического источника гарантий права собственности на недвижимость. В зарубежных странах престиж кадастра высок за счет его достоверности и точности, чего нельзя сказать про национальный, который даже на пороге второй четверти XXI в. не является полностью сформированным.

В-третьих, значительно уменьшит уровень коррупции и возможности допущения «кадастровых» ошибок в силу исключения человеческого фактора при формировании и предоставлении кадастровой информации.

В-четвертых, позволит значительно сократить время принятия решений. Внедрение технологий ИИ позволит быстро и качественно обрабатывать и обновлять большие кадастровые данные, что даст возможность получать и изменять информацию в онлайн-режиме. Кроме того, это позволит избежать необоснованных затрат на неэффективные технические средства сбора и обработки кадастровой информации и значительно сократит время формирования нужного контента.

Таким образом, внедрение искусственного интеллекта в сферу кадастра будет способствовать получению достоверных данных и результатов при наличии полной и достоверной информационной базы и будет способствовать повышению престижа кадастра.

¹⁵ Конституция Республики Узбекистан. <https://clck.ru/3CsH5i>

Заключение

Применение искусственного интеллекта как очередной этап автоматизации информации можно представить как будущее всей национальной кадастровой системы.

На повестке дня в Узбекистане стоит вопрос разработки Стратегии развития искусственного интеллекта, которая должна была быть принята еще в 2022 г. Данный акт должен содержать государственную программу поддержки научных исследований и инновационных проектов в области искусственного интеллекта, формирования большого объема цифровых данных на государственном языке, создания современной высокотехнологической инфраструктуры и аппаратных комплексов для решения задач искусственного интеллекта, подготовки кадров, а также совершенствования системы контроля и предотвращения рисков в сфере искусственного интеллекта.

Вместе с тем считаем целесообразным включить в данный документ такие вопросы, как:

1. Основные теоретические понятия (в том числе понятия «искусственный интеллект», «жизненный цикл искусственного интеллекта» и «разработчик искусственного интеллекта»).

2. Правовой статус искусственного интеллекта. На сегодняшний день, на наш взгляд, еще рано говорить об искусственном интеллекте как самостоятельном объекте или субъекте национального права. Целесообразно рассматривать совместную ответственность разработчика искусственного интеллекта и владельца алгоритмов.

3. Обязательность лицензирования деятельности с применением искусственного интеллекта. В настоящее время Координационная комиссия¹⁶ дает заключение по итогам изучения предоставленных документов претендентов в участники IT-парка.

4. Разработка системы этических принципов применения ИИ в соответствии с международными и конституционными нормами.

5. Законодательное закрепление определенного лимита обязательной финансовой государственной поддержки применения ИИ в сфере кадастра. Прямое финансирование из государственного бюджета данной сферы, на наш взгляд, четко выразило бы непосредственную заинтересованность государства в широком применении ИИ. В настоящее время государство поддерживает данную сферу путем предоставления льгот и преференций, бесплатного пользования зданиями, компенсаций затрат на подготовку кадров и др.

6. Предлагается включить в формируемый список зарубежных научно-исследовательских и высших образовательных учреждений в сфере кадастра Мельбурнский университет (Австралия), который является передовым вузом в мире в сфере изучения вопросов правового регулирования внедрения 3D-, 4D- и 5D-кадастров в сфере кадастра.

7. Предлагается рассмотреть вопрос присоединения Узбекистана к глобальному проекту Cadastr-2034. Это позволит сформировать системный подход при использовании ИИ путем формирования 3D-, 4D- и 5D-кадастров.

Искусственный интеллект для национального кадастра необходим как воздух. В настоящее время мы видим попытки приспособления старого кадастра

¹⁶ Координационная комиссия по реализации стратегии «Цифровой Узбекистан – 2030», утвержденной Указом Президента Республики Узбекистан № ПФ-6079 от 5 октября 2020 г.

к потребностям новой экономики – цифровой зеленой экономики, которая нуждается в достоверной информации о состоянии природных ресурсов. Реформирование управления национальным кадастром, выразившееся в создании специального органа – Агентства по кадастру, – стало поворотным моментом для национального кадастра в плане обновления технологической базы кадастровой деятельности. В Узбекистане уже сформирована определенная база для применения искусственного интеллекта, проявляющаяся в функционировании географических информационных систем, цифровых электронных карт и также систем по оценке объектов кадастра. Перспективной для национального кадастра сферой является использование искусственного интеллекта при регистрации прав на недвижимость, а также при распознавании документов. Тем не менее практическое применение искусственного интеллекта в кадастре опережает его правовую регламентацию, что порождает неясности в признании его в качестве официального источника кадастровой информации.

Список литературы

- Ameyaw, P. D., & De Vries, W. T. (2023). Blockchain technology adaptation for land administration services: The importance of socio-cultural elements. *Land Use Policy*, 125, 106485. <https://doi.org/10.1016/j.landusepol.2022.106485>
- Chandra, R., & Prihastomo, Y. (2012). *Artificial Intelligence Definition: A Review*. <https://doi.org/10.22541/au.164670471.11415616/v1>
- Doñnera, F., Thompson, R., Stoter, J., Lemmenc, Ch., Ploeger, H., van Oosterom, P., & Zlatanova, S. (2011). Solutions for 4D cadastre – with a case study on utility networks. *International Journal of Geographical Information Science*, 25(7), 1173–1189. <https://doi.org/10.1080/13658816.2010.520272>
- El Mekawy, M., Paasch, J., & Paulsson, J. (2014). Integration of 3D Cadastre, 3D Property Formation and BIM in Sweden. In *4th International Workshop on 3D Cadastres*, Dubai, United Arab Emirates (pp. 17–34).
- Hendriatiningsih, S., Soemarto, I., Laksono, B. E., Kurniawan, I., Dewi, N. K., & Soegito, N. (2007). Identification of 3-Dimensional Cadastre Model for Indonesian Purpose. In *Strategic Integration of Surveying Services FIG Working Week 2007*, Hong Kong SAR, China.
- 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>
- Karki, S., Thompson, R., McDougall, K., Cumerford, N., & van Oosterom, P. (2011). ISO land administration domain model and LandXML in the development of digital survey plan lodgement for 3D cadastre in Australia. In *Proceedings of the 2nd International Workshop on 3D Cadastres*, Delft, the Netherlands (pp. 65–84).
- Navratil, G. (2012). Combining 3D cadastre and public law – an Austrian perspective. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 61–72).
- Paulsson, J. (2012). Swedish 3D property in an international comparison. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 23–40).
- Podshivalov, T. P. (2022). Improving implementation of the Blockchain technology in real estate registration. *Journal of High Technology Management Research*, 33(2), 100440. <https://doi.org/10.1016/j.hitech.2022.100440>
- Przewiężlikowska, A. (2020). Legal aspects of synchronising data on real property location in polish cadastre and land and mortgage register. *Land Use Policy*, 95, 104606. <https://doi.org/10.1016/j.landusepol.2020.104606>
- Rich, E., & Knight, K. (1991). *Artificial Intelligence*. New York: McGraw-Hill.
- Sandberg, H. (2001). Three-dimensional division and registration of title to land: Legal aspects. In *Proceedings of the International Workshop on 3D Cadastres*, 2001, Delft (pp. 201–209).
- Sladić, D., Radulović, A., & Govedarica, M. (2020). Development of process model for Serbian cadastre. *Land Use Policy*, 98, 104273. <https://doi.org/10.1016/j.landusepol.2019.104273>
- Stoter, J., & Ploeger, H. (2003). Registration of 3D objects crossing parcel boundaries. In *Proceedings of 2003 FIG Working Week, Paris, France*, April 13–17, 2003.
- Stoter, J., & Zevenbergen, J. (2001). Changes in the definition of property: A consideration for a 3D cadastral registration system. In *Proceedings of the FIG Working Week*, Seoul.

- Tan, L. C., & Hussin, K. B. (2012). Establishing 3D Property Rights in Malaysia. In *Proceedings of the 2012 FIG Working Week, Knowing To Manage The Territory, Protect The Environment, Evaluate The Cultural Heritage*, Rome, Italy, 6–10 May 2012 (pp. 1–24).
- Van Oosterom, P., Ploeger, H., Stoter, J., Thompson, R., & Lemmen, Ch. (2006). Aspects of a 4D Cadaster: a first exploration. In *XXIII FIG Congress*, Munich, Germany.
- Van Oosterom, P., Stoter, J., Ploeger, H., Thompson, R., & Karki, S. (2011). World-wide inventory of the status of 3D Cadastres in 2010 and expectations for 2014. In *Proceedings of the 2011 FIG Working Week, Bridging the Gap between Cultures*, Marrakech, Morocco.
- Williamson, I. P., (1997). Strategic Management of Cadastral Reform – Institutional Issues. In *FIG Commission 7 Symposium on Cadastral Systems in Developing Countries*, Penang, Malaysia.

Сведения об авторе



Тошбоева Робия Собировна – доктор юридических наук, доцент, доцент кафедры бизнес-права, Ташкентский государственный юридический университет

Адрес: 100047, Узбекистан, г. Ташкент, ул. Сайилгох, 35

E-mail: robiyatoshboeva@gmail.com

ORCID ID: <https://orcid.org/0000-0003-2898-2109>

Google Scholar ID: <https://scholar.google.com/citations?user=OXu7SxQAAAAJ>

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран

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

История статьи

Дата поступления – 14 апреля 2024 г.

Дата одобрения после рецензирования – 25 апреля 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:349.4:004.8:528

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

DOI: <https://doi.org/10.21202/jdtl.2024.28>

Digital Technologies in the National Cadastre System of Uzbekistan: Issues of Legal Regulation

Robiya S. Toshboyeva

Tashkent State University of Law, Tashkent, Uzbekistan

Keywords

artificial intelligence,
cadastre information,
digital technologies,
ethics,
law,
legal regulation,
national legislation,
special legal regime,
state cadastre,
Uzbekistan

Abstract

Objective: to critically analyze the state of national legislation of Uzbekistan in terms of legal regulation of digitalization and the use of artificial intelligence in the cadastral sphere.

Methods: the research is based on such methods of scientific cognition as formal-legal and comparative-legal analysis, induction and deduction.

Results: the provisions that regulate digitalization and the use of artificial intelligence in the cadastral sphere were analyzed, legal gaps were identified. It was determined that the practical application of artificial intelligence technologies outpaces its legal regulation. The shortcomings of legal regulation in this sphere were noted (lacking legal definition of the legal status of artificial intelligence in the national legislation; regulation of business entities' participation in the management of artificial intelligence, etc.). The said shortcomings hinder its full application and harmonization with traditional sources of cadastral information. The author substantiated the need for universal digitization of the national cadastre and predicts the possibility of wider application of artificial intelligence in the natural-resource cadastral system. It is argued that the existing system in its current state may lead to wrong decisions and cadastral errors, hence, it is necessary to improve the legal regulation of cadastre.

Scientific novelty: for the first time the results of the national cadastre digitization were assessed. Forecasts were given about the possibility of using artificial intelligence in this area, subject to further improvement of legal regulation. The latter is fundamentally important for reforming the cadastral system, since the technological basis of this system does not fully meet the needs of the digital economy.

© Toshboyeva R. S., 2024

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: it is due to the lack of legal regulation of the artificial intelligence concept and legal status in the national legislation, as well as a unified approach to the cadastral system digitalization. Modern technologies are actively used in practice, but lack a sufficient legal basis. The main conclusions, proposals and recommendations of the study can be a basis for further improvement of the legal framework of Uzbekistan in terms of the application of artificial intelligence technologies.

For citation

Toshboyeva, R. S. (2024). Digital technologies in the national cadastre system of Uzbekistan: issues of legal regulation. *Journal of Digital Technologies and Law*, 2(3), 544–564. <https://doi.org/10.21202/jdtl.2024.28>

References

- Ameyaw, P. D., & De Vries, W. T. (2023). Blockchain technology adaptation for land administration services: The importance of socio-cultural elements. *Land Use Policy*, 125, 106485. <https://doi.org/10.1016/j.landusepol.2022.106485>
- Chandra, R., & Prihastomo, Y. (2012). *Artificial Intelligence Definition: A Review*. <https://doi.org/10.22541/au.164670471.11415616/v1>
- Doñnera, F., Thompson, R., Stoter, J., Lemmenc, Ch., Ploeger, H., van Oosterom, P., & Zlatanova, S. (2011). Solutions for 4D cadastre – with a case study on utility networks. *International Journal of Geographical Information Science*, 25(7), 1173–1189. <https://doi.org/10.1080/13658816.2010.520272>
- El Mekawy, M., Paasch, J., & Paulsson, J. (2014). Integration of 3D Cadastre, 3D Property Formation and BIM in Sweden. In *4th International Workshop on 3D Cadastres*, Dubai, United Arab Emirates (pp. 17–34).
- Hendriatiningsih, S., Soemarto, I., Laksono, B. E., Kurniawan, I., Dewi, N. K., & Soegito, N. (2007). Identification of 3-Dimensional Cadastre Model for Indonesian Purpose. In *Strategic Integration of Surveying Services FIG Working Week 2007*, Hong Kong SAR, China.
- 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>
- Karki, S., Thompson, R., McDougall, K., Cumerford, N., & van Oosterom, P. (2011). ISO land administration domain model and LandXML in the development of digital survey plan lodgement for 3D cadastre in Australia. In *Proceedings of the 2nd International Workshop on 3D Cadastres*, Delft, the Netherlands (pp. 65–84).
- Navratil, G. (2012). Combining 3D cadastre and public law – an Austrian perspective. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 61–72).
- Paulsson, J. (2012). Swedish 3D property in an international comparison. In *3rd International Workshop on 3D Cadastres: Developments and Practices*, 25–26 October 2012, Shenzhen, China (pp. 23–40).
- Podshivalov, T. P. (2022). Improving implementation of the Blockchain technology in real estate registration. *Journal of High Technology Management Research*, 33(2), 100440. <https://doi.org/10.1016/j.hitech.2022.100440>
- Przewiężlikowska, A. (2020). Legal aspects of synchronising data on real property location in polish cadastre and land and mortgage register. *Land Use Policy*, 95, 104606. <https://doi.org/10.1016/j.landusepol.2020.104606>
- Rich, E., & Knight, K. (1991). *Artificial Intelligence*. New York: McGraw-Hill.
- Sandberg, H. (2001). Three-dimensional division and registration of title to land: Legal aspects. In *Proceedings of the International Workshop on 3D Cadastres*, 2001, Delft (pp. 201–209).
- Sladić, D., Radulović, A., & Govedarica, M. (2020). Development of process model for Serbian cadastre. *Land Use Policy*, 98, 104273. <https://doi.org/10.1016/j.landusepol.2019.104273>
- Stoter, J., & Ploeger, H. (2003). Registration of 3D objects crossing parcel boundaries. In *Proceedings of 2003 FIG Working Week, Paris, France*, April 13–17, 2003.
- Stoter, J., & Zevenbergen, J. (2001). Changes in the definition of property: A consideration for a 3D cadastral registration system. In *Proceedings of the FIG Working Week*, Seoul.

- Tan, L. C., & Hussin, K. B. (2012). Establishing 3D Property Rights in Malaysia. In *Proceedings of the 2012 FIG Working Week, Knowing To Manage The Territory, Protect The Environment, Evaluate The Cultural Heritage*, Rome, Italy, 6–10 May 2012 (pp. 1–24).
- Van Oosterom, P., Ploeger, H., Stoter, J., Thompson, R., & Lemmen, Ch. (2006). Aspects of a 4D Cadaster: a first exploration. In *XXIII FIG Congress*, Munich, Germany.
- Van Oosterom, P., Stoter, J., Ploeger, H., Thompson, R., & Karki, S. (2011). World-wide inventory of the status of 3D Cadastres in 2010 and expectations for 2014. In *Proceedings of the 2011 FIG Working Week, Bridging the Gap between Cultures*, Marrakech, Morocco.
- Williamson, I. P., (1997). Strategic Management of Cadastral Reform – Institutional Issues. In *FIG Commission 7 Symposium on Cadastral Systems in Developing Countries*, Penang, Malaysia.

Author information



Robiya S. Toshboyeva – Dr. Sci. (Law), Associate Professor, Department of Business Law, Tashkent State University of Law

Address: 35 Sayilgokh Str., 100047 Tashkent, Uzbekistan

E-mail: robiyatoshboeva@gmail.com

ORCID ID: <https://orcid.org/0000-0003-2898-2109>

Google Scholar ID: <https://scholar.google.com/citations?user=OXu7SxQAAAAJ>

Conflict of interests

The author declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – April 14, 2024

Date of approval – April 25, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:347.211:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.29>

Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн

Фабио Северино

Traent SRL, Пиза, Италия

Людовика Спозини ✉

Школа перспективных исследований Сант'Анна, Пиза, Италия

Ключевые слова

блокчейн гибридный,
блокчейн публичный,
блокчейн частный,
Европейский союз,
законодательство
защита персональных
данных,
Общий регламент по защите
данных,
право,
право на забвение,
цифровые технологии

Аннотация

Цель: в статье рассматриваются проблемы, связанные с конфликтом между технологией блокчейн и «правом на забвение», предусмотренным европейской системой защиты данных.

Методы: в первом разделе кратко описаны эволюция технологии блокчейн, а также наиболее актуальные проблемы, возникающие между традиционными моделями блокчейна и законодательством Европейского союза. Среди последних проанализирован конкретный вопрос конфликта между природой традиционных блокчейнов (как частных, так и публичных моделей), как правило, неизменяемых, и правом индивида требовать удаления или изменения своих персональных данных. В этом разделе отмечается важность задачи по защите персональных данных, которая всегда была одной из главных для национальных законодателей. Приводится анализ правового регулирования защиты данных и соответствующей практики Европейского суда по правам человека. Поднимается проблема выражения свободного самоопределения личности в виде контроля над управлением персональными данными в Интернете. Второй раздел посвящен изучению возможных путей решения сложившегося противоречия, позволяющих сделать систему распределенных реестров совместимой с европейским законодательством о защите данных. Сделан акцент на модели, предложенной компанией Traent, гарантирующей право на удаление и изменение данных. Анализируются возможности данной модели по разрешению указанного противоречия.

✉ Контактное лицо

© Северино Ф., Спозини Л., 2024

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

Результаты: рассмотрены особенности новой модели и ее возможности по стратегическому использованию преимуществ публичных и частных блокчейнов. Показано, что данная модель гарантирует не только достоверность и подлинность цепочки, по которой была проведена транзакция, но и, что особенно важно, изменение и полное удаление персональных данных пользователя. Это инновационное решение потенциально дает возможность справиться с противоречием между требованиями конфиденциальности данных и развитием блокчейна в европейском контексте.

Научная новизна: компании Traent удалось реализовать «гибридную» модель, которая включает в себя как публичные, так и частные компоненты блокчейна, что позволяет достичь эффективного соответствия нормам Европейского союза в отношении защиты и конфиденциальности данных.

Практическая значимость: полученные выводы и предложения могут учитываться при совершенствовании соответствия блокчейн-технологий принципам Общего регламента Европейского союза по защите персональных данных.

Для цитирования

Северино, Ф., Спозини, Л. (2024). Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн. *Journal of Digital Technologies and Law*, 2(3), 565–584. <https://doi.org/10.21202/jdtl.2024.29>

Содержание

Введение

1. Определение, функционирование и основные особенности технологии блокчейна
 - 1.1. Единая технология, различные классификации
 - 1.2. Публичный и частный блокчейн... и третий путь
 - 1.3. Кейс: компания Traent и преимущества гибридного блокчейна
2. Конфликт между технологией блокчейна и «правом на забвение» в контексте европейского законодательства в области защиты данных. Решение компании Traent
 - 2.1. Несовместимость между «правом на забвение» и технологией блокчейна
 - 2.2. Модель, разработанная компанией Traent, гарантирующая право на удаление и изменение данных

Заключение

Список литературы

Введение

2008 г. стал поворотным для так называемой эры цифровой революции. Именно тогда была опубликована статья Сатоши Накамото «Биткойн: одноранговая система электронных денег»¹. Это произошло в рамках движения «киберпанк», выступавшего

¹ Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://clck.ru/3EGDkg>

против вызванных новыми технологиями ограничений индивидуальных свобод, и в частности, права на неприкосновенность частной жизни. Для достижения этой цели биткоин представлялся полезным инструментом: это электронная валюта, широко использующая криптографические технологии и позволяющая создавать безопасные и неопровергаемые системы обмена товарами, услугами и, прежде всего, информацией.

Накамото предложил создать коммуникационный протокол, т. е. неизменяемый реестр, организованный в отдельные блоки, каждый из которых содержит одну или несколько транзакций. Они соединяются вместе, образуя цепочку, отсюда и название «блокчейн». Каждый блок имеет «заголовок», в котором содержится хэш – ряд букв и цифр, кодирующий все транзакции, записанные в этом блоке, – а также отметка времени и хэш предыдущего блока.

При этом используются различные технологии, включая: i) шифрование с асимметричным ключом, позволяющее проверить источник сообщений, а также их целостность; ii) одноранговую систему, преимущество которой заключается в отсутствии необходимости в центральном органе для подтверждения транзакций; iii) «доказательство работы» – механизм формирования консенсуса, основанный на использовании вычислительных ресурсов для решения математической задачи. Иначе говоря, узел, которому первому удастся распространить правильное решение среди остальных участников сети, получает вознаграждение за оказанную услугу. В то же время система обеспечивает корректность этого результата именно тем, что для его получения задействовано большое количество ресурсов².

В основе данной технологии лежит сеть компьютеров, которые обмениваются между собой распределенным реестром, содержащим копии всех транзакций, совершенных в цепочке. Таким образом, можно гарантировать, с одной стороны, безопасность системы регистрации, поскольку переписать все блоки было бы очень сложно; с другой – ее прозрачность, поскольку каждый раз, когда совершается новая транзакция, она записывается в каждую «копию» распределенного реестра. Это означает, что каждый участник может проверять транзакции и иметь доступ к данным без необходимости наличия централизованной высшей инстанции. Вместо этого система перераспределяет полномочия по проверке между пользователями в практически равных долях, создавая эффективную, прозрачную и, прежде всего, более демократичную систему³. Эта технология, изначально созданная для обмена криптовалютой, благодаря

² Следует отметить, что это лишь один из многих существующих механизмов консенсуса, включая: i) так называемое доказательство владения (Proof of Stake, PoS), согласно которому возможность подтверждения транзакций прямо пропорциональна количеству активов, которыми обладает узел; ii) делегированное доказательство владения (Delegated Proof of Stake), основанное на своего рода голосовании, при котором каждый пользователь, обладающий активами в системе, может делегировать подтверждение транзакции другому; iii) консенсус на основе депозита (Deposit-based consensus), при котором для добавления блока в блокчейн необходимо сначала внести обязательный депозит; iv) доказательство существования (Proof of Existence), при котором валидацию могут осуществлять только те, кто имеет определенные полномочия или документы; v) доказательство полномочий (Proof of Authority, PoA), при котором полномочия на валидацию транзакций предоставляются исключительно на основе идентификации самого узла. Подробное объяснение каждого механизма см. (Sarzana & Nicotra, 2018).

³ European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis, где говорится: «Блокчейн частично забирает контроль над повседневным взаимодействием с технологиями у центральных элит, перераспределяя его между пользователями. При этом системы становятся более прозрачными и, возможно, более демократичными» (4). См. также (Lacity & Treiblmaier, 2022).

своему потенциалу сразу же распространилась далеко за пределы этой области (Sarzana & Nicotra, 2018; Rajasekaran et al., 2022; Belotti et al., 2019; Michael et al., 2018; Ammous, 2016)⁴ и теперь находит применение от сектора финансовых услуг, здравоохранения, управления цепочками поставок, так называемого электронного голосования⁵ до цифровых товаров (например, NFT) и паспортов товаров.

В 2015 г. произошел переход к так называемым технологиям второго поколения. Это выразилось в разработке Ethereum – первого программируемого блокчейна, способствовавшего появлению смарт-контрактов и развитию децентрализованных приложений на блокчейне. Более того, достоинства этой технологии вскоре были признаны и европейским законодателем. Было заявлено, что ее использование может ускорить процесс согласования и исполнения сделок, что дает значительные преимущества для развития внутреннего рынка⁶. Однако отмечалось также, что законодательство Европейского союза, сформировавшееся до появления блокчейна, не может справиться с возможными рисками и опасностями, которые блокчейн представляет для основных прав, и прежде всего, для защиты персональных данных⁷.

1. Определение, функционирование и основные особенности технологии блокчейна

С 2008 г. было реализовано несколько блокчейнов, каждый из которых имеет свои отличительные особенности. Из-за этой неоднородности очень трудно (если вообще возможно) дать единое и общее определение этому явлению⁸. Тем не менее можно сделать некоторые общие выводы.

Прежде всего, технология блокчейн является подкатегорией «технологии распределенных реестров» (Distributed Ledgers Technology, DLT), т. е. особых типов баз данных, в которых данные записываются, совместно используются и синхронизируются в распределенной сети компьютеров. Данные могут иметь любую меновую стоимость, поддающуюся экономической оценке; например, это могут быть деньги, контракты, истории болезней, сделки купли-продажи товаров и услуг, свидетельства о рождении или браке. Однако следует отметить, что DLT отличаются от блокчейна способом записи и проверки информации.

⁴ Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. <https://clck.ru/3EGEp4>

⁵ Подробный анализ этих вопросов см. (European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis; Gupta et al., 2023; Mccorry et al., 2021).

⁶ European Parliament. (2022). Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance).

⁷ Там же.

⁸ (Walch, 2016). Стоит отметить, что чрезвычайное разнообразие блокчейна не позволяет выработать общепринятое (и приемлемое) инклюзивное определение всех типов платформ, существующих на рынке в настоящее время (и тех, которые появятся в будущем). Однако если появится такое определение этого явления, которое позволит очертить его границы и, таким образом, рассматривать его в едином ключе, то оно неизбежно будет отличаться излишней жесткостью, которая плохо сочетается с технологическими изменениями. Поэтому предпочтительно, как это уже было отмечено в авторитетных источниках в отношении определения цифровой платформы, использовать функциональный подход для каждой конкретной ситуации. По этому вопросу см. (Bertolini et al., 2021).

Как уже говорилось, это распределенные базы данных, поскольку они работают в сети из нескольких узлов, обычно установленных на одном компьютере (технически – на сервере). При выполнении транзакции она передается в сеть, которая проверяет ее в соответствии с алгоритмом консенсуса (Sarzana & Nicotra, 2018). Таким образом, каждый блок в цепочке, формирующей реестр, неизменно связан с предыдущим и последующим блоками. Другими словами, после добавления блока он уже не может быть изменен без внесения изменений в последующую часть цепочки. Это гарантирует целостность реестра, поскольку для переписывания последующих блоков потребовалось бы одновременно переписать весь реестр, а это невыполнимая операция из-за стоимости и требуемой вычислительной мощности. Затем все данные становятся общедоступны для каждого узла в сети и непрерывно обновляются и синхронизируются.

1.1. Единая технология, различные классификации

В обиходе термин «блокчейн» используется для общего обозначения технологии, основанной на распределенном реестре. На самом деле в эту категорию входят различные типы блокчейнов, каждый из которых имеет свои характеристики и особенности.

Существуют так называемые публичные блокчейны, основополагающим свойством которых является их «децентрализованность». Во-первых, они, как правило, являются «безразрешительными», т. е. пользователи могут выполнять любые операции, в том числе читать существующие и предлагать новые блоки, а также подтверждать транзакции. Иными словами, таким блокчейнам (примером служит платформа Bitcoin) не требуется центральный орган, который выступал бы в качестве посредника или подтверждал транзакции, происходящие в сети. Вместо этого они используют одноранговый механизм, т. е. напрямую соединяют пользователей, которые одновременно становятся активными субъектами для подтверждения транзакций и пассивными, поскольку владеют всей информацией. Как мы уже упоминали выше (Sarzana & Nicotra, 2018), это система, основанная на так называемом механизме консенсуса, поскольку все участники обязаны проверять и создавать транзакции, следуя определенным правилам, которые уже закодированы в программном обеспечении блокчейна. Например, одним из наиболее широко используемых алгоритмов консенсуса является алгоритм «доказательство работы» (Proof of Work, PoW), который опирается на вычислительную мощность компьютеров (называемых «майнерами») для быстрого решения математических задач, которые становятся все более сложными после каждой подтвержденной транзакции. Кроме того, у каждого участника хранится копия реестра. Таким образом, каждый может участвовать в работе сети, а все данные доступны в любое время и в любом месте.

Такой одноранговый механизм делает систему гораздо более устойчивой к возможным атакам, поскольку для этого необходимо поразить большинство узлов, распределенных в сети (Aponte-Novoa et al., 2021). Фактически каждое изменение быстро становится видимым для всех участников, а криптографические подписи гарантируют целостность и аутентичность транзакций (это называется «устойчивостью к взлому» (Austin & Di Troia, 2022)).

Поэтому за каждую правильно подтвержденную транзакцию предусмотрены различные системы вознаграждения, а также действуют протоколы, делающие неправомерное поведение крайне затруднительным.

Из этих кратких рассуждений уже можно понять преимущества и недостатки открытого блокчейна этого типа. Децентрализованная (и, следовательно, распределенная) система обеспечивает как целостность транзакций, так и большую безопасность, поскольку ее сложнее атаковать. Кроме того, транзакции хранятся неограниченное время, что гарантирует верифицируемость всей цепочки. Наконец, они являются публичными и, следовательно, общедоступными, поскольку отсутствует централизованный контроль со стороны какого-либо органа.

С другой стороны, публичные блокчейны, как правило, очень медленно обрабатывают транзакции и, значит, плохо подходят для обработки больших объемов информации. Это связано с тем, что у них есть серьезная проблема масштабируемости, т. е. с увеличением количества узлов в сети скорость выполнения и обработки транзакций снижается⁹. Не говоря уже о воздействии на окружающую среду, которое оказывают такие модели¹⁰.

Существуют и «частные» блокчейны, доступ к которым имеют только авторизованные пользователи. Соответственно, персональные (и другие) данные участников сети распространяются только внутри нее. В частности, речь идет о пользователях, чья личность хорошо известна, поскольку для того, чтобы стать узлом, необходимо выполнить ряд требований и получить одобрение центрального администратора. Кроме того, желающие присоединиться к сети часто должны подписать условия обслуживания, определяющие их права и обязанности. Поэтому очевидно, почему в данном случае не требуются особо строгие механизмы консенсуса: здесь системе не нужно «завоевывать» доверие операторов с помощью дорогостоящих механизмов консенсуса, поскольку каждый узел, будучи легко идентифицируемым и узнаваемым, несет бремя ответственности (Raymond Choo et al., 2020). В системах такого типа проверка транзакций обычно делегируется доверенному подмножеству узлов. Другими словами, если публичный блокчейн в некотором роде можно назвать олицетворением демократии и децентрализации, то в частных реализована парадигма олигархии: не все узлы имеют равное значение.

Такая система, несомненно, имеет ряд технических преимуществ. Во-первых, она гораздо быстрее (поскольку только очень небольшая группа узлов отвечает за проверку и распространение новых блоков), а во-вторых, благодаря возможности ограничить доступ к содержимому блокчейна, она кажется более безопасной с точки зрения конфиденциальности и приватности. Однако именно здесь кроется одна из главных слабостей частных моделей. Если в публичных моделях безопасность технологии обусловлена распределением и децентрализацией реестра, то в частных моделях он не распределяется, а концентрируется в руках одного или нескольких субъектов.

⁹ Проблемы масштабируемости алгоритма «доказательство работы» обусловлены его конструкцией, которая требует значительных вычислительных мощностей для проверки транзакций и добавления блоков. При подключении большего количества узлов они все равно должны обрабатывать и подтверждать все транзакции независимо от того, что снижает общую пропускную способность. Кроме того, высокое энергопотребление и медленная передача блоков еще больше ограничивают масштабируемость этого алгоритма, что приводит к увеличению времени транзакций и повышению стоимости в периоды пикового спроса. По этому вопросу см. (Gramoli, 2022).

¹⁰ Подробнее о влиянии блокчейна на окружающую среду см. Bitcoin Energy Consumption Index. Digiconomist. <https://clck.ru/3EGHgF>

Обе описанные категории, в свою очередь, могут быть «разрешительными» или «безразрешительными»¹¹. Так, существуют «публичные безразрешительные блокчейны», в которых любой человек может участвовать в механизме консенсуса и предлагать транзакции (это, например, касается таких платформ, как Bitcoin или Ethereum), и «публичные разрешительные блокчейны», которые позволяют всем пользователям видеть журнал транзакций и совершать любые операции, хотя в механизме консенсуса участвует лишь небольшое количество узлов. Ярким примером является Ripple¹².

То же относится и к частным блокчейнам¹³, где различают «частные разрешительные блокчейны», которые ограничивают транзакции и возможности отображения реестра только теми узлами, которые участвуют в сети, и оператор платформы сам выбирает, кому разрешить участвовать в механизме консенсуса. Так происходит, например, в случае Rubix¹⁴. Прямо противоположное происходит в «частных безразрешительных блокчейнах»¹⁵, которые ограничивают круг лиц, которым разрешено совершать транзакции и получать доступ к реестру, но, в отличие от первых, здесь механизм консенсуса открыт для всех.

1.2. Публичный и частный блокчейн... и третий путь

Как публичные, так и частные блокчейны имеют свои преимущества и недостатки. Первые, как мы показали, обладают «универсальной» прозрачностью (поскольку транзакции видны всем участникам сети), надежны (благодаря своей децентрализованной природе они менее подвержены одномоментным отказам системы), децентрализованы, доступны (ими управляет глобально распределенная сеть узлов, что делает их очень устойчивыми) и неизменяемы. Однако они очень медленные, поскольку имеют проблему масштабируемости из-за объема транзакций и необходимости децентрализованного подтверждения; у них очень высокая стоимость транзакций, и они не гарантируют конфиденциальность, поскольку являются публичными. Аналогичным образом, частные блокчейны, безусловно, более эффективны, поскольку они масштабируются и работают быстрее (это объясняется тем, что нет необходимости в децентрализованном подтверждении и, следовательно, транзакции обрабатываются быстрее); они гарантируют конфиденциальность информации, содержащейся в сети, и организаторы сети полностью контролируют управление и правила сети. С другой стороны, частные блокчейны менее прозрачны, централизованы и менее безопасны.

Чтобы решить некоторые из проблем, присущих этим двум моделям, был разработан третий тип блокчейна – «гибридный». Эти модели обладают характеристиками

¹¹ Ismail, A. (2020). *Permissioned Blockchains for Real World Applications*. Lakehead University.

¹² Ripple. <https://clck.ru/3EGDyK>

¹³ Nascimento, S. et al. (2019). *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*. European Commission. <https://clck.ru/3EGDUK>

¹⁴ Rubix. <https://clck.ru/3EGE3L>

¹⁵ Однако следует отметить, что это очень редкий случай, поскольку частный безразрешительный блокчейн – это некое противоречие, так как «частный» обычно подразумевает ограниченный доступ, а «безразрешительный» – открытый доступ. Однако можно разработать блокчейн с некими гибридными характеристиками.

публичных и частных блокчейнов, но предлагают большую гибкость и адаптируемость к широкому спектру ситуаций использования. Во-первых, они гибкие, поскольку позволяют настраивать степень децентрализации и конфиденциальности в соответствии с конкретными потребностями приложения, для которого они используются. С другой стороны, такие системы более надежны, поскольку, объединяя публичные и частные элементы, можно повысить общую помехоустойчивость сети (Smith, 2020). Кроме того, они совместимы между собой и могут решать проблемы масштабируемости, уравнивая параметры контроля и децентрализации. Однако сочетание публичных и частных факторов может привести к повышению уровня сложности системы, что, в свою очередь, чревато появлением новых уязвимостей в системе безопасности. Наконец, разработка и внедрение гибридного блокчейна могут потребовать значительных ресурсов и очень высоких затрат.

1.3. Кейс: компания Traent и преимущества гибридного блокчейна

Переход к гибриднему блокчейну представляет собой важный момент эволюции этой области, которая отличается особой гибкостью и адаптивностью. С этой целью итальянская компания Traent¹⁶ реализовала гибридную модель блокчейна, способную объединить преимущества (и устранить недостатки) как публичных, так и частных систем¹⁷.

Как уже упоминалось ранее, в публичных блокчейнах каждый узел, участвующий в сети, имеет копию реестра, поэтому каждая копия содержит все транзакции и криптографические доказательства, связанные с каждым блоком в цепи. По этой причине публичный блокчейн более безопасен, поскольку для изменения транзакции потребуется, чтобы все узлы, которых потенциально бесконечное множество, изменили цепочку («устойчивость к ветвлению»¹⁸). Однако именно потому, что модифицировать цепочку и переписать ее очень сложно, данные в ней нельзя изменить или удалить после опубликования.

С другой стороны, частные блокчейны пытаются решить именно эту проблему: поскольку они распространяются среди ограниченного числа участников, можно ограничить обмен данными. Критическая важность этого механизма обусловлена тем, что пользователи, которые по определению не могут быть беспристрастными, также ответственны за подтверждение транзакций, происходящих на платформе. Это означает, что они могут легко изменить записи в цепочке, поскольку нет третьей стороны с функцией независимого контроля. У стороннего пользователя нет возможности проверить, была ли изменена цепочка.

¹⁶ Traent. <https://clck.ru/3EGJHN>

¹⁷ Следует отметить, что описание технического функционирования платформы выходит за рамки данного обсуждения, поэтому мы отсылаем к работе (Pelosi et al., 2023). Однако представляется целесообразным вкратце описать принцип работы системы Traent, чтобы читатель мог лучше разобраться в проблемах «права на забвение» и блокчейна.

¹⁸ Устойчивость к ветвлению – это способность сети блокчейн противостоять и восстанавливаться после хардфорка, т. е. необратимого расхождения ветвей блокчейна, вызванного конфликтующими правилами. Хардфорки возникают в результате спорных обновлений сети и могут привести к созданию новой криптовалюты. См. (Golden et al., 2020).

Блокчейн, предложенный компанией Traent, напротив, добивается «внешней» (или даже «публичной») проверяемости именно за счет использования гибридной модели. В частности, компания предоставляет заинтересованным пользователям частный блокчейн для совершения любой транзакции, которая материализуется в частном реестре в виде блока вместе с криптографическим доказательством. Впоследствии это доказательство публикуется на внешнем публичном блокчейне с помощью системного компонента под названием Notary (Pelosi et al., 2023). Таким образом, криптографические доказательства, связанные с отдельными блоками, записанными в (частном) реестре, публикуются в (публичном) блокчейне. Таким образом, пользователь может быть уверен, что транзакции не были изменены другими пользователями. Отсутствие ветвлений в цепочке проверяется на внешнем блокчейне благодаря внешнему криптографическому доказательству.

2. Конфликт между технологией блокчейн и «правом на забвение» в контексте европейского законодательства в области защиты данных. Решение компании Traent

Признание «права на забвение» в качестве фундаментального элемента защиты личной идентичности и свобод человека – недавнее достижение современного общества, основанного на модели платформенной экономики (Xue et al., 2020; Cohen, 2017; Kenney & Zysman, 2016; Stark & Pais, 2020; Acs et al., 2021). Защита персональных данных всегда была главной задачей наднациональных законодателей; она признана в Хартии основных прав Европейского союза в качестве автономного и независимого права¹⁹ на частную и семейную жизнь²⁰. Чтобы эффективно применять этот принцип и в то же время обеспечить свободное перемещение и защиту данных в рамках Евросоюза, Комиссия представила в 2012 г. пакет документов, направленных на гармонизацию законодательства в этой области между государствами-членами.

В этом отношении существенный вклад внесла судебная практика Суда Европейского союза (далее – СЕС), и в частности, известное дело Google Spain²¹. Дело касалось гражданина Испании, который обратился к оператору интернет-сайта и компании Google как поисковой системе, чтобы добиться удаления своих данных, опубликованных за несколько лет до этого в одной из национальных газет. В частности, истец заявил, что данные больше не являются актуальными, и требовал права на то, чтобы поисковая система не перенаправляла пользователей на страницу, где сообщалась недостоверная информация. В своем решении суд изложил ряд основных принципов эффективного осуществления права пользователей на удаление своих персональных данных в Интернете. Среди различных вопросов, затронутых в этом решении, суд признал право пользователя требовать,

¹⁹ Хартия Европейского союза об основных правах, OJ C 326, 26.10.2012 (сс. 391–407), Ст. 8.

²⁰ Там же, Ст. 7.

²¹ CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

чтобы определенный вредный контент больше не был доступен в сети и, соответственно, не индексировался в результатах поиска платформы. Это объясняется тем, что, по мнению СЕС, основные права, предусмотренные ст. 7 и 8 Ниццкого договора, должны превалировать над экономическими интересами провайдера, а также общества.

Несмотря на то, что наднациональный суд совершенно однозначно подтверждает высокую значимость причин, по которым пользователь претендует на право удаления информации, этого нельзя сказать о практике Европейского суда по правам человека. В качестве примера можно привести дело *Węgrzynowski and Smolczewski v. Poland*, где выводы были совершенно иными²². В этом решении ЕСПЧ не признает право пользователя на удаление онлайн-информации, а пытается найти баланс между свободой выражения мнения в соответствии со статьей 10 ЕКПЧ и «правом на забвение». Иными словами, суд счел полное удаление контента несоразмерным, а наиболее подходящим средством защиты было признано требование к онлайн-издателю опубликовать дополнительные разъяснения к статье, т. е. предоставить обновленную информацию по теме.

Впоследствии, в 2016 г., Европейский союз принял Общий регламент по защите данных 2016/679 (General Data Protection Regulation, далее – GDPR)²³, в котором в ст. 17 «Право на удаление (“право на забвение”))» наконец было четко указано, что «субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные»²⁴.

Таким образом, это положение признает два различных права: с одной стороны, право на «удаление данных», которое позволяет субъекту данных требовать удаления данных о нем, исходя из того, что по истечении определенного периода времени они больше не представляют интереса и не отражают его личность. С другой стороны, это положение также признает «право на забвение» в строгом смысле, которое шире

²² CEDU, *Węgrzynowski and Smolczewski v. Poland*, Application No. 33846/07, 16 July 2013. <https://clck.ru/3EGJgf>

²³ European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (Text with EEA relevance).

²⁴ Далее в документе определены условия, необходимые для реализации этого права пользователем: (a) персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях; (b) субъект данных отзывает свое согласие, на основании которого? согласно пункту (a) ст. 6(1) или пункту (a) ст. 9(2), проводилась обработка, и если отсутствует иное юридическое основание для обработки; (c) субъект данных возражает против обработки согласно ст. 21(1), и отсутствуют имеющее преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки согласно ст. 21(2); (d) персональные данные обрабатывались незаконно; (e) персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства – члена ЕС, под действие которого подпадает контролер; (f) персональные данные собирались в отношении предоставления услуг информационного общества согласно ст. 8(1). Кроме того, ст. 16 предусматривает право на исправление данных. Подробное обсуждение права на забвение после принятия GDPR см. (Alessi, 2017; Kocharyan et al., 2021; Mantelero, 2013; Politou et al., 2018; Finocchiaro, 2010; Peguera, 2019).

первого и требует от контролера удалить не только всю информацию, касающуюся субъекта данных, но и любую ссылку, копию или точное повторение указанных данных. Другими словами, предполагается, что пользователь должен иметь более широкий контроль над управлением своими данными в Интернете, что является выражением свободного самоопределения личности.

2.1. Несовместимость между «правом на забвение» и технологией блокчейна

Фундаментальной характеристикой блокчейна является его неизменяемость, что, однако, полностью противоречит статье 17 GDPR, которая позволяет пользователям в любое время потребовать и получить изменение или полное удаление своих данных. Это справедливо как для публичных, так и для частных моделей блокчейна. Первые фактически чрезвычайно безопасны, поскольку используют распределенную систему, в которой каждый участник сети имеет копию реестра. Однако это преимущество имеет тот недостаток, что изменить или удалить данные после их внесения в цепочку невозможно, так как информация должна быть удалена с каждого узла (действует так называемый принцип неизменности публичного блокчейна). С другой стороны, частные блокчейны пытаются решить эту проблему, позволяя пользователям выбирать, какие данные публиковать, а какие нет (и с кем ими делиться), однако за счет того, что система не является полностью безопасной. То же самое можно сказать и о простом изменении или исправлении данных, поскольку каждый блок в блокчейне содержит информацию о данных в предыдущем блоке. Это означает, что, если попытаться изменить информацию в одном блоке цепи, последующие блоки не пройдут верификацию.

Было разработано несколько альтернативных решений, чтобы сделать систему совместимой с европейским законодательством о защите данных, поскольку в ст. 17 не указано, как конкретно должно быть достигнуто «удаление» данных. Одни считали, что достаточно простого обезличивания данных, другие предлагали «вывести данные из употребления», т. е. обеспечить, чтобы контролер данных больше не мог использовать информацию в целях принятия решений и передать ее третьей стороне, принимал технические меры для защиты данных и, наконец, был обязан удалить данные, когда это возможно. Еще один вариант – сделать данные полностью недоступными, уничтожив закрытый ключ, соответствующий открытому ключу, которым владеет каждый пользователь сети. В этом отношении даже СЕС не совсем ясно толкует норму GDPR, но, видимо, признает, что стирание означает полное уничтожение данных. В частности, в деле *Peter Nowak v Data Protection Commissioner* за кандидатом на письменном экзамене было признано «право потребовать контролера данных обеспечить стирание, т. е. уничтожение, его экзаменационных ответов и комментариев экзаменатора к ним через определенный период времени»²⁵. По этому поводу Европейский центр парламентских исследований (European Parliamentary Research Service, EPRS)²⁶ также заявил, что

²⁵ CJEU, *Peter Nowak v Data Protection Commissioner*, Case C-434/16, 20 December 2017, ECLI:EU:C:2017:994.

²⁶ Service EPR. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?

«неясно, можно ли рассматривать это как общее утверждение, что стирание данных всегда равносильно уничтожению, тем более что в рассматриваемом деле право на стирание не рассматривалось напрямую. Таким образом, это заявление можно объяснить конкретным контекстом и тем фактом, что прямое уничтожение копии экзаменационных записей может быть наиболее простым способом уничтожения (хотя еще одним очевидным вариантом является вымарывание соответствующей информации)»²⁷.

2.2. Модель, разработанная компанией Traent, гарантирующая право на удаление и изменение данных

Компания Traent предлагает интересное решение, гарантирующее соблюдение права на забвение, а именно гибридный блокчейн. Эта модель предусматривает запись в блок (частного) реестра не всех данных, а лишь «ссылки»²⁸ на ту часть цепи, где хранятся данные. Кроме того, в этот же блок вставляется криптографическое доказательство («дайджест»). Таким образом, благодаря ссылке, записанной в (частной) цепочке, заинтересованный пользователь может получить доступ к полным внешним данным и с помощью дайджеста проверить, что они не были изменены.

Этот двойной механизм не только делает систему более безопасной, поскольку позволяет удостовериться в подлинности информации, содержащейся в блокчейне, но и позволяет пользователям удалять введенные данные: поскольку они находятся за пределами частного блокчейна, их можно удалить, не изменяя цепочку. Таким образом, верификация блокчейна остается действительной, поскольку блоки реестра фактически никогда не изменяются. Однако, поскольку дайджест связан с этими внешними данными (которых больше не существует, так как они были удалены), он перестает работать. В этот момент гибридная модель, разработанная компанией Traent, создает новый блок, вставляемый в частный реестр, в котором данные (к которым ведет ссылка и криптографическое доказательство), содержащиеся в предыдущем блоке, считаются удаленными. Благодаря этой системе пользователь может проверить, что цепочка не была изменена мошенническим путем, и в то же время данные являются подлинными, поскольку из следующего блока ясно, что была произведена операция по удалению данных.

Уже из этих кратких рассуждений ясно, что решение, предложенное компанией Traent, безусловно, в наибольшей степени соответствует ст. 17 GDPR, поскольку позволяет не только полностью удалять данные, но также и изменять их. Таким образом, удастся полностью реализовать как европейский регламент, так и интерпретацию, которую, как представляется, дал ему СЕС.

²⁷ Там же.

²⁸ Это может быть, например, URL.

Заключение

Европейский парламент недавно принял Закон об искусственном интеллекте (Artificial Intelligence Act, AIA)²⁹, призванный повысить доверие к системам искусственного интеллекта и снизить их риски. Для этого закон запрещает или строго ограничивает использование тех систем, которые представляют неприемлемый риск для безопасности, здоровья, достоинства и независимости человека. Вместе с тем предпринимаются усилия по поддержке инноваций и развитию все более совершенных технологий для использования их полного потенциала на внутреннем рынке³⁰.

Несмотря на принятие этого закона, вопрос об ответственности систем искусственного интеллекта продолжает волновать экспертов в этой области. В основном это связано с отсутствием эффективных технических решений, позволяющих полностью объяснить причины, побудившие алгоритм выдать тот или иной результат, так что нередко можно услышать о проблеме «черного ящика» (Springer et al., 2017; Veale & Zuiderveen Borgesius). Таким образом, блокчейн может стать ценным инструментом для достижения цели «надежного ИИ»³¹. Во-первых, он обеспечивает прозрачность алгоритмов, поскольку реестр и записи транзакций хранятся безопасно, децентрализованно и доступны всем участникам сети. Кроме того, это гарантирует неизменность результатов: реестр состоит из множества блоков, каждый из которых содержит серию транзакций и данных и защищен криптографической ссылкой на предыдущий блок. Таким образом, даже самое незначительное изменение одного из блоков делает недействительной всю цепочку.

В заключение можно сказать, что на сегодняшний день блокчейн представляется наиболее подходящим, а возможно, и единственным решением, отвечающим требованиям существующего европейского законодательства в области защиты данных и систем искусственного интеллекта. Однако эта технология все еще содержит ряд проблем, требующих решения, среди которых особенно актуальной является гарантия права пользователя на удаление и изменение своей информации. В этом смысле гибридная модель, реализованная компанией Traent, может стать особенно эффективной альтернативой³², как было кратко продемонстрировано в данной статье. Таким образом, становится возможным полностью использовать потенциал блокчейна для разработки объяснимых алгоритмов и систем искусственного интеллекта, а также устранить или, по крайней мере, снизить любые сомнения в совместимости блокчейна с Общим регламентом Европейского союза по защите персональных данных.

²⁹ European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

³⁰ Там же.

³¹ В Предложении Комиссии по Регламенту Европейского парламента и Совета, устанавливающем гармонизированные правила в области искусственного интеллекта (Artificial Intelligence Act), говорится: «Данное предложение направлено на реализацию второй цели по развитию экосистемы доверия путем создания правовой базы для надежного искусственного интеллекта. Предложение основано на ценностях ЕС и основных правах человека и направлено на то, чтобы дать людям и другим пользователям уверенность в принятии решений на основе ИИ, а также стимулировать предприятия к их разработке» (1). См. также (Nassar et al., 2019).

³² Для более детального ознакомления с технологией Traent и конкретными примерами преимуществ, которые она может дать, см.: Traent. <https://clck.ru/3EGKux>

Список литературы

- Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, 57, 1629–1659. <https://doi.org/10.1007/s11187-021-00561-x>
- Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, 32(1), 145.
- Ammous, S. (2016). *Blockchain technology: What is it good for?* <http://dx.doi.org/10.2139/ssrn.2832751>
- Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, 9, 140549–140564. <https://doi.org/10.1109/ACCESS.2021.3119291>
- Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6
- Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, 21(4), 3796–3838. <https://doi.org/10.1109/comst.2019.2928178>
- Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).
- Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, 51, 133–204.
- Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, 3, 391–404. (In Italian).
- Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. <https://doi.org/10.1201/9781003004998>
- Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. <https://doi.org/10.1007/978-3-031-12578-2>
- Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, 80, 3363–3370. <https://doi.org/10.1016/j.matpr.2021.07.254>
- Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, 32(3), 61–69.
- Kocharyan, H., Vardanyan, L., Hamulák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, 21(2), 96–115. <https://doi.org/10.2478/iclr-2021-0015>
- Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.
- Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, 29(3), 229–235.
- Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, 2(4), 33. <https://doi.org/10.1145/3461461>
- Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, 1, 35–44.
- Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, 10(1), e1340. <https://doi.org/10.1002/widm.1340>
- Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.
- Pelosi, A., Felicicoli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In 2023 *IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). <https://doi.org/10.1109/wetice57085.2023.10477792>
- Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34, 1247–1257. <https://doi.org/10.1016/j.clsr.2018.08.006>
- Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52, 102039. <https://doi.org/10.1016/j.seta.2022.102039>
- Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security)* (1st ed.). Springer Cham. <https://doi.org/10.1007/978-3-030-38181-3>
- Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipoa. (In Italian).

- Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.
- Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium on Designing the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).
- Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, 14(3), 47–72. <https://doi.org/10.6092/issn.1971-8853/12221>
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/crl-2021-220402>
- Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, 36, 713–765.
- Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, 2020(1), 8877128. <https://doi.org/10.1155/2020/8877128>

Сведения об авторах

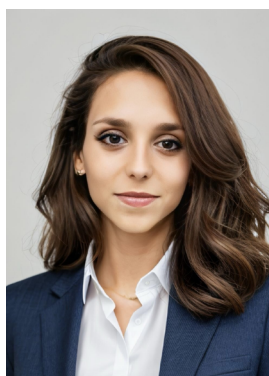


Фабио Северино – технический директор, компания Traent S.r.l.

Адрес: 56127, Италия, г. Пиза, ул. Борго Стретто, 3

E-mail: fabio.severino@traent.com

ORCID ID: <https://orcid.org/0000-0002-9538-1218>



Людовика Спозини – соискатель степени PhD в области права, Институт права, политики и развития (DIRPOLIS), Школа перспективных исследований Сант'Анна

Адрес: 56127, Италия, г. Пиза, ул. Виа Доменико Вернагалли, 22R

E-mail: ludovica.sposini@santannapisa.it

ORCID ID: <https://orcid.org/0000-0003-2188-8996>

Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность компании Traent SRL за предоставление всей технической документации, касающейся данной технологии, для написания статьи. Кроме того, авторы благодарят за оказанную поддержку Центр передового опыта в области регулирования робототехники и искусственного интеллекта имени Жана Монне (Jean Monnet Centre of Excellence on the Regulation of Robotics and AI, EURA).

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.19.31 / Право на информацию

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

История статьи

Дата поступления – 16 июня 2024 г.

Дата одобрения после рецензирования – 2 июля 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:347.211:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.29>

Overcoming the Friction between the “Right to be Forgotten” and Blockchain Technology through a New Approach

Fabio Severino

Traent SRL, Pisa, Italy

Ludovica Sposini ✉

Sant’Anna School of Advanced Studies, Pisa, Italy

Keywords

digital technologies,
European Union,
General Data Protection
Regulation,
Hybrid blockchain,
law,
Legislation,
Personal data protection,
private blockchain,
public blockchain,
right to be forgotten

Abstract

Objective: this paper explores the challenges arising from the conflict between blockchain technology and the “right to be forgotten” as provided by the European data protection framework.

Methods: in the First Section, the author provides a brief description of the evolution of blockchain technology and the most pressing issues between traditional blockchain models and UE’s legislations. Among the latter, the author analyzes the specific issue concerning the clash between the traditional blockchains (both private and public models), typically immutable, and the individual’s right to cancellation or modification of own personal data. This section emphasizes the importance of personal data protection, which has always been one of the main tasks for supranational legislators. The legal regulation of data protection and the relevant judicial practice of the European Court of Human Rights is analyzed. The author raises the problem of expressing the free self-determination of an individual in the form of controlling their personal data on the Internet. The Second Section of this contribution is dedicated to the study of probable ways to solve the existing incompatibility and to make the distributed ledger system compatible with the European data protection legislation. An emphasis is made on the model provided by “Traent” company, which ensures the right to data cancellation or modification. The capability of this model to solve the said contradiction is analyzed.

✉ Corresponding author

© Severino F., Sposini L., 2024

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

Results: the study delves into the peculiar features of the new model to understand how it strategically utilizes the advantages of public and private blockchains guaranteeing not only the validity and authenticity of the chain where the transaction was performed, but, most importantly, the modification and granular cancellation of client's personal data. This innovative solution offers a potential path forward for navigating the complex intersection of data privacy and blockchain innovation in the European context.

Scientific novelty: Traent has implemented a “hybrid” model blockchain that, incorporating both public and private components, to achieve an effective compliance with the European Union regulations, especially those concerning data protection and privacy.

Practical significance: the obtained conclusions and proposals can be taken into consideration in improving the compliance of blockchain technologies with the European Union General Data Protection Regulation.

For citation

Severino, F., & Sposini, L. (2024). Overcoming the Friction between the “Right to be Forgotten” and Blockchain Technology through a New Approach. *Journal of Digital Technologies and Law*, 2(3), 565–584. <https://doi.org/10.21202/jdtl.2024.29>

References

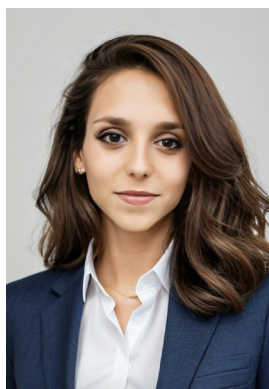
- Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, 57, 1629–1659. <https://doi.org/10.1007/s11187-021-00561-x>
- Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, 32(1), 145.
- Ammous, S. (2016). *Blockchain technology: What is it good for?* <http://dx.doi.org/10.2139/ssrn.2832751>
- Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, 9, 140549–40564. <https://doi.org/10.1109/ACCESS.2021.3119291>
- Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6
- Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, 21(4), 3796–3838. <https://doi.org/10.1109/comst.2019.2928178>
- Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).
- Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, 51, 133–204.
- Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, 3, 391–404. (In Italian).
- Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. <https://doi.org/10.1201/9781003004998>
- Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. <https://doi.org/10.1007/978-3-031-12578-2>
- Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, 80, 3363–3370. <https://doi.org/10.1016/j.matpr.2021.07.254>
- Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, 32(3), 61–69.

- Kocharyan, H., Vardanyan, L., Hamulák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, 21(2), 96–115. <https://doi.org/10.2478/iclr-2021-0015>
- Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.
- Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, 29(3), 229–235.
- Mccorrey, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, 2(4), 33. <https://doi.org/10.1145/3461461>
- Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, 1, 35–44.
- Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, 10(1), e1340. <https://doi.org/10.1002/widm.1340>
- Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.
- Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). <https://doi.org/10.1109/wetice57085.2023.10477792>
- Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34, 1247–1257. <https://doi.org/10.1016/j.clsr.2018.08.006>
- Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52, 102039. <https://doi.org/10.1016/j.seta.2022.102039>
- Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security)* (1st ed.). Springer Cham. <https://doi.org/10.1007/978-3-030-38181-3>
- Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).
- Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.
- Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium on Designing the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).
- Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, 14(3), 47–72. <https://doi.org/10.6092/issn.1971-8853/12221>
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/crl-2021-220402>
- Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, 36, 713–765.
- Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, 2020(1), 8877128. <https://doi.org/10.1155/2020/8877128>

Authors information



Fabio Severino – CTO, Traent SRL
Address: Borgo Stretto 3, 56127, Pisa, Italy
E-mail: fabio.severino@traent.com
ORCID ID: <https://orcid.org/0000-0002-9538-1218>



Ludovica Sposini – PhD Candidate (Law), DIRPOLIS Institute (Institute of Law, Politics and Development), Sant'Anna School of Advanced Studies
Address: Via Domenico Vernagalli 22R, 56127 Pisa, Italy
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: <https://orcid.org/0000-0003-2188-8996>
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The authors would like to thank Traent SRL for providing all the technical documentation concerning its technology for the purpose of this article. In addition, we would also like to thank the Jean Monnet Centre of Excellence on the Regulation of Robotics and AI (EURA) for the support.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 16, 2024
Date of approval – July 2, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024



Научная статья

УДК 34:004:347.4:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.30>

Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования

Дмитрий Александрович Казанцев ✉

Торгово-промышленная палата Российской Федерации, Москва, Россия

Павел Догнал

Оставский технический университет, Острава, Чехия

Павел Догнал – младший

ИТ-университет в Копенгагене, Копенгаген, Дания

Ключевые слова

аукцион,
законодательство,
закупка,
искусственный интеллект,
конкуренция,
нейросеть,
право,
регулирование,
тендер,
цифровые технологии

Аннотация

Цель: обоснование перспективных направлений правового регулирования отношений, связанных с использованием технологий искусственного интеллекта в конкурентных (коммерческих и публичных) закупках.

Методы: исследование проводилось на основе индукции, синтеза, аналогии, декомпозиции проблематики и обобщения выводов. Рассуждения строились на опыте проведения сложной закупки высокотехнологичного оборудования. Этот реальный пример был рассмотрен в качестве экспериментальной модели для исследования с последующим прогнозированием потенциального использования технологий искусственного интеллекта в конкурентных закупочных процедурах.

Результаты: сформулированы преимущества и потенциальные риски использования технологий искусственного интеллекта в закупочной работе, а также даны рекомендации по регулированию такого использования. Выделены рекомендации общеправового характера, касающиеся правосубъектности и деликтоспособности искусственного интеллекта, предложены формулировки новых норм, варианты регулирования использования новых инструментов проведения закупок. Доказано, что технологии искусственного интеллекта при продуманном использовании способны не только повысить качество работы и существенно снизить организационные издержки, но и при этом послужить развитию базовых принципов регулируемых закупок:

✉ Контактное лицо

© Казанцев Д. А., Догнал П., Догнал – младший П., 2024

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.

прозрачности процедур, развития конкуренции за подряд между квалифицированными поставщиками, обоснованности решений, экономической эффективности использования денежных средств заказчика.

Научная новизна: несмотря на большое количество работ, посвященных как проблематике искусственного интеллекта в целом, так и его использованию в закупках в частности, данная проблематика рассматривается в статье на основе преимущественно индуктивного рассуждения, строящегося на рассмотрении частного случая и опыте проведения сложной закупки для цели наукоемких исследований, преломляющегося через призму сущностного соотнесения между собой базовых понятий «цифровизация», «автоматизация», «роботизация» и т. п.

Практическая значимость: описанные в настоящей работе направления использования искусственного интеллекта могут быть реализованы корпоративными, а в перспективе и государственными заказчиками для повышения качества своих закупок. При этом рекомендации по нормативному регулированию такой инновации представляются востребованными как на законодательном, так и на локальном уровне.

Для цитирования

Казанцев, Д. А., Догнал, П., Догнал – младший, П. (2024). Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования. *Journal of Digital Technologies and Law*, 2(3), 585–610. <https://doi.org/10.21202/jdtl.2024.30>

Содержание

Введение

1. Субъектность ИИ в закупочных отношениях

2. Область использования ИИ в закупках

3. ИИ при подготовке закупки

4. ИИ при проведении закупки

Заключение

Список литературы

Введение

Конкурентные закупки традиционно относятся к регулируемым видам деятельности. Различны методы такого регулирования и инструменты, предписанные регулятором, но публичная закупка как сущность не остается без внимания законодателя, пожалуй, ни в одном из государств Европы. А конкуренция между потенциальными поставщиками за подряд остается одной из основ публичной закупки.

При этом конкуренция за подряд, будучи не самоцелью, а лишь одним из инструментов обеспечения качества закупки, реализуется в виде различных инструментов. Сами эти инструменты постепенно изменяются по мере развития экономических отношений. Эта ситуация одним из своих следствий имеет то, что качественная трансформация закупочных отношений с неизбежностью требует и трансформации

соответствующего правового регулирования. Речь может идти как о модернизации существующих норм, так и о модернизации самой правовой доктрины конкурентных закупок. И во втором случае перед юристами может встать вопрос о формировании принципиально новой системы норм.

Новая система правового регулирования закупок может сложиться и безотносительно к экономическому и технологическому развитию, а просто в силу традиций и специфики развития местного законодательства. Так, например, уже сегодня мы наблюдаем весьма несхожие между собой подходы к проведению конкурентных закупок, предусмотренные, например, законодательством о федеральной контрактной системе США, законодательством о контрактной системе России, Директивой ЕС о публичных закупках от 2014 г. и Закупочным кодексом Италии. Но ниже речь пойдет именно о тех проблемах правового регулирования, которые обусловлены применением в закупках качественно новых инструментов, и прежде всего, инструментов так называемого искусственного интеллекта (далее – ИИ).

Для сферы правового регулирования закупок такая перспектива сегодня уже не является лишь абстрактным теоретизированием. Цифровая трансформация современных хозяйственных и общественных отношений выражается, помимо прочего, и в повсеместном внедрении технологий, условно именуемых искусственным интеллектом, в бизнес-процессы коммерческих и публичных закупок. Сразу стоит оговориться: на современном уровне развития технологий несколько преждевременно говорить об искусственном интеллекте в прямом смысле этого слова. Международные исследования ставят под вопрос корректность самого именованья нейросетей полноценным искусственным интеллектом и признавать за ними возможность полноценного мышления и решения творческих задач (Lee et al., 2021). Этот базовый тезис важен как отправная точка в рассуждениях о применимости и необходимости инновационных технологий обработки больших данных в работе, связанной с подготовкой и проведением закупки.

Здесь же стоит оговориться, что в современной закупочной работе нет универсального инструмента, способного нивелировать или хотя бы минимизировать риски при проведении любой закупки. Таким инструментом, например, не смог стать электронный аукцион. Таким инструментом в обозримом будущем не станут и нейросети. Более того, при закупке стандартизированной, серийной продукции применение нейросетей для анализа рынка и выбора победителя зачастую представляется избыточным.

Однако при закупке сложного, а тем более уникального оборудования количество влияющих на качество закупки факторов и их взаимосвязей настолько велико, что для успешного выбора победителя необходима машинная обработка информации. И подчас в рамках такой обработки нужно не просто автоматизированное вычисление параметров по заранее заданной человеком матрице, а привлечение искусственного интеллекта.

Дело в том, что объем данных, подлежащих обработке для качественного проведения такой закупки, если и не выходит за пределы возможностей человека, то подчас требует привлечения неоправданного объема ресурсов – проще говоря, большого количества времени высококлассных специалистов. Что еще хуже, в ходе обработки этого массива данных такие специалисты будут тратить большую часть своего времени не на экспертную оценку, а на рутинную по своей сути работу: сопоставление показателей, выстраивание таблиц и т. п.

С этой работой несравненно быстрее, а возможно и более качественно, справится искусственный интеллект. Однако проблема состоит в том, что принятие искусственным интеллектом решений в рамках бизнес-процессов не может быть полностью прозрачным. Процесс обработки больших данных в той или иной степени остается для стороннего наблюдателя «черным ящиком»: понятны вводные параметры и полученный результат, но процесс трансформации одного в другое не может быть полностью подконтролен человеку.

И само это обстоятельство ставит перед нами несколько вопросов, требующих в том числе и правового разрешения. Уместно ли использование искусственного интеллекта в бизнес-процессах в целом и в процессах закупок в частности? Кто при этом отвечает за решения, принятые искусственным интеллектом? И какова роль человека в таких отношениях?

С привлечением индуктивного рассуждения от частного к общему, а также основываясь на методах синтеза, аналогии, обобщения и использования практической ситуации в качестве экспериментальной модели мы попробуем ответить на эти вопросы на примере закупки сложной продукции для цели наукоемких исследований. Ниже базовые параметры этой закупки будут раскрыты при описании тематического исследования, после чего ключевые тезисы будут предложены в дискуссионном разделе и обобщены в заключении.

1. Субъектность ИИ в закупочных отношениях

Прежде всего необходимо заметить: универсального устоявшегося определения искусственного интеллекта в целом и нейросетей в частности на сегодня не существует. Нет его ни в нормативных актах, ни в юридической доктрине. Как правило, исследователи пишут о сочетании цифровой среды, автономности функционирования алгоритма, его способности к самообучению и к целевой обработке больших массивов информации.

Например, предлагается понимать ИИ как электронную систему, обладающую способностью физически проявлять себя, в том числе чувствовать, обрабатывать информацию и воздействовать на окружающий мир в некоторой степени (Calo, 2015). В крайнем выражении такой подход выражен в концепции так называемого сильного искусственного интеллекта, под которым исследователи понимают такую технологию, которая ментальными свойствами и характером обработки доступной ей информации идентична человеческому сознанию, в том числе в части комплексной интерпретации информации, способности к творчеству и интуиции (Searle, 1990).

Альтернативный подход к пониманию искусственного интеллекта базируется не на внешнем выражении и последствиях его деятельности, а на субъективных факторах его работы. Последователи этого подхода готовы назвать искусственным интеллектом любой интеллект, осознающий себя в качестве самостоятельной личности, независимо от того, будет ли он сопоставим с интеллектом человека или даже будет уступать ему по возможностям интеллектуальной деятельности (Bokovnya et al., 2020). При всей кажущейся простоте подобного подхода на практике сегодня не так-то легко найти пример ИИ, идентифицирующего себя в качестве не просто мыслящего субъекта, а именно самостоятельной личности. И дело здесь не только в несовершенстве технологий робототехники. Несмотря на активное развитие науки, все еще актуален тезис о том, что попытки создания искусственного интеллекта в подлинном смысле этого слова до сих пор не достигли ожидаемого уровня в силу расхождений между

знаниями человечества о строении мозга и возможностями нейробиологии, психологии и кибернетики (Hawkins & Blakeslee, 2004).

А потому на сегодня наиболее реалистичной следует признать концепцию искусственного интеллекта как программно-аппаратного комплекса, не имеющего с человеческим разумом ничего общего в плане сущности мышления, однако способного при этом решать в совокупности аналогичные по сложности либо более сложные задачи (Bokovnya et al., 2020).

Например, в варианте, предложенном Н. Н. Черногором, определение искусственного интеллекта звучит так: «Технология, определяющая способность некой информационной системы без непосредственного участия человека правильно интерпретировать внешние данные (внешнюю информацию), уточнять базу (базы) данных с их учетом, извлекать уроки из допущенных ошибок и использовать полученные знания для достижения конкретных целей, решения конкретных задач посредством гибкой адаптации в условиях плохо определенной ситуации» (Черногор, 2022). Эти признаки как нельзя лучше подходят если не для теории закупочной деятельности, то уж, во всяком случае, для ее практики.

Продуманное регулирование закупочных отношений, реализуемых с использованием технологий искусственного интеллекта, невозможно без разрешения базовых вопросов о соотношении прав и обязанностей. В контексте разговора о применении технологий искусственных интеллектов эти вопросы прямо детерминированы проблематикой субъектности искусственного интеллекта. Проще говоря, можем ли мы рассматривать искусственный интеллект в качестве субъекта правоотношения или же исключительно в качестве инструмента реализации своих правоотношений иными субъектами?

Сразу необходимо оговориться, что вопрос о правовой субъектности искусственного интеллекта невозможно решать раз и навсегда. «То, что составляет понятие «искусственный интеллект», – субъективно и похоже на движущуюся мишень. То, что один человек воспринимает как ИИ, не обязательно является им для другого; то, что считалось искусственным интеллектом, скажем, пятнадцать лет назад, сегодня обыденность. Даже вопрос «что такое интеллект?» является дискуссионным» (Greenstein, 2022). Это тот случай, когда не только отдельные правоотношения, но и базовые аспекты правоспособности и правосубъектности зависят от достигнутого уровня технологий в конкретный момент времени (речь при этом идет не только о параметрах самих технологий, но и о качестве их применения, в том числе в хозяйственных отношениях).

Однако на сегодня, даже с учетом активного развития нейросетей и повсеместной роботизации производств, все еще актуальным остается тезис о том, что существующие понятия правоспособности и дееспособности явно не предусматривают даже теоретическую возможность обладания ими искусственным интеллектом, и приложение к искусственному интеллекту правовой субъектности означает лишь механическую экстраполяцию прав человека на действия искусственного интеллекта (Nevejans, 2016).

Во многом это обусловлено тем, что само право как продукт интеллектуальной деятельности человека и результат развития общественных отношений между людьми по самой своей природе антропоцентрично. И даже не субъектность как таковая, а именно правовая субъектность сущностей, нетождественных человеку, является принципиально новой категорией для системы существующих правовых

институтов. Но не менее важно и то, что сама деятельность ИИ во внешнем ее выражении сегодня не предполагает не только тождества, но даже и близкого подобия деятельности человека даже с учетом того, что скорость и объемы обработки информации нейросетью количественно несравненно превосходят способности человека. А значит, «подходы, которые предлагают обосновать правосубъектность роботов и ИИ с учетом сущности одушевленных субъектов, у которых есть реальная, а не только формально-юридическая воля, получают развитие только после того, как развитие цифровых технологий достигнет объективно высокого уровня» (Бегишев, 2020).

Вместе с тем условность термина «искусственный интеллект» вовсе не означает сомнительность самой технологии. Самообучающиеся алгоритмы обработки больших данных уже сегодня показывают свою прикладную значимость. Не являясь панацеей, технологии обработки больших данных, и в частности, те из них, за которыми закрепилось наименование нейросетей, являются фактором экономического успеха в современном мире.

Разумеется, экономический успех требует рационального и продуманного «точечного» применения нейросетей именно в тех сферах хозяйственных отношений, в которых они могут принести максимальную пользу. А это, в свою очередь, требует современной регуляторики, опирающейся как на понимание самой сути хозяйственных отношений, так и на понимание современных технологий.

Применение таких технологий в закупочных отношениях должно исходить из примата того, что «отношения с использованием искусственного интеллекта – это всегда отношения между субъектами права или по поводу объектов права. В любом случае это отношения, которые на том или ином этапе инициированы, запрограммированы человеком – субъектом права с той или иной степенью ответственности (в том числе в рамках деятельности юридических лиц). Волеизъявление человека на те или иные действия искусственного интеллекта может быть выражено в разной степени: от действий ИИ, находящихся под полным контролем воли человека, до автономных действий ИИ, опять же допускаемых и осознаваемых в своих возможных пределах и последствиях человеком (группой лиц)» (Шахназаров, 2022). Только этот подход сегодня позволяет нам решить ряд организационно-правовых вопросов: от определения сферы эффективного применения ИИ до распределения ответственности за последствия его работы.

И лишь отчасти можно согласиться сегодня с тезисом о том, что «юристам не обязательно постигать математические и технические тайны цифровизации; цифровизация не входит в предмет юридической науки. Об этом приходится писать, поскольку многие из тех, кто посвятил свои исследования цифровизации, игнорируют то обстоятельство, что науки делятся на технические и социальные, а юридические науки – науки социальные, и технические нормы не являются предметом их анализа» (Лазарев, 2023). Однако эта мысль напоминает нам о важнейшем тезисе: регулятор не должен и не может подменять собой инженера. А создаваемое регулятором право должно быть адекватно регулируемым отношениям, что применительно к регулированию ИИ невозможно без привлечения профильных экспертов по современным технологиям.

При этом эксперты по цифровым технологиям, и по ИИ в частности, не должны подменять собой регулятора и пытаться использовать для регулирования соответствующих отношений несвойственные им правовые категории. Особенно важно это при разговоре о правовых последствиях отношений, реализуемых с использованием современных цифровых технологий. «С онтологической точки зрения все

передовые технологии являются не субъектами, а объектами, и нет никаких оснований предоставлять им права или привлекать их к юридической ответственности. Даже в свете существующих правил юридической ответственности на основе различных правовых критериев всегда теоретически возможно идентифицировать человека, который понесет ответственность за ущерб, возникший в результате производства или эксплуатации устройства с системой ИИ» (Ивлиев, Егорова, 2022).

Частным следствием вопроса правосубъектности ИИ является вопрос о его деликтоспособности. Регулирование ИИ требуется, помимо прочего, еще и для того, чтобы исключить размывание ответственности за последствия работы ИИ. Матрица такой ответственности является темой для отдельного исследования, однако в любом случае сегодня важно помнить базовый принцип: за последствия работы искусственного интеллекта ответственность несет конкретное физическое или юридическое лицо.

В силу специфики деликтоспособности ИИ, а точнее в силу отсутствия таковой на современном этапе его развития, внедрение этой технологии может быть лишь неоднородным. Максимально упрощая, степень распространения ИИ должна быть обратно пропорциональна риску для жизни и здоровья людей в соответствующей сфере.

Использование ИИ в хозяйственной деятельности на практике сопряжено с риском причинения им вреда, что также является предметом специальных исследований (Bertolini, 2013). При этом американские эксперты уже обсуждают необходимость реализации концепции уголовной ответственности за действия ИИ с учетом вины создателя, программиста, пользователя и других лиц, имеющих отношение к работе ИИ (Hallevy, 2013). Альтернативным решением вопроса является наделение искусственного интеллекта правосубъектностью юридических лиц, например корпораций: такой подход позволяет с помощью юридической фикции применить ответственность к ИИ и при этом обеспечить реальную компенсацию нанесенного ущерба (Chesterman, 2020).

С одной стороны, использование технологий ИИ при подготовке закупки, при описании требований к закупаемой продукции, при выборе победителя закупки и на иных стадиях закупочной работы позволяет минимизировать риск субъективизма должностного лица заказчика. Этот риск традиционно считается одним из фундаментальных в сфере закупок. С другой стороны, сама технология ИИ порождает сегодня ряд специфических рисков, обусловленных именно использованием этой технологии, а точнее, ее несовершенством.

«Применение моделей ИИ может приводить к возникновению рисков, основанных на неверных или неправильно интерпретированных результатах моделей. Реализация данного риска может привести к финансовым потерям, ошибочным решениям, репутационным последствиям. <...> Модель может содержать фундаментальные ошибки (например, ошибки программного кода), что может привести к некорректным расчетам и неточным прогнозам. Модель может быть использована не по назначению. В связи с тем, что модели ИИ обучаются для решения конкретных задач, применение их для решения иных задач может приводить к ошибочным результатам работы. Данные, которые использует модель в процессе эксплуатации, могут существенно отличаться по статистическим свойствам от данных, на которых она была разработана. Неточные и неполные данные могут исказить процесс выявления закономерностей и привести к ошибочным результатам»¹.

¹ Банк России. (2023). Применение искусственного интеллекта на финансовых рынках: доклад для общественных консультаций (с. 28–29). Москва.

Также интуитивно очевидны в контексте использования ИИ риски, связанные с информационной безопасностью. Причем эти риски могут реализовываться как в форме утечки конфиденциальной информации, так и в форме злонамеренного воздействия на сами алгоритмы обработки информации с целью искажения результатов такой обработки.

Наконец, нужно упомянуть о том, что и исследователи, и практики отмечают подверженность нейросетей риску «смещения»: функциональные способности модели при решении отдельных задач регрессируют с течением времени². Остается открытым вопрос о причинах такого регресса, однако само наличие такого риска необходимо учитывать как при внедрении ИИ в бизнес-процессы, так и при формулировке соответствующих регуляторных норм.

2. Область использования ИИ в закупках

Для определения области эффективного использования ИИ требуется сочетание, по меньшей мере, двух факторов. Во-первых, необходимо наличие у заказчика развитых и упорядоченных закупочных практик, прошедших стадии цифровизации и автоматизации. Чрезвычайно сложно и зачастую нерационально использовать технологии ИИ там, где часть закупочных документов оформляется на бумажных носителях, а решения принимаются по непрозрачным правилам. Во-вторых, необходимо определение тех закупок, при осуществлении которых использование ИИ будет очевидным образом положительно влиять на результат. И, разумеется, внедрение современных технологий ИИ требует организационных, финансовых и временных инвестиций, а потому необходимо убедиться в том, что эти инвестиции окупятся эффектом применения ИИ.

Если говорить о первом факторе, то прежде всего стоит разграничить понятия цифровизации и автоматизации. Цифровизация сводится к переводу бизнес-процессов в электронную среду. Как правило, цифровизация сопряжена с выполнением бизнес-процессов в сети Интернет и удостоверением сделок электронными подписями. Цифровизация является необходимым, но недостаточным условием на пути к автоматизации, поскольку зачастую не означает оптимизации сложившихся бизнес-процессов. Автоматизация же означает именно оптимизацию бизнес-процессов за счет внедрения машинной обработки информации и представляет собой следующий качественный шаг внедрения электронных технологий.

В качестве примера можно привести российскую контрактную систему (хотя она и не является уникальной в смысле перечисленных ниже аспектов). Ее цифровизация началась еще в первые годы XXI в. Сперва в качестве правовой основы для совершения юридически значимых действий в электронной среде был законодательно урегулирован институт электронной подписи. Вскоре после этого стали возникать электронные торговые площадки – специализированные порталы для проведения конкурентных закупок в электронной форме. Затем крупнейшие заказчики постепенно перевели в цифровую среду весь цикл закупочных отношений от прогнозирования и планирования закупки до заключения и исполнения контракта.

² Chen, L., Zaharia, M., & Zou, J. (2023, July). How is ChatGPT's Behavior Changing over Time? <https://clck.ly/3CdmQ3>

Закон КНР от 31 августа 2018 г. «Об электронной коммерции» нормативно урегулировал понятие оператора электронной торговой площадки как организации, которая предоставляет двум или нескольким сторонам возможность торговать услугами, вести деятельность интернет-магазинов, осуществлять поиск продавцов и покупателей, а также публиковать информацию, необходимую для ведения подобной деятельности³. При этом китайский законодатель разделил три типа сходных субъектов, участвующих в работе ЭТП:

- Оператор ЭТП как юридическое лицо или структура без образования юридического лица, который предлагает онлайн-среду для цифрового бизнеса и проведения взаиморасчетов сторон, обмена информацией и прочие услуги, способствующие заключению сделки электронной коммерции ее сторонами.

- Оператор, работающий на ЭТП, т. е. пользователь электронной торговой площадки.

- Онлайн-продавец как участник рынка электронной коммерции, не использующий ЭТП, а продающий товары, работы или услуги через собственный сайт или через иные каналы распространения информации в сети Интернет.

При этом на оператора ЭТП возложена обязанность по обеспечению кибербезопасности⁴, а также по формированию и поддержанию работоспособности системы оценки пользователей, осуществляющих предпринимательскую деятельность при помощи ЭТП⁵.

Электронная форма закупочной деятельности позволила существенно повысить прозрачность закупочной работы (что особенно важно для публичных закупок), а также оптимизировать организационные издержки на выполнение закупочных бизнес-процессов. Но по своей сути это были те же бизнес-процессы, которые до того проходили вне цифровой среды. Для качественной модернизации самих бизнес-процессов в закупочную работу стали постепенно внедряться инструменты автоматизации, т. е. обработки определенных объемов информации по заданному алгоритму без участия человека. В качестве примера такой автоматизации в закупочной работе можно привести сквозное наследование данных с предзаполнением форм каждого последующего документа, формируемого в рамках единого закупочного цикла, информацией предшествующего документа. Другой пример – это автоматизированный подбор и автоматизированное ранжирование предварительных предложений о поставке в рамках той процедуры, которая в России именуется малой электронной закупкой, а в международной практике – динамическими закупками (“Dynamic purchasing systems” в Директиве ЕС о публичных закупках⁶ и “Sistemi dinamici di acquisizione” в Закупочном кодексе Италии⁷).

Таким образом, можно констатировать, что с начала XXI в. «в российских закупках произошли качественные изменения. В настоящий момент на первый план выходят не только вопросы модернизации бизнес-процессов и экономической

³ Art. 9 Law of the People’s Republic of China dated August 31, 2018 “On E-Commerce”.

⁴ Art. 30. Law of the People’s Republic of China dated August 31, 2018 “On E-Commerce”.

⁵ Art. 39. Law of the People’s Republic of China dated August 31, 2018 “On E-Commerce”.

⁶ Art. 34 Directive 2014/24/EU on public procurement.

⁷ Art. 55 Codice dei contratti pubblici.

эффективности. Государство старается системно подходить к решению вопросов результативности закупок путем оптимизации всех связанных процессов на каждом этапе закупочной процедуры и внедрения сквозной автоматизации. Как отмечают заказчики, электронные закупочные процедуры обеспечивают оптимизацию расходов бюджета и трудозатрат, повышение эффективности закупок в среднем на 25–30 %» (Шмелева, 2019а).

Если в закупочной работе реализована сквозная цифровизация и внедрены инструменты автоматизации, по крайней мере, ее базовых «узлов», то можно говорить о наличии предпосылок для использования технологий искусственного интеллекта. Однако даже при наличии такого базиса не стоит стремиться к тотальному применению ИИ ко всему спектру закупочной работы. С точки зрения оптимизации бизнес-процессов нейросети нужны лишь там, где их использование поможет существенно сократить затраты времени и при этом повысить качество проведения закупки.

В качестве практического примера можно рассмотреть закупку, в действительности имевшую место при строительстве магнитопровода на проекте одного из крупнейших научно-исследовательских центров Европы, специализирующегося на изысканиях в сфере ядерной физики. Этот проект потребовал создания нового ускорительного комплекса для изучения свойств плотной барионной материи.

Магнитопровод, необходимый для работы этого ускорителя элементарных частиц, представляет собой быстровозводимую конструкцию весом более 700 тонн, обладающую особыми материальными и магнитными свойствами. Корпус магнитопровода является ключевой частью детектора, работающего в составе ускорительного комплекса. Как назначение этого комплекса, так и технические характеристики магнитопровода можно, вне всякого сомнения, отнести к категории наукоемких.

Научно-исследовательский центр как головная организация проекта разработал конструкторскую документацию будущего магнитопровода. Согласно конструкторской документации, изготовление основных частей магнитопровода было распределено между двумя производителями, которые должны были выполнять производство параллельно. Параллельное производство, в свою очередь, было необходимо для соблюдения сроков реализации проекта.

В качестве производителей были выбраны заводы в разных странах: один из них располагался в Краматорске, другой – в Генуе. Изготовленные на этих заводах части для обработки и предварительного монтажа направлялись в Чехию. В Чехии же производились конструкции, обеспечивающие транспортировку отдельных частей изделия в научно-исследовательский центр, к месту их окончательной установки.

После изготовления на заводах базовые элементы конструкции прошли сложный процесс приемо-сдаточных испытаний, в рамках которых строго проверялись в том числе такие параметры каждого элемента, как размер, химический состав, механические свойства, магнитные свойства и др. Если хотя бы по одному из параметров было бы выявлено отклонение, то это могло поставить под угрозу реализации весь проект.

После успешной приемки на заводах-изготовителях заготовки были отправлены в Чехию. При этом, учитывая тот факт, что заготовки были произведены в разных странах, важно было обеспечить правильный выбор таможенного режима ввоза заготовок в Чехию для их последующей одновременной переработки. Для того чтобы приступить к переработке поставленных заготовок, чешский завод

на основе конструкторской документации научно-исследовательского центра разработал собственную заводскую конструкторскую документацию, которая включала следующие разделы:

1. Входной контроль заготовок: замер размеров, геометрии деталей; составление технических паспортов.
2. Порядок обработки заготовок.
3. Требования к изготовлению деталей, необходимых для сборки магнитопровода.
4. Требования к изготовлению оснастки для сборки и разборки магнитопровода.
5. Технологическая карта контрольной сборки магнитопровода на заводе с участием представителей научно-исследовательского центра, включающая установку и настройку взаимного расположения деталей люльки.
6. Методика измерения горизонтальности опорных плит и контрольных замеров геометрии плит на различных этапах сборки.
7. Порядок подготовки к отгрузке: сверление отверстий и расположение фиксирующих штифтов после контрольной сборки, маркировка штифтов, создание карты расположения штифтов, разборка, упаковка, погрузка, транспортировка.

Наконец, научно-исследовательским центром была организована временная таможенная зона для таможенного оформления компонентов, ввозимых из Чехии. Такой шаг был обусловлен габаритами и массой отдельных деталей, что не позволяло довести указанную продукцию до стандартных таможенных терминалов.

Кратко описанный выше пример показывает, что комплексная закупка высокотехнологичной продукции представляет собой полноценный многоэтапный проект, в котором могут быть задействованы предприятия из разных стран. Эта закупка не ограничивается лишь проведением тендера, а включает в себя задачи в самых разных областях. Причем каждая из этих задач тесно связана со смежными задачами и непосредственным образом влияет на успех реализации всего проекта. Для успешного осуществления такой покупки необходимо провести экспертные изыскания в сфере инженерии и технологии, логистики, таможенного оформления, бухгалтерского оформления, проведения самого тендера, подготовки и заключения международного договора. Сложность закупки усугубляется тем, что сбой хотя бы в одном из этих направлений делает невозможным использование конечным потребителем высокотехнологичной продукции.

Какие ключевые риски можно усмотреть в описанном выше примере?

Прежде всего, это риск выбора поставщика. Неопытный, неквалифицированный производитель (или просто завод, не имеющий необходимого оборудования) не сможет производить необходимую высокотехнологичную продукцию.

Второй риск – это риск ошибок в технической документации. Неверный расчет или даже просто неверное описание данных на одном из этапов изготовления или сборки может поставить под угрозу результат всей поставки.

Третий риск – это риск транспортировки. Важно учитывать, что габариты и масса даже отдельных элементов описываемой техники требовали привлечения к перевозке десятка грузовиков. В то же время стоимость высокотехнологичной продукции диктовала повышенные требования к безопасности при транспортировке.

Поскольку закупка высокотехнологичной продукции часто связана с международным сотрудничеством, риск таможенного оформления соседствует с логистическим риском. А тот факт, что конечным потребителем была научная организация, расположенная за пределами ЕС, только увеличивала значимость этого риска.

Наконец, риск, который нельзя сбрасывать со счетов, – это риск ошибки при оформлении договорных отношений и расчетов за изготовление, наладку и транспортировку. Правильные, своевременные и точно выполненные расчеты при такой покупке – задача сложная сама по себе. Непредвиденные зачеты и необходимость, например, приобрести для исполнителя дополнительный инструмент за счет средств заказчика только усугубляют трудности и увеличивают риск преднамеренной ошибки.

Традиционно такие риски полностью возлагаются на сотрудников заказчика и поставщика. В этой ситуации возможность минимизации каждого риска полностью зависит от квалификации работника, уровня его знаний, объема доступной ему информации и наличия времени на ее обработку. Однако современный уровень информационных и управленческих технологий позволяет отделить профессиональные знания и компетентность человека от задач по сбору и обработке информации. Ведь ИИ способен обрабатывать несравненно большие объемы информации за значительно меньшее время.

Представляется, что для решения именно таких задач в области управления бизнесом ключевым является не вопрос сущности когнитивных процессов или самоидентификации, а способность обрабатывать большие объемы информации за меньшее время и с меньшими затратами по сравнению с человеком или группой людей. Обработка больших данных представляет собой сферу эффективного применения искусственного интеллекта. В приведенном примере это могут быть, во-первых, данные о квалификации потенциальных производителей, в том числе сведения об их опыте, квалификации работников, культуре производства, наличии необходимого оборудования, соблюдении социальной и экологической ответственности, финансовая устойчивость и др. Во-вторых, это данные о возможных логистических комбинациях и связанных с ними транспортных, административных, погодных и других рисках. В-третьих, это обработка массива инженерно-технической информации с формированием предложений по оптимальным параметрам.

«При осуществлении закупок менеджерам и специалистам приходится изучить огромное количество информации, чтобы принять оптимальное решение. Множество процессов зависит от человеческого фактора, субъективного мнения, сложившихся стереотипов мышления. Искусственный интеллект при осуществлении закупок обладает рядом неоспоримых преимуществ. Это, например:

1. Анализ информации о поставщиках. Искусственный интеллект способен быстро и эффективно обеспечить работу с поставщиками. Он легко находит контрагентов и их контакты, дает информацию о финансовом состоянии компании и анализирует отзывы заказчиков о качестве их работы. При этом время на обработку информации значительно сокращается, а ее количество увеличивается.

2. Управление расходами. Искусственный интеллект на основе машинного обучения способен проанализировать затраты за определенный период времени и определить ситуации, в которых была реальная возможность сэкономить. Программные комплексы способны оперативно сравнивать цены на закупку, сопоставить их с индексами на рынке и порекомендовать более выгодное предложение.

3. Управление рисками. Искусственный интеллект собирает информацию о возможных рисках в цепочке поставок. При этом бизнес может увеличить скорость обработки заказов, оптимизировать расходы и улучшить качество покупаемой продукции <...>.

4. Планирование объема и закупочной цены. Искусственный интеллект учитывает средние расходы за предыдущий период и значимые изменения, способные внести свои коррективы. Для расчета оптимальной цены используются данные о бюджете компании, общей ситуации на рынке, особенности спроса и налоговые обязательства»⁸.

Важно подчеркнуть: обработка информации не тождественна принятию решений. Применительно к роботизации закупок это означает, что экспертиза уполномоченных сотрудников не устраняется из процесса подготовки и проведения закупки. ИИ лишь предлагает экспертам собранную, подготовленную и структурированную информацию. При этом эксперт имеет полномочия как по проверке и дополнению данных, представленных ИИ, так и по формулировке выводов на основании этих данных. Иными словами, рациональное использование технологий ИИ в закупках не исключает, а усиливает экспертную компоненту работы человека.

3. ИИ при подготовке закупки

Условно использование ИИ в закупочной работе можно разделить на роботизацию подготовки закупки и роботизацию проведения закупки. Два эти направления могут развиваться и регулироваться параллельно и обособленно.

Например, сегодня в регулируемых закупках часто вовсе игнорируется или в значительной степени редуцируется такой важнейший этап закупочной работы, как конъюнктурное исследование рынка. А ведь именно это исследование способно дать адекватный ответ на вопрос не только о начальной (максимальной) цене, но и о наиболее эффективном способе закупки! Нейросеть способна за минимальное время собрать и обработать информацию из максимального числа открытых источников, а также структурировать ее по заданным человеком параметрам.

Так, для обоснованного расчета цены важно принимать во внимание не только отвлеченные показатели вроде уровня инфляции или несколько прайс-листов от случайно выбранных поставщиков, но и факторы сезонности, логистики, наличия производств и объемы этих производств, стоимость владения, издержки на потенциальный ремонт оборудования и сопряженные с ним простои и т. д. С учетом всех этих факторов цена превращается из во многом условного показателя в результаты действительного исследования рынка. Да и пресловутый человеческий фактор, который в том или ином виде немало влияет на результаты определения начальной максимальной цены (далее – НМЦ), при использовании нейросети потенциально может быть если и не вовсе устранен, то до известной степени минимизирован.

Не менее важен выбор по итогам исследования рынка релевантного способа закупки: статистика несостоявшихся аукционов поневоле наводит на мысль о том, что классическое ценовое соревнование не всегда может дать заказчику ожидаемый эффект. Для выбора лучшего способа важно учесть уровень формальной и фактической конкуренции на рынке закупаемой продукции, степень эластичности ценообразования (без которого аукцион во многом теряет свой смысл), важность неценовых факторов при выборе лучшего предложения, а в случае

⁸ Большие данные в управлении закупками. Plarforma. <https://clck.ly/3CdmRP>

с госзаказом – еще и репутацию контрактной системы среди местных поставщиков. Такое исследование требует обработки еще больших массивов информации, чем при обосновании НМЦ. И нейросеть вполне могла бы послужить инструментом обработки такой информации.

Нельзя не упомянуть и о такой трудоемкой работе, как составление требований к закупаемой продукции и требований к участникам закупки. И та и другая категория требований должна одновременно удовлетворять предельной точности описания (дабы гарантировать заказчику поставку качественной продукции) и универсальности формулировок (дабы избежать необоснованного ограничения конкуренции). Если же речь идет не о заказе серийной продукции массового спроса, а, например, о возведении инженерных коммуникаций, то ко всему прочему добавляется насущная необходимость составления сложной технической документации.

Подготовка закупки традиционно остается внутренним делом заказчика. Это верно даже при том, что законодательство о публичных закупках в большинстве стран так или иначе регулируют отдельные элементы такой подготовки – например, выбор способа закупки, составление требований к потенциальным поставщикам и т. д. Можно утверждать, что внедрение технологий ИИ в работу по подготовке к объявлению конкурентной закупки не потребует слома существующих норм или радикального изменения правоотношений, связанных с закупкой. Уместнее говорить не столько об изменении законодательства, сколько о его дополнении.

Например, выбор способа закупки из числа предусмотренных законодательством инструментов может быть нормативно предусмотрен не только на основании формальных признаков закупки (таких как размер НМЦ или категория закупаемой продукции), но и результатами конъюнктурного исследования рынка, проведенного ИИ. И в том и в другом случае человеческий фактор, потенциально сопряженный с риском злоупотребления, исключен из принятия решения. И в том и в другом случае основания для выбора способа закупки остаются прозрачными. При этом выбор способа закупки с опорой на результаты исследования, проведенного ИИ, в целом ряде случаев может быть эффективнее с точки зрения реальной закупочной практики, чем принятие того же решения на основании формальных критериев.

Проще говоря, для использования ИИ в подготовке закупки нужна лишь его легализация. Сам процесс подготовки закупки при этом может стать более простым и более эффективным. Но при этом внедрение ИИ не приведет ни к коренному пересмотру, ни к выхолащиванию процесса подготовки закупки.

4. ИИ при проведении закупки

Несколько иначе обстоит дело с внедрением ИИ в процедуру проведения конкурентного определения поставщика. Эта активность традиционно относится к ведению тендерной комиссии. И хотя использование ИИ не приведет к исключению комиссии из закупочной работы (ключевые решения о выборе победителя закупки в любом случае будут приниматься коллегиально), но само по себе привлечение к комиссионной

работе ИИ потребует заметной корректировки не только норм, но отчасти даже и сложившихся институтов закупочного законодательства.

Новые технологии не посягают, да и не должны посягать на такие фундаментальные принципы, как прозрачность и эффективность публичной закупки. Использование этих технологий не должно приводить к необоснованному ограничению конкуренции между потенциальными поставщиками. Но сами инструменты реализации в практической деятельности этих базовых принципов с внедрением ИИ могут претерпеть существенные корректировки.

Например, традиционно к полномочиям тендерной комиссии относят решение о соответствии или несоответствии участника закупки требованиям закупочной документации. Это одно из ключевых решений в процессе проведения закупки, поскольку лишь поставщики, признанные соответствующими требованиям закупочной документации, могут претендовать на победу. Зачастую принятие этого решения сопряжено с исследованием большого объема документов, представленных поставщиками. Но не стоит забывать и о том, что использование ИИ поможет значительно снизить трудозатраты на подобные камеральные проверки.

Уже сегодня участник регулируемой закупки декларирует свое соответствие целому ряду требований. Если статус декларации будет законодательно включать и право заказчика на проверку ее содержания, то саму такую проверку вполне можно поручить нейросети. Разумеется, и положительные, и отрицательные результаты проверки должны сопровождаться ссылкой на источники информации, послужившей обоснованием для решения, а само решение остается за закупочной комиссией.

Снижение издержек на проведение проверок за счет использования ИИ позволит учитывать в ходе таких проверок более широкий спектр факторов, влияющих на качество поставки. Например, уже сегодня законодательство КНР весьма рационально требует: «Если предметом тендера является проект с проведением строительных работ, то в заявке должны содержаться краткие биографические сведения и опыт работы будущего руководителя проекта и основного технического персонала, а также технические характеристики того оборудования, которое будет задействовано в проекте»⁹. Не только опыт работы, но и история взаимодействия с предыдущими заказчиками, используемое для производства оборудование, культура самого производства и даже цепочка поставщиков – все это факторы, имеющие существенное, а порой и решающее значение для выбора контрагента, особенно при заказе на изготовление сложных и высокотехнологичных изделий.

При этом не стоит думать, что ИИ будет самостоятельно выбирать победителя закупки и отклонять предложения его конкурентов. Здесь уместно напомнить те тезисы, с которых начиналась данная статья: если мы рассматриваем ИИ не в качестве субъекта, а именно в качестве инструмента проведения закупочной работы, то за последствия обработки информации с помощью нейросети должны отвечать уполномоченные специалисты. А значит, сперва в корпоративном, а затем и в нормативном регулировании необходимо закрепить матрицу распределения ответственности за последствия применения нейросети между такими специалистами

⁹ Ст. 27 Закона Китайской Народной Республики от 30.08.1999 «О тендерах».

и иными субъектами, оказавшими воздействие на ИИ при обработке данной конкретной информации.

При этом ошибочно было бы полагать, что распределение ответственности за работу ИИ означает увеличение ответственности уполномоченных субъектов. По большому счету речи о возникновении новых сфер ответственности не идет вовсе: сегодня специалисты тендерной комиссии точно так же отвечают за обоснованность решений об оценке и сопоставлении предложений, а инструменты вроде нейросети лишь облегчают подготовительную работу к принятию такого решения.

Этот тезис верен и для одного из самых смелых направлений потенциального использования ИИ в закупочной деятельности – для выбора победителя закупки. Разумеется, речь идет о многофакторном выборе. Ведь для ускорения аукциона во многом достаточно сочетания инструментов автоматизации и предварительных предложений поставщиков. А вот если требуется найти баланс между ценой и качеством, то именно нейросети уместно поручить такое многокритериальное сопоставление.

Не будучи субъектом правоотношения, ИИ может становиться его участником просто потому, что это может обеспечивать более высокую эффективность хозяйственных отношений. «Юристам следует уже сейчас разрабатывать нормы, регулирующие ситуации, когда автономные алгоритмы смогут дополнить и заменить человеческое усмотрение в определении оптимальных правовых норм и сумеют находить соответствующие различия между людьми и использовать их для персонализации санкций, прав и обязанностей» (Харитонов, Ци Сунь, 2023). С помощью ИИ можно использовать большое количество критериев сопоставления предложений при сохранении общей прозрачности логики сопоставления. Такой подход в числе прочего поможет существенно минимизировать риск субъективизма при оценке. Ведь именно этот риск является одним из самых популярных доводов при критике любой альтернативы аукциону.

Не стоит забывать и об упомянутых выше динамических закупках. Для их успешного проведения поставщикам необходимо разместить и по мере необходимости актуализировать свои предварительные предложения о поставке на специализированном портале. Когда заказчик заявляет на том же портале свою потребность в той или иной продукции, то алгоритмы портала автоматизированно подбирают предварительные предложения, релевантные этой потребности. Таким образом, проводится полноценное сопоставление конкурирующих предложений, но за счет автоматизации процесса сбора этих самых предложений вся процедура занимает несколько дней, а не несколько недель, как того требует классический тендер.

Однако для успеха такой конкурентной процедуры чрезвычайно важно качество не только описания заказчиком своей потребности, но и описания потенциальным поставщиком своего предварительного предложения. Технологии ИИ уже сегодня вполне способны оптимизировать и те и другие описания (разумеется, последняя редакция в любом случае остается за человеком). Кроме того, при проведении динамических закупок ИИ мог бы напоминать поставщикам о факторах, в силу которых может потребоваться актуализация предварительных предложений.

Наконец, вполне уместно использовать нейросеть для такой узкоспециализированной, но при этом чрезвычайно важной работы, как определение категории продукции, предложенной поставщиком, ведь от точности определения категории может зависеть попадание предварительного предложения в автоматизированную выборку. «Когда пользователи размещают в каталоге сведения о своей продукции,

им необходимо отнести ее к определенной категории: бумага, полиграфическая продукция, медицинские препараты, зоотовары, канцтовары, текстильные изделия, инженерно-строительные товары, мебель и т. д. Ранее им приходилось вручную выбирать нужную категорию из длинного списка, на что уходило много времени. Нейросеть избавила поставщиков от рутинной процедуры. Достаточно загрузить изображение продукции, и искусственный интеллект за несколько секунд проанализирует картинку, после чего предложит подходящие категории на выбор. По статистике, на сегодня точность определения категории составляет 92 %. Этот показатель будет расти, поскольку нейросеть, как и чат-бот, постоянно обучается и пополняет свой багаж знаний на основе различных моделей»¹⁰.

Описанными выше примерами не исчерпывается потенциал использования ИИ при проведении конкурентных закупок. Часть из описанных выше направлений практически не требует корректировки законодательства – например, использование нейросетей для повышения эффективности динамической закупки. Другие направления потребуют формулировки норм и правил использования новых, неизвестных ранее инструментов – например, многокритериальный выбор победителя с привлечением ИИ. Но в любом случае можно утверждать: использование цифровых технологий уже сегодня становится фактором качества закупок.

Заключение

Резюмируя сказанное выше, стоит признать, что без корректировки существующих норм внедрение технологий искусственного интеллекта в закупочную работу невозможно. Однако именно в сфере закупок речь идет лишь о корректировке, а вовсе не о сломе всей системы регулирования. При этом с точки зрения регулируемых отношений внедрение технологий искусственного интеллекта представляется и уместным, и оправданным. Эти технологии при продуманном использовании способны не только повысить качество работы и существенно снизить организационные издержки, но и послужить развитию базовых принципов регулируемых закупок: прозрачности процедур, развития конкуренции за подряд между квалифицированными поставщиками, обоснованности решений, экономической эффективности использования денежных средств заказчика.

Можно выделить, по крайней мере, следующие направления потенциального внедрения ИИ в закупочную работу:

1. Прогнозирование потребности в закупаемой продукции и управление складскими резервами в целом.
2. Управление текущими контрактами, контроль событий исполнения.
3. Оценка потребности и оценка необходимости проведения закупки для ее удовлетворения.
4. Оценка рисков.
5. Формулировка перечня требований к предмету закупки и подготовка закупочной документации.

¹⁰ Умные закупки: как искусственный интеллект и API-сервисы помогают пользователям Портала поставщиков. (2023, 17 марта). Tadvise. <https://clck.ly/3CdnFb>

6. Предварительное исследование рынка закупаемой продукции и выбор закупочных инструментов.
7. Сбор предложений потенциальных поставщиков.
8. Оценка и сопоставление предложений потенциальных поставщиков.
9. Управление поставкой.

В каждом из этих направлений ИИ не подменяет собой человека, а лишь помогает ему принять более взвешенное решение и при этом потратить на такое решение меньше времени и сил. «Искусственный интеллект должен заменить рутинные процессы: сбор, фильтрацию и классификацию данных о расходах, после чего в автоматизированном режиме определяются признаки нерациональных трат. Аналитика в первую очередь базируется на информации об уже проведенных закупках. В результате использование технологий искусственного интеллекта при автоматизации закупочной деятельности значительно расширит программные возможности по направлениям автоматизированного мониторинга цен, сравнения закупаемых товаров, что позволит выбрать наиболее оптимального подрядчика» (Сергеева, 2022).

А значит, вопрос к юридическому экспертному сообществу заключается лишь в том, чтобы определить пилотные сферы применения нейросетей в закупочной работе, очертить рамки использования этой технологии в названных сферах и урегулировать полномочия и ответственность субъекта использования нейросетей. Эта работа потребует привлечения технологической экспертизы. Однако она не выглядит неосуществимой. А ее результаты послужат основой для постепенного внедрения современных технологий и в смежных отраслях (Siciliani et al., 2023; Burger & Nietzsche, 2023).

Да, в рамках существующих норм внедрение нейросетей во всех названных сферах является непростой задачей. Даже максимально обобщая, стоит помнить о том, что «цифровизация государственных закупок – это не просто вопрос приобретения самых передовых технологий. Это также требует изменения инструментов и способов закупок, которые позволили бы государству осуществлять взаимодействие с новыми технологиями, а также эффективно и быстро интегрировать их в практическую действительность» (Шмелева, 2019b). Однако и фундаментальных, революционных преобразований при таком внедрении вполне можно избежать.

Дело в том, что во всех описанных выше ситуациях нейросеть по своему статусу остается именно инструментом. А лицом, принимающим решение, остается человек. Более того, при использовании цифрового инструмента фиксируются, а значит становятся прозрачными, и входные параметры использования, заданные нейросети для обработки информации, и выходные данные по результатам этой обработки. Уполномоченный субъект может принять их, а может и скорректировать. Обоснование корректировки также фиксируется в электронной среде.

Иными словами, именно в сфере закупок внедрение искусственного интеллекта в качестве одного из инструментов возможно при сохранении корпуса действующего законодательства в целом и системы информационного обеспечения закупок в частности. Потребуется лишь дополнение отдельных норм, таких как нормы об обосновании НМЦ, нормы об оценке участников закупки и т. д., легализацией альтернативного механизма принятия решения. Важно то, что этот механизм направлен не только на повышение скорости обработки больших объемов информации, но и на минимизацию риска субъективизма принятия решений. Проще

говоря, использование нейросетей не нарушает, а развивает принципы регулирования закупок.

Речь ни в коем случае не идет о том, чтобы полностью заменить контрактные службы нейросетью, как часто обсуждается применительно к иным профессиям. В рамках закупок задача нейросети ровно противоположная: во-первых, облегчить работы контрактной службы, «приняв» у нее трудоемкие рутинные вопросы, а во-вторых, дать возможность сотрудникам контрактной службы сосредоточиться на вопросах, требующих высокой профессиональной экспертизы.

Список литературы

- Бегишев, И. Р. (2020). Искусственный интеллект и робот как правовые категории. *Безопасность бизнеса*, 6, 32–36. <https://elibrary.ru/fnittf>
- Ивлиев, Г. П., Егорова, М. А. (2022). Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта. *Журнал российского права*, 6(26), 32–46. <https://doi.org/10.12737/jrl.2022.060>
- Лазарев, В. В. (2023). Юридическая наука в свете перспектив цифровизации. *Журнал российского права*, 2(27), 5–19. EDN: <https://elibrary.ru/wzftgd>. DOI: <https://doi.org/10.12737/jrp.2023.013>
- Сергеева, С. А. (2022). Искусственный интеллект в сфере закупок: возможности и перспективы. *Инновации и инвестиции*, 12, 216–219. <https://elibrary.ru/glsnmk>
- Харитонов, Ю. С., Ци Сунь. (2023). Верховенство закона и алгоритмизация принятия решений в России, Китае, Европе: перспективы персонализации правового регулирования. *Право и бизнес*, 2, 11–17.
- Черногор, Н. Н. (2022). Искусственный интеллект и его роль в трансформации современного правопорядка. *Журнал российского права*, 4(26), 5–15. EDN: <https://elibrary.ru/daazjp>. DOI: <https://doi.org/10.12737/jrl.2022.037>
- Шахназаров, Б. А. (2022). Правовое регулирование отношений с использованием искусственного интеллекта. *Актуальные проблемы российского права*, 9(17), 63–72. EDN: <https://elibrary.ru/yownjo>. DOI: <https://doi.org/10.17803/1994-1471.2022.142.9.063-072>
- Шмелева, М. В. (2019а). Цифровые технологии в государственных и муниципальных закупках: будущее или реальность. *Актуальные проблемы российского права*, 1(12), 36–42. EDN: <https://elibrary.ru/frvgv>. DOI: <https://doi.org/10.17803/1994-1471.2019.109.12.036-042>
- Шмелева, М. В. (2019б). Цифровая трансформация системы государственных и муниципальных закупок. *Юрист*, 7, 15–22. EDN: <https://elibrary.ru/cirwbi>. DOI: <https://doi.org/10.18572/1812-3929-2019-7-15-22>
- 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>
- Bokovnya, A. Y. Begishev, I. R., Khisamova, Z. I., Narimanova, N. R., Sherbakova, L. M., & Minina, A. A., (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, 41, 115–121. EDN: <https://elibrary.ru/efscya>. DOI: <https://doi.org/10.36097/rsan.v1i41.1489>
- Burger, M., Nitsche, A., & Arlinghaus, J. (2023). Hybrid intelligence in procurement: Disillusionment with AI's superiority? *Computers in Industry*, 150, 103946. <https://doi.org/10.1016/j.compind.2023.103946>
- Calo, R. (2015). Robotics and the New Cyberlaw. *Californian Law Review*, 103(3), 513–563.
- Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International and Comparative Law Quarterly*, 69(4), 819–844. <https://doi.org/10.1017/S0020589320000366>
- Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, 30, 291–323. <https://doi.org/10.1007/s10506-021-09294-4>
- Hallevy, G. (2013). *When Robots Kill: Artificial Intelligence under Criminal Law*. University Press of New England.
- Hawkins, J., & Blakeslee, S. (2004). *On Intelligence*. Times Books, Henry Holt and Co.
- Lee, J.-A., Hilty, R., & Liu, K.-C. (Eds.). (2021). *Artificial intelligence and intellectual property*. Oxford University Press. <https://doi.org/10.1093/oso/9780198870944.001.0001>
- Nevejans, N. (2016). *European Civil Law Rules in Robotics: Study*. Brussels: European Parliament's Committee on Legal Affairs.
- Searle, J. R. (1990). Is the Brain's Mind a Computer Program? *Scientific American*, 262(1), 26–31. <https://doi.org/10.1038/scientificamerican0190-26>
- Siciliani, L., Taccardi, V., Basile, P., Di Ciano, M., & Lops, P. (2023). AI-based decision support system for public procurement. *Information Systems*, 119, 102284. <https://doi.org/10.1016/j.is.2023.102284>

Сведения об авторах



Казанцев Дмитрий Александрович – кандидат юридических наук, член Совета по развитию системы закупок, Торгово-промышленная палата Российской Федерации

Адрес: 109012, Россия, г. Москва, ул. Ильинка, 6/1с1

E-mail: info@dkazantsev.ru

ORCID ID: <https://orcid.org/0000-0003-2182-5776>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149755



Павел Догнал – соискатель степени PhD в области права, Остравский технический университет

Адрес: 708 33, Чехия, г. Острава, ул. 17.листопаду, 15/2172

E-mail: pavel.dohnal@vsb.cz

ORCID ID: <https://orcid.org/0009-0001-2733-7418>



Павел Догнал – младший – магистрант, ИТ-университет в Копенгагене

Адрес: 2300, Дания, г. Копенгаген, ул. Руэд Ланггаардс Вей, 7

E-mail: pavd@itu.dk

ORCID ID: <https://orcid.org/0009-0005-6457-1982>

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.27.41 / Сделки

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

История статьи

Дата поступления – 11 марта 2024 г.

Дата одобрения после рецензирования – 26 марта 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:347.4:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.30>

Using Artificial Intelligence for Competitive Procurements: Legal Regulation Issues

Dmitriy A. Kazantsev ✉

Chamber of Commerce and Industry of the Russian Federation, Moscow, Russia

Pavel Dohnal

Technical University of Ostrava, Ostrava, Czech Republic

Pavel Dohnal Jr.

IT University of Copenhagen, Copenhagen, Denmark

Keywords

artificial intelligence,
auction,
competition,
digital technologies,
law,
legislation,
neuron network,
procurement,
regulation,
tender

Abstract

Objective: to substantiate the promising directions of legal regulation of relations in the use of artificial intelligence technologies in competitive (commercial and public) procurement.

Methods: the study was conducted using induction, synthesis, analogy, decomposition of problems and generalization of conclusions. The reasoning was based on the experience of a complex procurement of high-tech equipment. This real-life example was considered as an experimental model for the study and subsequent prediction of the potential use of artificial intelligence technologies in competitive procurement procedures.

Results: advantages and potential risks of using artificial intelligence technologies in procurement work were formulated; recommendations on regulating such use were given. The authors highlighted recommendations of general legal nature concerning the legal personality and delictual capacity of artificial intelligence and proposed the wordings for new norms and options for regulating the use of new procurement tools. It was proved that artificial intelligence technologies, if used thoughtfully, may not only improve the work quality and significantly reduce organizational costs, but also help to develop the basic principles of regulated procurement: transparency of procedures, development of competition for contracts

✉ Corresponding author

© Kazantsev D. A., Dohnal P., Dohnal Jr. P., 2024

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.

between qualified suppliers, reasonableness of decisions, and economic efficiency of the customer's expenditures.

Scientific novelty: despite a large number of works devoted to both the problems of artificial intelligence in general and its use in procurement in particular, the article considers this topic on the basis of mainly inductive reasoning, built on handling a particular case and experience of complex procurement for knowledge-intensive research, refracted through the prism of essential correlation between the basic concepts of "digitalization", "automation", "robotization" and so on.

Practical significance: the directions of using artificial intelligence described in this paper can be implemented by corporate and, in the future, by public customers to improve the quality of their procurement. At the same time, the recommendations on the normative regulation of such innovation seem to be in demand both at the legislative and local levels.

For citation

Kazantsev, D. A., Dohnal, P., & Dohnal Jr., P. (2024). Using Artificial Intelligence for Competitive Procurements: Legal Regulation Issues. *Journal of Digital Technologies and Law*, 2(3), 585–610. <https://doi.org/10.21202/jdtl.2024.30>

References

- Begishev, I. R. (2020). Artificial intelligence and robot as legal categories. *Bezopasnost Biznesa*, 6, 32–36. (In Russ.).
- 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>
- Bokovnya, A. Y., Begishev, I. R., Khisamova, Z. I., Narimanova, N. R., Sherbakova, L. M., & Minina, A. A., (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, 41, 115–121. <https://doi.org/10.36097/rsan.v1i41.1489>
- Burger, M., Nitsche, A., & Arlinghaus, J. (2023). Hybrid intelligence in procurement: Disillusionment with AI's superiority? *Computers in Industry*, 150, 103946. <https://doi.org/10.1016/j.compind.2023.103946>
- Calo, R. (2015). Robotics and the New Cyberlaw. *Californian Law Review*, 103(3), 513–563.
- Chernogor, N. N. (2022). Artificial intelligence and its role in the transformation of the modern law and order. *Journal of Russian Law*, 4(26), 5–15. (In Russ.). <https://doi.org/10.12737/jrl.2022.037>
- Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International and Comparative Law Quarterly*, 69(4), 819–844. <https://doi.org/10.1017/S0020589320000366>
- Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, 30, 291–323. <https://doi.org/10.1007/s10506-021-09294-4>
- Hallevey, G. (2013). *When Robots Kill: Artificial Intelligence under Criminal Law*. University Press of New England.
- Hawkins, J., & Blakeslee, S. (2004). *On Intelligence*. Times Books, Henry Holt and Co.
- Ivliev, G. P., & Egorova, M. A. (2022). Legal issues of the legal status of artificial intelligence and products created by artificial intelligence systems. *Journal of Russian Law*, 6(26), 32–46. (In Russ.). <https://doi.org/10.12737/jrl.2022.060>
- Kharitonova, Yu. S., & Qi Sun. (2023). Rule of law and algorithmization of decision-making in Russia, China, and Europe: prospects for personalization of legal regulation. *Law and Business*, 2, 11–17. (In Russ.).
- Lazarev, V. V. (2023). Legal science in the light of the prospects of digitalization. *Journal of Russian Law*, 2(27), 5–19. (In Russ.). <https://doi.org/10.12737/jrp.2023.013>
- Lee, J.-A., Hilty, R., & Liu, K.-C. (Eds.). (2021). *Artificial intelligence and intellectual property*. Oxford University Press. <https://doi.org/10.1093/oso/9780198870944.001.0001>

- Nevejans, N. (2016). *European Civil Law Rules in Robotics: Study*. Brussels: European Parliament's Committee on Legal Affairs.
- Searle, J. R. (1990). Is the Brain's Mind a Computer Program? *Scientific American*, 262(1), 26–31. <https://doi.org/10.1038/scientificamerican0190-26>
- Sergeeva, S. A. (2022). Artificial intelligence in the field of procurement: opportunities and prospects. *Innovations and Investments*, 12, 216–219. (In Russ.).
- Shakhnazarov, B. A. (2022). Legal regulation of relations using artificial intelligence. *Actual Problems of Russian Law*, 9(17), 63–72. <https://doi.org/10.17803/1994-1471.2022.142.9.063-072>
- Shmeleva, M. V. (2019a). Digital Technologies in State and Municipal Procurement: The Future or Reality. *Actual Problems of Russian Law*, 1(12), 36–42. (In Russ.) <https://doi.org/10.17803/1994-1471.2019.109.12.036-042>
- Shmeleva, M. V. (2019b). Digital transformation of the system of state and municipal procurement. *Jurist*, 7, 15–22. <https://doi.org/10.18572/1812-3929-2019-7-15-22>
- Siciliani, L., Taccardi, V., Basile, P., Di Ciano, M., & Lops, P. (2023). AI-based decision support system for public procurement. *Information Systems*, 119, 102284. <https://doi.org/10.1016/j.is.2023.102284>

Authors information



Dmitriy A. Kazantsev – Cand. Sci. (Law), member of the Council on Purchasing Development, Chamber of Commerce and Industry of the Russian Federation

Address: 6/1 Ilyinka Str., building 1, 109012 Moscow, Russia

E-mail: info@dkazantsev.ru

ORCID ID: <https://orcid.org/0000-0003-2182-5776>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149755



Pavel Dohnal – PhD Candidate, Technical University of Ostrava

Address: 17.listopadu 15/2172, 708 33 Ostrava, Czech Republic

E-mail: pavel.dohnal@vsb.cz

ORCID ID: <https://orcid.org/0009-0001-2733-7418>



Pavel Dohnal Jr. – graduate student, IT University of Copenhagen

Address: Rued Langgaards Vej 7, 2300 Copenhagen, Denmark

E-mail: pavd@itu.dk

ORCID ID: <https://orcid.org/0009-0005-6457-1982>

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – March 11, 2024

Date of approval – March 26, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:349.2:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.31>

Использование искусственного интеллекта при найме работников: проблемы и перспективы правового регулирования

Денис Александрович Новиков

Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Ключевые слова

алгоритм,
закон,
искусственный интеллект,
наем работника,
персональные данные,
право,
работник,
работодатель,
трудовое право,
цифровые технологии

Аннотация

Цель: определить правовые проблемы использования искусственного интеллекта при найме работников и обозначить основные направления их решения.

Методы: формально-юридический и сравнительно-правовой анализ, правовое прогнозирование, правовое моделирование, синтез, индукция, дедукция.

Результаты: выявлен ряд правовых проблем, возникающих при использовании искусственного интеллекта (ИИ) при найме работников, среди которых защита персональных данных соискателя, получаемых при применении искусственного интеллекта; дискриминация и необоснованный отказ в приеме на работу из-за предвзятости алгоритмов искусственного интеллекта; юридическая ответственность за принятое генеративным алгоритмом решение при найме работника. Автор полагает, что для оптимального решения указанных проблем необходимо обратить внимание на передовой опыт зарубежных стран, прежде всего на те страны, где приняты специальные законы о регулировании применения ИИ при найме работников и выработаны руководства для работодателей, применяющих генеративные алгоритмы в аналогичных целях. Кроме того, следует учесть законодательскую работу Европейского союза и США в сфере управления рисками, возникающими при использовании ИИ.

Научная новизна: в работе проведено комплексное исследование правовых проблем, возникающих при использовании ИИ при найме работников, зарубежного опыта их решения, что позволило автору выработать рекомендации по усовершенствованию российского законодательства в данной сфере. Проблему защиты персональных данных соискателей при использовании искусственного интеллекта для

© Новиков Д. А., 2024

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.

найма автор предлагает решить путем дополнения трудового законодательства нормами, закрепляющими требования по прозрачности и согласованности сбора, обработки и хранения информации при применении генеративных алгоритмов. Перечень и объем допустимых для сбора персональных данных следует отобразить в специальном государственном стандарте. Решение проблемы дискриминации из-за предвзятости алгоритмов видится в обязательной сертификации и ежегодном мониторинге программ искусственного интеллекта для найма, а также запрете скоринговых инструментов оценки соискателей. Автор придерживается позиции, что искусственный интеллект не может «вершить судьбу» соискателя: ответственность за решения, принятые алгоритмом о найме, возлагается исключительно на работодателя, в том числе в случаях привлечения третьих лиц для осуществления подбора работников.

Практическая значимость: полученные результаты могут быть использованы для ускорения разработки и принятия правовых норм, правил, инструментов и стандартов в сфере использования ИИ для найма работников. Отсутствие надлежащего правового регулирования в данной сфере создает существенные риски как для прав человека, так и для развития отраслей экономики, в которых задействуются генеративные алгоритмы в целях найма работников.

Для цитирования

Новиков, Д. А. (2024). Использование искусственного интеллекта при найме работников: проблемы и перспективы правового регулирования. *Journal of Digital Technologies and Law*, 2(3), 611–635. <https://doi.org/10.21202/jdtl.2024.31>

Содержание

Введение

1. Проблемы использования искусственного интеллекта при найме работников
 - 1.1. Защита персональных данных соискателя, получаемых при применении искусственного интеллекта для найма
 - 1.2. Дискриминация и необоснованность отказа в приеме на работу из-за предвзятости алгоритмов искусственного интеллекта для найма работников
 - 1.3. Юридическая ответственность за принятое искусственным интеллектом решение о найме работника
2. Зарубежный опыт нормативного регулирования использования искусственного интеллекта для найма работников
 - 2.1. Нормативное регулирование использования искусственного интеллекта для найма работников в США
 - 2.2. Нормативное регулирование использования искусственного интеллекта для найма работников в Европейском союзе

Заключение

Список литературы

Введение

За последние годы в сфере трудовых отношений искусственный интеллект (далее – ИИ) стал важнейшим инструментом осуществления управленческих процессов и процедур. Крупные компании и корпорации все более склонны передавать функции по найму работников технологии ИИ. Например, транснациональная корпорация Unilever уже обрабатывает с помощью ИИ 1,8 млн заявлений о приеме на работу и нанимает 30 тысяч новых работников в год (Ginu & Anson, 2021); 99 % компаний из списка Fortune 500 (500 крупнейших компаний США по годовым доходам) полагаются на ИИ для найма работников (Fuller et al., 2021). За рубежом применяются такие платформы, как AllyO, Arya, BambooHR, Entelo, Ideal, Jibe, Talenture, Taleo, TextRecruit, Textio, Toptal, TurboHire, Turing, Paradox, Recruitee, Upwork, Zoom.ai, ZohoRecruit.

Российские компании («Альфа-Банк», ВТБ, «Додо Пицца», «Мегафон», МТС, РЖД, «Ростелеком», «Сбербанк», «Яндекс» и др.) постепенно интегрируют в свои кадровые решения ИИ для найма работников¹. Как показало исследование HRLink, 24 % российских компаний уже применяют ИИ в процессах найма работников, 6 % планируют внедрить такие решения в течение года, 71 % сотрудников кадровых отделов позитивно воспринимают внедрение ИИ в свою работу². В России среди ИИ-инструментов для найма работников используются такие платформы, как AmazingHiring, FriendWork Recruiter, GoRecruit Hireman, HireVue, Hurma, My new job, PeopleForce, Playhunt, Recright, Talantix, uForce, Yva.ai, Робот Вера, СберПодбор и др.³ Следует учесть, что данные сервисы ИИ для найма работников постоянно совершенствуются, дополняются новыми функциями, в том числе благодаря технологии машинного обучения.

Вследствие бурного развития программного обеспечения для найма работников и его практического применения работодателями в Российской Федерации ставится вопрос о выработке государственной политики в данной сфере. Так, в паспорте национальной программы «Цифровая экономика Российской Федерации» (утв. протоколом Президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 04.06.2019 № 7) отмечается усиление процессов цифровизации в сфере занятости населения и обозначается необходимость одобрения концепции комплексного правового регулирования отношений, возникающих в связи с развитием цифровой экономики. В 2020 г. авторы такой Концепции указали, что для трансформации законодательства в сфере цифровой экономики необходимо сосредоточиться на изменениях трудового законодательства в вопросах,

¹ В России искусственный интеллект начал подбирать персонал. (2023, 11 августа). Ura.ru. <https://clck.ru/3CVvmv>

² Исследование HRLink: 71 % HR-специалистов позитивно относится к ИИ. (2023, 26 декабря). Искусственный интеллект Российской Федерации. <https://clck.ru/3CVvqB>

³ В августе 2023 г. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации заявило о запуске на платформе «Гостех» эксперимента «Государственные кадры», предполагающего использование ИИ для найма на государственную службу. К 2030 г. планируется создать на основе ИИ новую информационную HR-систему развития госслужащих. См.: Искусственный интеллект будет нанимать госслужащих: заменит ли технология конкурсную комиссию? (2023, 23 августа). RG.ru. <https://clck.ru/3CVvvC>

которые касаются правовой защиты граждан в «условиях информационных технологических новаций в сфере труда и дистанционной занятости»⁴.

Кроме того, учитывая тот факт, что ИИ уже изменил и изменит в будущем еще больше способы сбора, обработки и анализа данных о потенциальных работниках, появляются дополнительные риски нарушения прав человека в сфере труда. Поэтому перед работниками, работодателями, разработчиками и государством встает логичный вопрос о правовых последствиях применения ИИ при найме работников. Ведь необходимо учитывать тот факт, что вместе с якобы положительными последствиями глобальной трансформации трудовых отношений в сферах, где используются новые информационные средства производства, возникают реальные неблагоприятные последствия, связанные с перераспределением капитала в обществе и уменьшением социальной защиты трудящихся (Новиков, 2023). Следовательно, правовая проблематика использования ИИ при найме работников заключается в том, как следует регулировать отношения, возникающие при использовании технологии ИИ в целях найма работников и как с юридической точки зрения оценивать решения, принятые алгоритмом.

Проблематика использования ИИ при найме работников обсуждается в российской (Щербакowa, 2021; Serova & Shcherbakova, 2022) и зарубежной юридической науке (De Stefano, 2019; Köchling & Wehner, 2020; Reddy, 2022; Hunkenschroer & Kriebitz, 2023; Basu & Dave, 2024). Однако на сегодняшний день большинство исследований являются фрагментарными, охватывающими отдельные участки данной научной проблемы. Вследствие этого следует обратить более пристальное внимание на правовые проблемы использования ИИ при найме работников и попробовать выработать рекомендации для их решения в рамках нормативного урегулирования.

1. Проблемы использования искусственного интеллекта при найме работников

Процедура найма работников – это ряд мероприятий, которые можно разделить на четыре основных этапа: поиск, отсев, собеседование и отбор⁵. Соответственно, под ИИ в сфере найма работников следует понимать алгоритм, обученный принимать автоматические решения о найме на каждом из этапов (Haenlein & Kaplan, 2019). В алгоритмах найма работников ИИ обучается на данных, полученных от предыдущих кандидатов до и после найма, чтобы сделать прогноз о возможности найма потенциальных кандидатов (Kuncel et al., 2014). К технологиям, содержащим такие алгоритмы, относятся асинхронное видеоинтервью, чат-боты и другие автоматизированные платформы, которые интерпретируют и оценивают ответ кандидата в режиме реального времени и предоставляют оценку интервью (Langer et al., 2019). Алгоритмы ИИ определяют набор правил, используемых для преобразования входных данных в выходные решения и могут быть обучены для имитации человеческих решений о приеме на работу.

⁴ Фонд развития центра разработки и коммерциализации новых технологий. (2020). Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. Москва.

⁵ Bogen, M., & Rieke, A. (2018). Help wanted: an examination of hiring algorithms, equity, and bias. APO. <https://goo.su/wc44>

Работодатели, применяя такие технологии, предполагают, что инструменты ИИ объективны и поэтому могут управлять процессом принятия решений, свободным от предвзятости, которая влияет на человеческие суждения⁶, благодаря чему компании могут улучшить отбор работников, усовершенствовать их профессиональное развитие, удержание и управление эффективностью (Estrada et al., 2024). И, соответственно, логичным может показаться вывод, что риск дискриминации и необоснованного отказа в приеме на работу при использовании ИИ уменьшается, как и риск найма на работу менее квалифицированного работника.

В свою очередь, исследование М. К. Ли показывает, что, по мнению работников, справедливо, чтобы окончательное решение принимали люди, если речь идет о потенциале работников или карьерном росте. Если люди согласны с тем, что алгоритмическая система выполняет аналитические задачи (например, планирование работы), то человеческие задачи (например, прием на работу, оценка работы) должны выполняться людьми (Lee, 2018). М. Лангер и К. Дж. Кёниг отмечают, что использование технологии ИИ при найме работников в сочетании с недостатком знаний и прозрачности того, как работают алгоритмы, усиливает эмоциональную напряженность и снижает межличностное отношение и социальное взаимодействие (Langer et al., 2023). Итак, социальные исследования демонстрируют, что работники признают вспомогательную роль ИИ при найме, акцентируя внимание на важности принятия окончательного решения работодателем.

С другой стороны, исследование, проведенное Й. Бигманом, продемонстрировало, что люди меньше морально возмущены, когда решение о приеме на работу принимает алгоритм ИИ, а не человек (Bigman et al., 2023). Однако данный результат не доказывает беспристрастность алгоритма по сравнению с человеческим решением, а подтверждает лояльное отношение людей к информационным технологиям, от которых они менее ожидают необъективности, чем от человека. Кроме того, такое предположение подразумевает, что разработчики этих алгоритмов, данные, на которых строятся эти технологии, и организации, в которых они применяются, беспристрастны. Как указывают А. Кёхлинг и М. С. Вернер, в исследованиях технологий найма с использованием ИИ было установлено, что алгоритм может быть дискриминационным, однако остается открытым вопрос, являются ли алгоритмы более справедливыми, чем человек (Köchling & Wehner, 2020).

Можно констатировать, что использование для найма работников алгоритмов ИИ создает фундамент для социальных противоречий между сторонами трудовых отношений, не говоря о правовых проблемах, речь о которых пойдет ниже.

1.1. Защита персональных данных соискателя, получаемых при применении искусственного интеллекта для найма

С одной стороны, персональные данные могут быть частью обучающих данных, используемых для создания новых моделей алгоритмов путем выявления закономерностей. С другой – эти математические модели могут быть применены к персональным данным, чтобы делать выводы или прогнозы о соискателях. ИИ позволяет автоматически принимать решения на основе факторов и критериев, которые заранее

⁶ UNESCO. Artificial Intelligence: Examples of ethical dilemmas. (2023, 21 April). <https://clck.ru/3CVwHU>

не определены, а меняются в зависимости от базы данных, «питающей» алгоритм (Lukács & Váradi, 2023). То есть все функционирование системы найма работников с помощью ИИ основано на обработке персональных данных сотрудников. Поэтому очевидно, что автоматизированное принятие решений о найме на основе ИИ вступает в существенное противоречие с требованиями о защите персональных данных.

Действующее законодательство устанавливает исчерпывающий перечень документов, предъявляемых работником при найме, однако объем и виды сведений, добровольно передаваемых работодателю в процессе отбора, собеседования, законом не определены. На сегодняшний день отсутствует унифицированный перечень персональных данных, которые может использовать ИИ в процессе найма работников, а также правовой механизм контроля за их сбором, обработкой и анализом. Кроме того, законодательство не ограничивает работодателя в приемах и способах проверки деловых качеств (слово «в частности» при описании содержания понятия «деловые качества» в Постановлении Пленума Верховного Суда РФ от 17.03.2004 № 2 указывает на то, что признаки деловых качеств не имеют исчерпывающего характера). Аналогичная позиция представлена в судебной практике по делам о проведении различного, в том числе психологического, тестирования при приеме на работу для проверки деловых качеств (определение Московского городского суда от 24.02.2016 № 33-3692/16, решение Мытищинского городского суда Московской области от 21.01.2016 № 2-396/2016, определение Московского городского суда от 21.12.2017 № 33-52746/2017).

Таким образом, порядок оценки деловых качеств работника при приеме на работу нормативно не урегулирован, в связи с чем работодатель вправе самостоятельно избрать форму (в том числе с использованием ИИ), в которой он будет проводить такую оценку, и закрепить ее в локальных актах организации. Здесь также важен аспект прозрачности и согласованности проведения сбора данных о соискателе с применением ИИ, который должен оформляться отдельным соглашением.

Еще одним вектором данной проблемы является то, что персональные данные о соискателе, полученные работодателем в результате их сбора ИИ, являются конфиденциальными и не должны использоваться никаким другим образом, кроме принятия решения о найме, храниться у третьих лиц (например, разработчиков) либо им передаваться. В этом аспекте наибольший риск имеет использование «открытых» систем ИИ, таких как ChatGPT, Bard и других чат-ботов⁷. Информация, введенная в «открытую» систему ИИ, может быть непреднамеренно передана другому пользователю и сохранена в нейронной сети ИИ, чтобы использоваться для дальнейшего обучения системы. При использовании «закрытых» систем ИИ (т. е. специальных программ разработчиков) существует риск некачественных протоколов защиты и хранения данных, которые могут спровоцировать утечку и распространение персональных данных соискателей. Необходимо учитывать проблему правовых последствий несанкционированного использования персональных данных, которые работодатель получил о соискателе с помощью ИИ и которые умышленно или по неосторожности (вследствие ненадежных протоколов защиты информации) были использованы не по назначению либо переданы третьим лицам.

⁷ Markel, K. A., Mildner, A. R., & Lipson, J. L. (2023, September 29). AI and employee privacy: important considerations for employers. Reuters. <https://clck.ru/3CVwcu>

1.2. Дискриминация и необоснованность отказа в приеме на работу из-за предвзятости алгоритмов искусственного интеллекта для найма работников

Б. Ситватхару и Р. Пиллаи отмечают, что ИИ осуществляет необходимую фильтрацию кандидатов на основе различных характеристик человека, таких как предыдущий опыт, возраст, пол и квалификация (Sivathanu & Pillai, 2018). Соответственно с помощью алгоритмов машинного обучения, закодированных в ИИ, могут быть найдены закономерности или предпочтения по какой-либо из характеристик, которые не воспринимались другими людьми, включая самого субъекта данных, что в свою очередь создает почву для дискриминации при найме работников и может повысить риски необоснованных отказов в приеме на работу. В результате такой практики могут возникнуть проблемы, когда работодатели запрограммируют систему ИИ не нанимать конкретного человека или группу людей на определенную должность, а впоследствии система обучится не нанимать этого человека или данную группу людей на другие должности. Необходимо заметить, что система ИИ, созданная для найма работников, может сделать это только в том случае, если она была запрограммирована и обучена определенным образом при использовании предыдущих данных о найме. Например, Сбербанк с 2019 г. применяет скоринговый ИИ для оценки вероятности увольнений при найме соискателя. С помощью системы банк присваивает скоринг-балл кандидату и вычисляет, как скоро он решит уволиться. Система анализирует резюме соискателей, предыдущий опыт работы и другие параметры из открытых источников, согласие на использование которых предоставляет соискатель⁸.

К чему может привести использование скоринг-моделей для найма работников, хорошо проиллюстрировал случай с компанией Amazon. Данная транснациональная компания с 2015 г. не только активно задействовала ИИ для подбора сотрудников, но и уже столкнулась из-за этого с проблемами юридического характера. Алгоритм компании Amazon принимал дискриминационные решения по приему на должности исключительно мужчин, а кадровая служба данные решения не проверяла (система обучалась на резюме, представленных претендентами, получившими работу за десятилетний период, большая часть из которых были мужчинами). Дело дошло до исковых заявлений, судебных процессов, и в конечном итоге Amazon пришлось отказаться от использования ИИ для найма сотрудников⁹. Предвзятость скоринговых моделей ИИ для найма подтверждают и научные исследования. Так, Л. Чен и его коллеги подтвердили, что в поисковых системах женщины ранжируются ИИ несколько ниже, чем мужчины (Chen et al., 2018).

Итак, в зависимости от того, как настроены системы ИИ, они могут дискриминировать людей и отсеивать тех, кто им не подходит, или ранжировать резюме людей на основе несправедливых критериев, выработанных машинным обучением.

Аналогичным образом применение технологии эмоционального ИИ (Emotion AI) формирует риск дискриминации и необоснованного отказа в приеме на работу,

⁸ Сбербанк научил искусственный интеллект предсказывать увольнения. (2019, 18 октября). Forbes. <https://clck.ru/3CVwoY>

⁹ Oppenheim, M. (2018, 11 October). Amazon scraps "sexist AI" recruitment tool. Independent. <https://clck.ru/3CVwqY>

когда считывание эмоций и интонаций на собеседовании происходит путем применения видео-, аудио- и других биометрических датчиков. Как указывает О. В. Федосеева, ИИ осуществляет распознавание эмоций по мимике и считывает их с помощью оптических датчиков, которые фиксируют выражение лица в режиме реального времени либо в записи с веб-камер (Федосеева, 2021). Полученные данные обрабатываются алгоритмами машинного обучения, определяя тип микровыражений, тональность и эмоциональность голосовой реакции. В широком смысле «чтение» микровыражений лица и тональности в голосе позволяет ИИ обнаруживать эмоции потенциальных работников и осуществлять профессиональное прогнозирование.

Применяя технологию эмоционального ИИ, работодатель желает не просто удостовериться в профессиональной компетентности потенциального работника, а диагностировать его эмоциональные реакции на те или иные вопросы, связанные с трудовой деятельностью у данного работодателя (например, это могут быть мимические или интонационные реакции на вопросы о готовности работать сверхурочно, о причинах ухода с предыдущей работы и т. п.). В частности, программа VCV московских разработчиков позволяет просматривать видеоролики собеседований, а к моменту личной встречи исключить заведомо неподходящих кандидатов, предварительно оценить soft skills и соответствия ценностям компании для скоринга настроения и поведения кандидатов. Программные продукты другой московской компании, Sever.AI, дают возможность просматривать видео с ответами, анализировать изображение (внешнее поведение кандидата), звук (его речь, тембр) и текст (содержание ответов).

Исследуя риски задействования такого программного обеспечения при найме работников, сотрудники Московского технологического института провели в 2021 г. эксперимент с программами MyInterview и Curious Thing и установили, что программы по-разному считывают эмоции соискателей с разными камерами и микрофонами, при разных поворотах головы и в разных зонах экрана. Также они практически не понимают интонаций в голосе, сказанных с сильным акцентом¹⁰. Как отмечает Т. Прадип, при проведении собеседований с использованием ИИ негативно сказываются на оценке соискателя проблемы с сетевым подключением, синдром дефицита внимания или недостаточная концентрация кандидата, поэтому для принятия финального решения о трудоустройстве необходимо участие человека (Pradeep, 2024).

Как видим, поскольку инструменты ИИ управляются данными, полученными из объективной действительности, трудно, если не невозможно, избежать риска того, что инструменты ИИ закодируют и усугубят определенные предубеждения. Поэтому одной из наиболее серьезных проблем в сфере найма работников при использовании ИИ является наличие предвзятых алгоритмов – алгоритмов, приводящих к дискриминации, необъективным и незаконным решениям. М. Джексон называет предвзятыми алгоритмами предубеждения, которые ИИ может повторить при принятии решений (Jackson, 2021).

¹⁰ МТИ: ИИ-софт для проведения собеседований не понимает даже, на каком языке говорит кандидат. (2021, 8 июля). Хабр. <https://clck.ru/3CVxKF>

Основными характеристиками предвзятых алгоритмов при найме работников с использованием ИИ являются:

1) предвзятость выборки – данные, на которых учится ИИ, не точно отражают реальную картину мира. Как указывает Ж. Чен, почти каждый алгоритм машинного обучения опирается на предвзятые базы данных (Chen, 2023);

2) алгоритмическая предвзятость, которая возникает из-за алгоритма, а не из-за данных. При разработке алгоритма алгоритмическая предвзятость может быть обусловлена несколькими факторами, такими как глубина нейронной сети или предварительная информация, необходимая алгоритму. Как отмечает Ю. С. Харитонов, алгоритмическая предвзятость существует даже тогда, когда у разработчика алгоритма нет намерения дискриминации, и даже когда рекомендательная система не принимает на вход демографическую информацию (Харитонов и др., 2021);

3) предвзятость репрезентации, возникающая во время сбора данных и связанная с неравномерным сбором данных, при котором не учитываются вбросы или аномалии. Предвзятость репрезентации также может возникнуть, когда не учитывается разнообразие населения, например, данные, которые не включают все демографические группы в равной степени;

4) предвзятость измерений, проявляющаяся в неравнозначных выводах или допускающая ошибки при построении обучающего набора данных. Эти ошибки могут привести к необъективным результатам в отношении определенных демографических групп¹¹.

В целом, если при сборе и обработке данных генеративному алгоритму не хватает количества и качества по определенным характеристикам, он не сможет объективно отобразить реальность, что приведет к неизбежной предвзятости алгоритмических решений и, соответственно, принятию работодателем несправедливого и, возможно, незаконного решения об отказе в приеме на работу более достойного кандидата либо, наоборот, трудоустройству менее квалифицированного соискателя.

1.3. Юридическая ответственность за принятое искусственным интеллектом решение о найме работника

В современных исследованиях высказываются позиции, что прикладное управление ИИ уже стало способным сделать видимость того, будет ли программа посылать свои собственные решения работнику (Ivanova et al., 2018), или что нынешние информационно-социальные изменения затрагивают и трансформируют характер трудовых отношений таким образом, что личное общение субъектов отношения отходит на второй план, а личное общение будет заменено отношениями между работниками в цифровой среде (Lőrincz, 2018). Данные позиции не выдерживают критики, ведь сама идея признать систему с ИИ в качестве субъекта права противоречит таким представлениям о субъекте права, как социально-правовая ценность, достоинство, автономная правовая воля, а также вступает в противоречие с составом правоотношения, составом правонарушения и ничтожна в рамках института представительства (Хисамова, Бегишев, 2020).

¹¹ Roller, A. (2023, September 8). AI hiring bias: How HR can understand and mitigate potential pitfalls. <https://clck.ru/3CVxwT>

ИИ не может более быть участником общественных отношений, так как не имеет способности устанавливать взаимодействие между субъектами права по поводу удовлетворения материальных или культурных потребностей. Также не существует никакого общественно значимого результата, которого ИИ хотел бы достичь. Субъектов права ИИ может исключительно датифицировать под конкретные алгоритмические задачи, заданные при программировании и усовершенствованные путем машинного обучения. Поэтому признание за ИИ правосубъектности невозможно, исходя из программного свойства его взаимосвязи с внешним миром. М. Х. Джаррахи отмечает, что принятие решений на основе ИИ и человека должно дополнять друг друга (а не заменять) и использовать их сравнительные преимущества (Jarrahi, 2018). ИИ является средством автоматизации процессов найма потенциальных работников, цифровым инструментом взаимодействия между элементами производственной системы на уровне сбора, обработки, анализа и хранения информации.

Таким образом, ИИ в правовой реальности может существовать исключительно в качестве объекта права. Все решения, принятые ИИ, должны быть контролируемы и объяснимы человеком (работодателем), который и несет ответственность за их последствия. Окончательное решение о найме работника либо об отказе в приеме на работу на основе информации, полученной от ИИ, может принимать исключительно работодатель или его уполномоченный орган.

2. Зарубежный опыт нормативного регулирования использования искусственного интеллекта для найма работников

Использование технологий ИИ для оптимизации процесса принятия решений по найму работников является привлекательным для работодателей, но, как мы увидели, создает существенные правовые проблемы, которые необходимо решать на законодательном уровне. Возможность принятия нормативных актов в данной сфере пока что находится в России на уровне научных дискуссий и концептуальных разработок, поэтому актуальным представляется обращение к исследованию передового опыта зарубежных стран.

2.1. Нормативное регулирование использования искусственного интеллекта для найма работников в США

Наибольший прогресс в урегулировании отношений по найму работников с использованием ИИ демонстрируют США, где на уровне отдельных штатов уже приняты соответствующие нормативно-правовые акты.

Иллинойс стал первым штатом, принявшим закон, специально регулирующий использование работодателями ИИ для проведения собеседований с потенциальными сотрудниками. Закон Иллинойса о видеоинтервью с использованием искусственного интеллекта (Artificial Intelligence Video Interview Act) вступил в силу в январе 2020 г.¹² Данный закон требует от работодателей, которые «рассматривают кандидатов на должности, расположенные в Иллинойсе¹³», выполнить все следующие действия: прежде чем просить кандидатов предоставить видеоинтервью, уведомить

¹² Artificial Intelligence Video Interview Act (820 ILCS 42). <https://clck.ru/3CVz5D>

¹³ Там же.

соискателей о том, что работодатель может использовать ИИ для анализа видеоинтервью соискателя и оценки его соответствия работе; предоставить соискателю информацию о том, как работает ИИ и какие общие характеристики он использует для оценки соискателей; получить согласие соискателя на то, чтобы его оценивал ИИ. Закон также устанавливает, что в течение 30 дней после получения запроса от соискателя работодатель должен удалить видеоинтервью с кандидатом и проинструктировать любое лицо, получившее копию видеоинтервью, сделать то же самое, включая все резервные копии, созданные в электронном виде.

Кроме того, 9 августа 2024 г. в штате Иллинойс был принят Закон о трудоустройстве с использованием искусственного интеллекта (HB3773)¹⁴. Этот Закон, вступающий в силу 1 января 2026 года, вносит изменения в Закон о правах человека штата Иллинойс (Illinois Human Rights Act) и направлен на предотвращение дискриминационных последствий использования ИИ в процессе принятия решений при трудоустройстве. Закон требует от работодателей уведомлять об использовании ИИ для следующих целей, связанных с трудоустройством: набор персонала, прием на работу, продвижение по службе, продление трудовых отношений, отбор на обучение или стажировку, увольнение, дисциплинарное взыскание, установление срока трудового договора.

Закон штата Мэриленд, принятый в марте 2020 г.¹⁵, требует от работодателей выполнения определенных требований для использования технологии распознавания лиц при собеседовании с соискателями. Закон предписывает работодателю получить подписанное согласие от соискателей, прежде чем он сможет использовать технологию распознавания лиц «с целью создания шаблона лица» во время собеседования.

Городской совет Нью-Йорка принял 11 декабря 2021 г. местный закон № 144 об автоматизированных инструментах принятия решений о приеме на работу (Automated Employment Decision Tools), который вступил в силу 5 июля 2023 г. Согласно закону № 144, автоматизированный инструмент принятия решения о приеме на работу – это любой вычислительный процесс, основанный на машинном обучении, статистическом моделировании, анализе данных или ИИ, который выдает упрощенный результат, включая оценку, классификацию или рекомендацию, используемый для существенной помощи или замены дискреционного принятия решений о приеме на работу, которые затрагивают физических лиц. Данный закон обязывает работодателей проводить «проверку на предвзятость» любого автоматизированного инструмента принятия решения о приеме на работу перед его использованием и уведомлять работников и кандидатов, проживающих в Нью-Йорке, об использовании работодателем таких инструментов при оценке или анализе для приема на работу или продвижения по службе, а также о должностных квалификациях и характеристиках, которые будет оценивать ИИ. Также работодатели обязаны уведомить кандидатов за десять дней до использования ИИ для принятия решения о найме.

17 мая 2024 г. Совет по гражданским правам штата Калифорния опубликовал Правила по защите от дискриминации при трудоустройстве в автоматизированных системах принятия решений (Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems)¹⁶. Правила определяют автоматизированную

¹⁴ Illinois House Bill 3773 (2024, September 9). <https://clck.ru/3DcoQm>

¹⁵ Md. Code, Lab. & Empl. § 3-717. <https://clck.ru/3CVzMD>

¹⁶ Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems. (2024, 17 May). <https://goo.su/FwwU>

систему принятия решений как вычислительный процесс, в том числе основанный на машинном обучении, статистике или других методах обработки данных или ИИ, который проверяет, оценивает, классифицирует, рекомендует или иным образом принимает решение или облегчает принятие решения человеком, которое влияет на сотрудников или кандидатов. В Правилах подчеркивается, что использование автоматизированной системы принятия решений не заменяет требования об индивидуальной оценке соискателя.

Правила также вводят определение агента работодателя, включая в него любое лицо или третью сторону, которая обеспечивает администрирование автоматизированных систем принятия решений для использования работодателем при принятии решений о найме, которые могут привести к отказу в приеме на работу или иным образом негативно повлиять на условия, положения, льготы или привилегии при приеме на работу. Это означает, что работодатель несет ответственность за действия третьих лиц, которых работодатель нанимает для управления системами принятия решений, если эти системы принятия решений оказывают дискриминационное воздействие. Кроме того, Правила обязывают работодателей и все другие организации, подпадающие под действие положения, хранить любые кадровые или иные записи о трудоустройстве, «связанные с любой практикой трудоустройства и влияющие на любые трудовые преимущества любого кандидата или сотрудника (включая все заявления, кадровые, членские или рекомендательные записи или файлы, а также все данные машинного обучения)» в течение четырех лет.

17 мая 2024 г. в штате Колорадо был принят комплексный нормативный акт в сфере ИИ – Закон о защите прав потребителей при использовании искусственного интеллекта (Consumer Protections for Artificial Intelligence Act)¹⁷, в содержание которого включены нормы, касающиеся трудовых отношений. Закон, вступающий в силу 1 февраля 2026 г., распространяется как на разработчиков, так и на организации, внедряющие ИИ в свою работу, и требует проявлять «разумную осторожность», чтобы избежать дискриминационных алгоритмов. Закон направлен на «системы искусственного интеллекта высокого риска», под которыми понимаются любые системы ИИ, принимающие или являющиеся существенным фактором в принятии значимого решения, в том числе в сфере трудоустройства. Чтобы соответствовать закону, работодатели должны внедрить политику и программу управления рисками, ежегодно проводить оценку воздействия, уведомлять сотрудников или соискателей об использовании работодателем ИИ, если он используется для принятия решения в отношении работника или соискателя, сделать общедоступное заявление с кратким описанием типов систем высокого риска, которые использует работодатель. Работодатели обязаны сообщить генеральному прокурору Колорадо об обнаружении алгоритмической дискриминации в течение 90 дней с момента обнаружения.

Важную роль в продвижении потенциальных норм использования ИИ при найме работников в США исполняет Комиссия по соблюдению равноправия при трудоустройстве (EEOC). 28 октября 2021 г. EEOC выступила с «Инициативой по искусственному интеллекту и справедливости алгоритмов»¹⁸, в которой обозначила необходимость изучения практики применения ИИ при найме работников и выработки специальных руководств для работодателей, которые в последующем должны стать основой для правового регулирования на федеральном уровне.

¹⁷ Consumer Protections for Artificial Intelligence Act. (2024, 17 May). <https://clck.ru/3DcuBv>

¹⁸ EEOC Artificial Intelligence and Algorithmic Fairness Initiative. (2021, 28 October). <https://clck.ru/3CVzfn>

12 мая 2022 г. ЕЕОС выпустила руководство «Закон об американцах с ограниченными возможностями и использование программного обеспечения, алгоритмов и искусственного интеллекта для оценки кандидатов на работу и сотрудников»¹⁹. В данном руководстве ЕЕОС выделяет три наиболее распространенных способа, которыми использование работодателями ИИ может нарушать права лиц с ограниченными возможностями.

Во-первых, работодатель может нарушить права лиц с ограниченными возможностями, если потребует от соискателя с инвалидностью, мешающей ему работать руками, пройти тест на знание предмета, требующий использования клавиатуры или трекпада, без каких-либо приспособлений или альтернативной версии теста.

Во-вторых, алгоритм, который использует работодатель, может намеренно или ненамеренно отсеять человека с инвалидностью, даже если он способен выполнять работу с разумными приспособлениями. Это может произойти, например, если программное обеспечение для проведения собеседования, предназначенное для анализа навыков соискателя по решению проблем, поставит более низкие оценки кандидату на работу с дефектом речи, из-за которого программе трудно интерпретировать его ответ в соответствии с речевым шаблоном, который программа была обучена распознавать.

В-третьих, алгоритмический инструмент принятия решений, который работодатель использует для оценки кандидатов на работу, может нарушить ограничения на вопросы, связанные с инвалидностью, и медицинскими обследованиями, для лиц с ограниченными возможностями. Такое нарушение может произойти, если инструмент ИИ, который работодатель использует для оценки кандидатов, задает вопросы (напрямую) о наличии инвалидности, либо может вызвать ответ, содержащий информацию о наличии инвалидности у человека.

18 мая 2023 г. ЕЕОС издала документ «Избранные вопросы: Оценка неблагоприятного воздействия программного обеспечения, алгоритмов и искусственного интеллекта, используемых в процедурах отбора при приеме на работу»²⁰, в котором изложила свое видение дальнейшего урегулирования найма работников с использованием ИИ.

Во-первых, процесс отбора соискателей, в котором используется ИИ, может быть признан дискриминационным, если показатель отбора лиц определенной расы, цвета кожи, религии, пола или национального происхождения или комбинации таких характеристик (например, сочетание расы и пола) составляет менее 80 % от показателя незащищенной группы. Имеется в виду ситуация, схожая с уже рассмотренным случаем в компании Amazon, когда ИИ осуществил выбор кандидата, основываясь на предыдущем опыте отбора на должности, и предпочел преимущественно мужчин.

Во-вторых, работодатели несут ответственность за любое негативное воздействие, вызванное инструментами ИИ, которые приобретаются или используются сторонними поставщиками ИИ, и не могут полагаться на собственные прогнозы или

¹⁹ EEOC The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees. (2022, 12 May). <https://clck.ru/3CVzk3>

²⁰ EEOC Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964. (2023, May 18). <https://clck.ru/3CVzoG>

исследования поставщиков ИИ о том, окажут ли их инструменты ИИ негативное воздействие на соискателей. В данном случае подтверждается мысль об отсутствии правосубъектности у ИИ и возложении ответственности за принятые решения алгоритмом на работодателя.

В-третьих, работодатели должны систематически проверять инструменты ИИ, чтобы убедиться, что они не являются дискриминационными. Если существует вероятность того, что инструмент ИИ оказывает неравное воздействие, работодатель должен доказать, что использование этого инструмента связано с работой и соответствует деловой необходимости и что нет менее дискриминационных альтернатив, которые были бы столь же эффективны. Данная рекомендация ЕЕОС должна содействовать выявлению в программном обеспечении ИИ для найма работников предвзятых алгоритмов.

18 мая 2023 г. Бюро финансовой защиты потребителей (CFPB), Министерство юстиции (DOJ), Комиссия по соблюдению равноправия при трудоустройстве (ЕЕОС) и Федеральная торговая комиссия (FTC) опубликовали совместное заявление по поводу дискриминации и предвзятости²¹, в котором подчеркиваются три направления по регулированию ИИ при найме работников:

1) применение существующих правовых норм – существующие законы и нормативные акты в равной степени применимы к использованию автоматизированных систем и новых технологий, ведомства будут применять существующие правовые основы к ИИ;

2) устранение вредных последствий – ИИ может увековечить незаконную предвзятость, автоматизировать незаконную дискриминацию и привести к другим вредным последствиям, что подчеркивает необходимость бдительности при использовании ИИ в практике трудоустройства;

3) защита индивидуальных прав – обязательной является защита прав человека от дискриминационной практики ИИ.

24 апреля 2024 г. Министерство труда США (DOL) выпустило Руководство о том, как работодателям из числа федеральных подрядчиков следует вести себя при использовании ИИ для найма работников (Artificial Intelligence and Equal Employment Opportunity for Federal Contractors)²². Согласно Руководству федеральные подрядчики обязаны: обосновать необходимость использования ИИ для найма работников; проанализировать, насколько процедура отбора с помощью ИИ связана с работой; проводить мониторинг используемых программ ИИ на предмет наличия предвзятых алгоритмов; изучить потенциально менее дискриминационные альтернативные процедуры отбора соискателей. В Руководстве подчеркивается, что полное исключение человека из процесса может привести к нарушению федеральных законов о занятости. Федеральный подрядчик несет ответственность за использование продуктов и услуг третьих лиц для найма работников с применением ИИ. Также Руководство закрепляет перечень «перспективных практик», которых рекомендуется придерживаться федеральным подрядчикам: заранее уведомлять

²¹ Joint statement on enforcement efforts against discrimination and bias in automated systems. (2023, April 25). <https://clck.ru/3CVzxw>

²² Artificial Intelligence and Equal Employment Opportunity for Federal Contractors (2024, April 24). <https://clck.ru/3Dcv8d>

соискателей об использовании ИИ при найме; прозрачно прояснять соискателям политику и процедуру использования ИИ для найма; убедиться, что система ИИ, полученная от поставщика, может быть подвергнута контролю и мониторингу; проводить тестирование системы ИИ, используемую для найма работников, и приспособить ее для отдельных защищенных категорий населения; контролировать использование ИИ при принятии решений о трудоустройстве и отслеживать получаемые данные для дальнейшей стандартизации и усовершенствования алгоритмов.

2.2. Нормативное регулирование использования искусственного интеллекта для найма работников в Европейском союзе

В отличие от США, где федеральным законодательством все еще не урегулированы вопросы использования ИИ для найма работников, в Европейском союзе 21 мая 2024 г. был принят Регламент ЕС об искусственном интеллекте (Artificial Intelligence Act)²³, который предусматривает создание общей нормативной базы для использования ИИ. Данный Регламент содержит нормы, регулирующие использование ИИ в трудовых отношениях, в частности при найме работников.

Регламентом устанавливаются три категории программных продуктов (систем) ИИ, разделенных по степени риска, согласно которым осуществляется регулирование их использования: запрещенные системы (с недопустимой степенью риска); системы с высокой степенью риска; остальные системы ИИ (общего назначения, общего назначения с системными рисками). Последняя категория программных продуктов ИИ на данном этапе не подпадает под действие Регламента и специально не регулируется.

Недопустимый риск предполагает запрет применения эмоционального ИИ в процессе трудоустройства (исключение – медицинские показания и соображения безопасности), целенаправленного использования программных продуктов ИИ для выявления определенных уязвимостей (в силу возраста, инвалидности, конкретной социальной или экономической ситуации кандидатов) или категоризации людей на основе биометрических либо персональных данных (путем определения расы, политических взглядов, членства в профсоюзе, религиозных, философских убеждений соискателей). Также к запрещенным системам ИИ в контексте найма работников ст. 5 Регламента относит те, которые используют методы подсознательного либо манипулятивного воздействия с целью искажения поведения кандидата путем существенного ухудшения его способности принимать обоснованные решения; осуществляют скоринговую оценку на основе социального поведения или известных, предполагаемых или прогнозируемых личных характеристик (например, чтобы сделать прогноз о возможном увольнении работника на основе предыдущего опыта трудовой деятельности); создают или расширяют базы данных распознавания лиц посредством нецелевого извлечения изображений лиц из Интернета или видеозаписей с камер видеонаблюдения.

²³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). <https://clck.ru/3DdUr7>

К системам ИИ высокой степени риска Регламент относит программные продукты, используемые, в частности, для найма и отбора людей (размещение целевых объявлений о приеме на работу, анализ и фильтрация заявлений о приеме на работу, оценка кандидатов), для принятия решений, влияющих на условия трудовых отношений, продвижения по службе и прекращения трудовых отношений, для распределения задач на основе индивидуального поведения, личных черт или характеристик и для мониторинга или оценки людей в трудовых отношениях. По мнению авторов Регламента, эти системы ИИ могут оказать значительное влияние на будущие карьерные перспективы, средства к существованию людей и права работников, увековечивать исторически сложившиеся модели дискриминации, например, в отношении женщин, определенных возрастных групп, инвалидов, лиц определенного расового или этнического происхождения, нарушать их основные права на защиту персональных данных и неприкосновенность частной жизни²⁴.

Не рассматриваются в качестве систем высокой степени риска, согласно ст. 6 Регламента, программные продукты ИИ, если они не представляют значительного риска причинения вреда здоровью, безопасности или основным правам физических лиц, в том числе из-за отсутствия существенного влияния на результаты принятия решений, в случае выполнения одного или нескольких из следующих критериев: а) система ИИ предназначена для выполнения узкой процедурной задачи; б) система ИИ предназначена для улучшения результата ранее выполненного человеком действия; в) система ИИ предназначена для выявления моделей принятия решений или отклонений от предыдущих моделей принятия решений и не предназначена для замены или влияния на ранее проведенную человеком оценку без надлежащей проверки со стороны человека; d) система ИИ предназначена для выполнения подготовительной задачи к оценке, соответствующей целям примеров использования перечисленных в Приложении III Регламента (например, в случае предварительной каталогизации заявлений от кандидатов с помощью алгоритма ИИ).

Регламент содержит способы управления рисками для программных продуктов ИИ с высокой степенью риска. К таким способам относится: тестирование системы ИИ (идентификация и анализ прогнозируемых рисков); оценка рисков с участием и без участия нотифицированного органа (на протяжении всего жизненного цикла системы ИИ); разработка и принятие надлежащих и целенаправленных мер по управлению рисками. Управление рисками возложено на развертывателя (deployer) – лицо, использующее систему ИИ в соответствии с его полномочиями (за исключением случаев, когда система ИИ используется для личной непрофессиональной деятельности). Развертывателем может быть как работодатель, так и лицо, которое по заданию работодателя использует систему ИИ в целях отбора и найма работников.

Регламентом закрепляются обязанности развертывателей систем ИИ высокой степени риска, которые в том числе должны нивелировать потенциальные нарушения прав соискателей. Например, развертыватели обязаны обеспечить достаточную степень прозрачности работы системы ИИ высокой степени риска (то есть система

²⁴ Там же.

ИИ должна проектироваться и использоваться таким образом, чтобы позволить интерпретировать выходные данные системы и использовать их надлежащим образом); информировать соискателей и работников о том, что на них будет распространяться действие системы ИИ высокой степени риска; гарантировать надлежащий уровень точности, надежности и кибербезопасности системы ИИ высокой степени риска (системы ИИ высокой степени риска должны быть устойчивы к несанкционированным попыткам третьих лиц изменить алгоритмы их использования, результаты или производительность из-за уязвимости системы). При использовании систем ИИ высокой степени риска Регламент рекомендует не полагаться исключительно на автоматически принятые решения и задействовать людей для их финальной проверки или оценки.

Результаты работы алгоритмов, предоставляемые системами ИИ высокой степени риска при найме работников, могут быть под влиянием предубеждений, которые склонны постепенно усиливаться путем машинного обучения и тем самым закреплять и усиливать существующую дискриминацию, в частности в отношении лиц, принадлежащих к определенным уязвимым группам. Поэтому Регламент обращает внимание на недопустимость предвзятости алгоритмов в системах ИИ высокой степени риска. В частности, наборы больших данных в системах ИИ должны учитывать в той степени, в которой этого требует их целевое назначение, особенности, характеристики или элементы, свойственные конкретным географическим, контекстуальным, поведенческим или функциональным условиям, в которых предполагается использовать систему ИИ. Системы ИИ высокой степени риска, которые продолжают обучаться после ввода развертывателями в эксплуатацию, должны разрабатываться таким образом, чтобы устранить или максимально снизить риск возможного влияния предвзятости и необъективных результатов на исходные данные для будущих операций.

Таким образом, зарубежный опыт демонстрирует основные направления правового регулирования использования ИИ для найма работников, которые соответствуют ранее выделенным правовым проблемам в данной сфере: положения, касающиеся применения ИИ для найма, должны содержать требования о прозрачности и согласованности сбора, обработки и хранения информации, непредвзятости алгоритмов и их периодическом мониторинге, ответственности работодателя за решения, принятые ИИ при найме работников.

Заключение

Интенсивное внедрение ИИ в сферу управления трудом, в частности наем работников, формирует как потенциальные возможности, так и существенные риски. С одной стороны, ИИ может значительно оптимизировать и улучшить эффективность процедур по найму работников, а с другой – возникают проблемы правового характера, связанные с нарушением прав соискателей и ответственностью работодателя за ошибки алгоритмов.

Соответственно, учитывая выделенные проблемы и исследованный зарубежный опыт, для российского законодателя актуальной представляется разработка и включение в трудовое законодательство следующих положений согласно трем основным направлениям регулирования использования ИИ для найма работников.

I. Прозрачность и согласованность сбора, обработки и хранения информации при использовании ИИ для найма работников.

Глава 14 Трудового кодекса РФ (далее – ТК РФ) закрепляет нормы, касающиеся защиты персональных данных работников, в том числе относящихся к обеспечению прозрачности и согласованности сбора, обработки, хранения и использования таких данных. Разумным представляется распространение положений данной главы на соискателей и лиц, поступающих на работу, и дополнение соответствующих статей главы 14 ТК РФ такими положениями: работодатель обязан заранее письменно уведомить соискателей о том, что ИИ может быть использован для сбора, обработки и анализа их персональных данных; работодатель обязан заранее письменно уведомить соискателей об использовании ИИ для проведения и анализа видеointервью; работодатели должны объяснить, какой программный продукт ИИ используется, как он работает и какие характеристики применяются для оценки деловых качеств соискателей; соискатели должны дать свое письменное согласие на оценку их деловых качеств с помощью программного обеспечения ИИ; работодатель не имеет права передавать видеозаписи соискателя другим лицам, в том числе разработчикам программного обеспечения; работодатель обязан удалить данные, полученные ИИ о соискателе, в том числе в ходе видеointервью, в течение 15 дней после получения письменного требования от соискателя; работодатель не имеет права использовать технологию ИИ для найма инвалидов.

Перечень и объем персональных данных, который допустимо обрабатывать с помощью ИИ при найме, следует урегулировать с помощью механизма стандартизации. Необходимо заметить, что в 2020 г. Федеральным агентством по техническому регулированию и метрологии была разработана Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект» на период 2021–2024 гг., предусматривающая разработку 217 стандартов, среди которых не нашлось места стандартам в сфере использования ИИ для найма работников. В данном случае нужно учесть положения ГОСТ Р 59277-20206 от 03.01.2021, которым утвержден «Национальный стандарт системы искусственного интеллекта. Классификация систем искусственного интеллекта». Национальный стандарт системы ИИ содержит классификацию информации в зависимости от соответствия следующим классам конфиденциальности: класс «0» – открытая информация; класс «1» – внутренняя информация; класс «2» – конфиденциальная информация; класс «3» – секретная информация. Данная классификация должна позволить закодировать в системах ИИ для найма работников четкий перечень и допустимые пределы сбора информации о соискателях.

II. Непредвзятость алгоритмов ИИ для найма работников.

Крайне важно кодировать программы ИИ для найма работников так, чтобы избежать предвзятости алгоритмов и, как следствие, дискриминации и необоснованного отказа в приеме на работу. Инструментом обеспечения непредвзятости алгоритмов ИИ для найма работников может стать обязательная сертификация соответствующего программного обеспечения.

Сертификация программного обеспечения и алгоритмов ИИ на сегодняшний день не является в России обязательной, согласно Постановлению Правительства РФ от 01.12.2009 № 982 «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия

которой осуществляется в форме принятия декларации о соответствии»²⁵, где указывается, что программное обеспечение проходит подтверждение соответствия с заявленными производителем техническими условиями или государственными стандартами исключительно в добровольной системе сертификации продукции. В свою очередь, развитие систем ИИ и возникновение существенных рисков, связанных с возможным нарушением трудовых прав граждан, требует включения в перечень продукции, подлежащей обязательной сертификации, программ ИИ и машинного обучения на основе разработанных государственных стандартов, а также периодического мониторинга. Поэтому следует обязать работодателей проводить обязательный ежегодный мониторинг используемой технологии ИИ для найма и направлять отчет о проведенном мониторинге в тот центр по сертификации, где программа, которую использует работодатель, проходила сертификацию.

Также актуальным представляется рассмотрение вопроса о запрете использования работодателями даже при наличии согласия соискателя скоринговых моделей ИИ для найма работников как имеющих значительный риск предвзятости при прогнозировании трудового поведения соискателя.

III. Ответственность работодателя за принятые генеративным алгоритмом решения о найме работников.

ИИ не может обладать правосубъектностью и быть ответственным за результаты сбора, обработки и анализа данных соискателей и принятие решений о найме. Более того, данная позиция уже отображена в п. 6 ч. 1 ст. 86 действующего ТК РФ, где закрепляется, что при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Данная норма должна быть распространена также на соискателей и лиц, поступающих на работу. То есть работодатели несут ответственность за любое негативное воздействие, вызванное инструментами ИИ. Кроме того, работодатель несет ответственность за действия третьих лиц, которых работодатель нанимает для управления системами принятия решений, в том числе автоматизированными, если такие системы принятия решений оказывают дискриминационное воздействие. Последнее положение также актуально закрепить в ст. 90 ТК РФ.

Список литературы

- Новиков, Д. А. (2023). Критические замечания относительно либерального понимания в социологических и правовых исследованиях феномена труда в информационном обществе. *Ежегодник трудового права*, 13, 81–91. <https://doi.org/10.21638/spbu32.2023.105>
- Федосеева, О. В. (2021). К вопросу о создании и развитии эмоционального искусственного интеллекта. *Россия: тенденции и перспективы развития*, 16-1, 674–676.
- Харитонов, Ю. С., Савина, В. С., Паньини, Ф. (2021). Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права. *Вестник Пермского университета. Юридические науки*, 53, 488–515. <https://doi.org/10.17072/1995-4190-2021-53-488-515>
- Хисамова, З. И., Бегишев, И. Р. (2020). Сущность искусственного интеллекта и проблема определения правосубъектности. *Московский юридический журнал*, 2, 96–106. <https://doi.org/10.18384/2310-6794-2020-2-96-106>

²⁵ Постановление Правительства РФ от 01.12.2009 № 982. КонсультантПлюс. <https://clck.ru/3EPpur>

- Щербакова, О. В. (2021). Использование программ искусственного интеллекта при найме работников. *Электронное приложение к Российскому юридическому журналу*, 3, 72–76. https://doi.org/10.34076/22196838_2021_3_72
- Basu, N., & Dave, R. (2024). Artificial intelligence and job sector – need for laws. *Educational Administration: Theory And Practice*, 30(3), 690–701. <https://doi.org/10.53555/kuey.v30i3.1337>
- Bigman, Y. E., Wilson, D., Arnestad, M. N., Waytz, A., & Gray, K. (2023). Algorithmic discrimination causes less moral outrage than human discrimination. *Journal of Experimental Psychology: General*, 152(1), 4–27. <https://doi.org/10.1037/xge0001250>
- Chen, L., Ma, R., Hannák, A., & Wilson, C. (2018). Investigating the impact of gender on rank in resume search engines. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 651, 1–14. <https://doi.org/10.1145/3173574.3174225>
- Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, 10, 567. <https://doi.org/10.1057/s41599-023-02079-x>
- De Stefano, V. (2019). “Negotiating the algorithm”: automation, artificial intelligence and labor protection. *Comparative Labor Law & Policy Journal*, 41(1), 15–46. <https://doi.org/10.2139/ssrn.3178233>
- Estrada, G., Coronado, M., Soria, Y., Jiménez, S., Cristobal, J., Torres, E., Camargo, M., Taipe, M., Aparicio, S., Luis, J., & Briceño B. (2024). Inteligencia artificial en la gestión de los recursos humanos. *Revista de Climatología Edición Especial Ciencias Sociales*, 24, 2082–2092.
- Fuller, J., B. Raman M., Sage-Gavin, E., Hines, K. et al. (2021). *Hidden workers: untapped talent*. Harvard Business School Project on Managing the Future of Work and Accenture.
- GINU, G., Mary, T., Anusha, B., & Anson, M. (2021). A systematic review of artificial intelligence and hiring: Present Position and Future Research Areas. *Indian Journal of Economics and Business*, 20(2), 57–70. <http://dx.doi.org/10.5281/zenodo.5407602>
- Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, 61(4), 5–14. <https://doi.org/10.1177/0008125619864925>
- Hunkenschroer, A. L., & Kriebitz, A. (2023). Is AI recruiting (un)ethical? A human rights perspective on the use of AI for hiring. *AI Ethics*, 3, 199–213. <https://doi.org/10.1007/s43681-022-00166-4>
- Ivanova, M., Bronowicka, J., Kocher, E., & Degner, A. (2018). *The App as a Boss? Control and Autonomy in Application-Based Management: Working Paper*. Europa-Universität Viadrina Frankfurt. <https://doi.org/10.11584/arbeit-grenze-fluss.2>
- Jackson, M. (2021). Artificial intelligence & algorithmic bias: the issues with technology reflecting history & humans. *Journal of Business & Technology Law*, 16(2), 299–316.
- Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577–586. <https://doi.org/10.1016/j.bushor.2018.03.007>
- Köchling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic preview of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 13, 795–848. <https://doi.org/10.1007/s40685-020-00134-w>
- Kuncel, N., Klieger, D., & Ones, D. (2014). In hiring, algorithms beat instinct. *Harvard Business Review*, 92(5), 32.
- Langer, M., Cornelius, J. K., & Andromachi, F. (2023). Information as a double-edged sword: the role of computer experience and information on applicant reactions towards novel technologies for personnel selection. *Computers in Human Behavior*, 81, 19–30. <https://doi.org/10.1016/j.chb.2017.11.036>
- Langer, M., König, C. J., Sanchez, D. R.-P., & Samadi, S. (2019). Highly automated interviews: applicant reactions and the organizational context. *Journal of Managerial Psychology*, 35(4), 301–314. <https://doi.org/10.1108/jmp-09-2018-0402>
- Lee, M. K. (2018). Understanding perception of algorithmic decisions: fairness, trust, and emotion in response to algorithmic management. *Big Data & Society*, 5(1), 1–16. <https://doi.org/10.1177/2053951718756684>
- Lőrincz, G. (2018). Kommentár a munka törvénykönyvéről szóló 2022. évi I. törvényhez: Munkajogi sci-fi. *Pécsi Munkajogi Közlemények*, 11(1-2), 7–34.
- Lukács, A., & Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, 50, 105848. <https://doi.org/10.1016/j.clsr.2023.105848>
- Pradeep, T. (2024). Labour law in the era of artificial intelligence and automation. *International Journal For Multidisciplinary Research*, 6(2). <https://doi.org/10.36948/ijfmr.2024.v06i02.16324>
- Reddy, S. (2022). The legal issues regarding the use of artificial intelligence to screen social media profiles for the hiring of prospective employees. *Obiter*, 43(2), 113–131. <https://doi.org/10.17159/obiter.v43i2.14254>
- Serova, A. V., & Shcherbakova, O. V. (2022). The employee’s right to privacy transformation: digitalization challenges. *Kutafin Law Review*, 9(3), 437–465. <https://doi.org/10.17803/2713-0525.2022.3.21.437-465>
- Sivathanu, B., & Pillai, R. (2018). Smart HR 4.0 – how industry 4.0 is disrupting HR. *Human Resource Management International Digest*, 26(4), 7–11. <https://doi.org/10.1108/hrmid-04-2018-0059>

Сведения об авторе



Новиков Денис Александрович – кандидат юридических наук, доцент, доцент кафедры трудового и социального права, Санкт-Петербургский государственный университет

Адрес: 199034, Россия, г. Санкт-Петербург, Университетская наб., 7–9

E-mail: d.novikov@spbu.ru

ORCID ID: <https://orcid.org/0000-0003-2727-5357>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57218897105>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/CAA-7871-2022>

Google Scholar ID: <https://scholar.google.com/citations?user=gEjH4S4AAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149154

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.63.33 / Трудовые ресурсы. Трудоустройство

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

История статьи

Дата поступления – 6 августа 2023 г.

Дата одобрения после рецензирования – 22 августа 2023 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:349.2:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.31>

Using Artificial Intelligence in Employment: Problems and Prospects of Legal Regulation

Novikov Denis A.

Saint Petersburg State University, Saint Petersburg, Russia

Keywords

algorithm,
artificial intelligence,
digital technologies,
employee,
employer,
hiring of an employee,
labor law,
law,
legislation,
personal data

Abstract

Objective: to identify the legal problems of using artificial intelligence in hiring employees and the main directions of solving them.

Methods: formal-legal analysis, comparative-legal analysis, legal forecasting, legal modeling, synthesis, induction, deduction.

Results: a number of legal problems arising from the use of artificial intelligence in hiring were identified, among which are: protection of the applicant's personal data, obtained with the use of artificial intelligence; discrimination and unjustified refusal to hire due to the bias of artificial intelligence algorithms; legal responsibility for the decision made by a generative algorithm during hiring. The author believes that for the optimal solution of these problems, it is necessary to look at the best practices of foreign countries, first of all, those which have adopted special laws on the regulation of artificial intelligence for hiring and developed guidelines for employers using generative algorithms for similar purposes. Also, the European Union's and USA's legislative work in the area of managing risks arising from the use of artificial intelligence should be taken into account.

Scientific novelty: the article contains a comprehensive study of legal problems arising from the use of artificial intelligence in hiring and foreign experience in solving these problems, which allowed the author to develop recommendations to improve Russian legislation in this area. As for the problem of applicants' personal data protection when using artificial intelligence for hiring, the author proposes to solve it by supplementing the labor legislation with norms that enshrine the requirements for transparency and consistency in the collection, processing and storage of information

© Novikov D. A., 2024

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.

when using generative algorithms. The list and scope of personal data allowed for collection should be reflected in a special state standard. The solution to the problem of discrimination due to biased algorithms is seen in the mandatory certification and annual monitoring of artificial intelligence software for hiring, as well as the prohibition of scoring tools for evaluating applicants. The author adheres to the position that artificial intelligence cannot “decide the fate” of a job seeker: the responsibility for the decisions made by the algorithm is solely on the employer, including in cases of involving third parties for the selection of employees.

Practical significance: the obtained results can be used to accelerate the development and adoption of legal norms, rules, tools and standards in the field of using artificial intelligence for hiring. The lack of adequate legal regulation in this area creates significant risks both for human rights and for the development of industries that use generative algorithms to hire employees.

For citation

Novikov, D. A. (2024). Using Artificial Intelligence in Employment: Problems and Prospects of Legal Regulation. *Journal of Digital Technologies and Law*, 2(3), 611–635. <https://doi.org/10.21202/jdtl.2024.31>

References

- Basu, N., & Dave, R. (2024). Artificial intelligence and job sector – need for laws. *Educational Administration: Theory And Practice*, 30(3), 690–701. <https://doi.org/10.53555/kuey.v30i3.1337>
- Bigman, Y. E., Wilson, D., Arnestad, M. N., Waytz, A., & Gray, K. (2023). Algorithmic discrimination causes less moral outrage than human discrimination. *Journal of Experimental Psychology: General*, 152(1), 4–27. <https://doi.org/10.1037/xge0001250>
- Chen, L., Ma, R., Hannák, A. & Wilson, C. (2018). Investigating the impact of gender on rank in resume search engines. *Proceedings of the 2018 chi conference on human factors in computing systems*, 651, 1–14. <https://doi.org/10.1145/3173574.3174225>
- Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, 10. <https://doi.org/10.1057/s41599-023-02079-x>
- De Stefano, V. (2019). “Negotiating the algorithm”: automation, artificial intelligence and labor protection. *Comparative Labor Law & Policy Journal*, 41(1), 15–46. <https://doi.org/10.2139/ssrn.3178233>
- Estrada, G., Coronado, M., Soria, Y., Jiménez, S., Cristobal, J., Torres, E., Camargo, M., Taipe, M., Aparicio, S., Luis, J., & Briceño B. (2024). Inteligencia artificial en la gestión de los recursos humanos. *Revista de Climatología Edición Especial Ciencias Sociales*, 24, 2082–2092. (In Spanish).
- Fedoseeva, O. V. (2021). On creating and developing emotional artificial intelligence. *Rossiia: tendencii i perspektivy razvitiya*, 16-1, 674–676. (In Russ.).
- Fuller, J., B. Raman M., Sage-Gavin, E., Hines, K. et al. (2021). *Hidden workers: untapped talent*. Harvard Business School Project on Managing the Future of Work and Accenture.
- GINU, G., Mary, T., Anusha, B., & Anson, M. (2021). A systematic review of artificial intelligence and hiring: Present Position and Future Research Areas. *Indian Journal of Economics and Business*, 20(2), 57–70. <http://dx.doi.org/10.5281/zenodo.5407602>
- Haenlein, M. & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, 61(4), 5–14. <https://doi.org/10.1177/0008125619864925>
- Hisamova, Z. I., & Begishev, I. R. (2020). The nature of artificial intelligence and the problem of legal personality determination. *Moscow Juridical Journal*, 2, 96–106. (In Russ.). <https://doi.org/10.18384/2310-6794-2020-2-96-106>

- Hunkenschroer, A. L., & Kriebitz, A. (2023). Is AI recruiting (un)ethical? A human rights perspective on the use of AI for hiring. *AI Ethics*, 3, 199–213. <https://doi.org/10.1007/s43681-022-00166-4>
- Ivanova, M., Bronowicka, J., Kocher, E., & Degner, A. (2018). *The App as a Boss? Control and Autonomy in Application-Based Management: Working Paper*. Europa-Universität Viadrina Frankfurt. <https://doi.org/10.11584/arbeitsgrenze-fluss.2>
- Jackson, M. (2021). Artificial intelligence & algorithmic bias: the issues with technology reflecting history & humans. *Journal of Business & Technology Law*, 16(2), 299–316.
- Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577–586. <https://doi.org/10.1016/j.bushor.2018.03.007>
- Kharitonova, Yu. S., Savina, V. S., & Pagnini, F. (2021). Artificial intelligence's algorithmic bias: ethical and legal Issues. Perm University Herald. *Juridical Sciences*, 53, 488–515. (In Russ.). <https://doi.org/10.17072/1995-4190-2021-53-488-515>
- Köchling, A., & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic preview of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 13, 795–848. <https://doi.org/10.1007/s40685-020-00134-w>
- Kuncel, N., Klieger, D., & Ones, D. (2014). In hiring, algorithms beat instinct. *Harvard Business Review*, 92(5), 32.
- Langer, M., Cornelius, J. K., & Andromachi, F. (2023). Information as a double-edged sword: the role of computer experience and information on applicant reactions towards novel technologies for personnel selection. *Computers in Human Behavior*, 81, 19–30. <https://doi.org/10.1016/j.chb.2017.11.036>
- Langer, M., König, C. J., Sanchez, D. R.-P., & Samadi, S. (2019). Highly automated interviews: applicant reactions and the organizational context. *Journal of Managerial Psychology*, 35(4), 301–314. <https://doi.org/10.1108/jmp-09-2018-0402>
- Lee, M. K. (2018). Understanding perception of algorithmic decisions: fairness, trust, and emotion in response to algorithmic management. *Big Data & Society*, 5(1), 1–16. <https://doi.org/10.1177/2053951718756684>
- Lőrincz, G. (2018). Kommentár a munka törvénykönyvéről szóló 2032. évi I. törvényhez: Munkajogi sci-fi. *Pécsi Munkajogi Közlemények*, 11(1-2), 7–34. (In Hungarian)
- Lukács, A., & Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, 50, 105848. <https://doi.org/10.1016/j.clsr.2023.105848>
- Novikov, D. A. (2023). Critical remarks on the liberal understanding in sociological and legal studies of the phenomenon of labour in the information society. *Russian Journal of Labour & Law*, 13, 81–91. (In Russ.). <https://doi.org/10.21638/spbu32.2023.105>
- Pradeep, T. (2024). Labour law in the era of artificial intelligence and automation. *International Journal For Multidisciplinary Research*, 6(2). <https://doi.org/10.36948/ijfmr.2024.v06i02.16324>
- Reddy, S. (2022). The legal issues regarding the use of artificial intelligence to screen social media profiles for the hiring of prospective employees. *Obiter*, 43(2), 113–131. <https://doi.org/10.17159/obiter.v43i2.14254>
- Serova, A. V., & Shcherbakova, O. V. (2022). The employee's right to privacy transformation: digitalization challenges. *Kutafin Law Review*, 9(3), 437–465. <https://doi.org/10.17803/2713-0525.2022.3.21.437-465>
- Shcherbakova, O. V. (2021). The use of artificial intelligence programs when recruiting employees. *Electronic Supplement to the Russian Juridical Journal*, 3, 72–76. (In Russ.). https://doi.org/10.34076/22196838_2021_3_72
- Sivathanu, B., & Pillai, R. (2018). Smart HR 4.0 – how industry 4.0 is disrupting HR. *Human Resource Management International Digest*, 26(4), 7–11. <https://doi.org/10.1108/hrmid-04-2018-0059>

Author information



Denis A. Novikov – Cand. Sci. (Law), Associate Professor, Department of Labor and Social Law, Saint Petersburg State University

Address: 7–9 Universitetskaya nab., 199034 Saint Petersburg, Russia

E-mail: d.novikov@spbu.ru

ORCID ID: <https://orcid.org/0000-0003-2727-5357>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57218897105>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/CAA-7871-2022>

Google Scholar ID: <https://scholar.google.com/citations?user=gEjH4S4AAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149154

Conflict of interests

The author declares no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – August 6, 2023

Date of approval – August 22, 2023

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:349.2:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.32>

Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии

Фотиос Спайропулос

Университет Филипс, Никосия, Кипр
Spyropoulos Law Firm, Афины, Греция

Ключевые слова

искусственный интеллект,
киберпреступность,
право,
преступление,
преступность,
техноэтика,
цифровая криминология,
цифровое общество,
цифровые технологии,
этика

Аннотация

Цель: опираясь на современные научные подходы к «цифровому обществу» и новые подходы в криминологии, выявить и определить цифровую криминологию, направленную на изучение возможных способов использования искусственного интеллекта преступниками, в том числе в рамках так называемой ИИ-преступности.

Методы: проблемы связи искусственного интеллекта с преступностью в «гибридном мире» переосмысливаются в статье преимущественно с учетом междисциплинарности, на уровне которой аргументы подкрепляются соответствующими отсылками к «цифровой криминологии» и ее небинарному образу мышления в рамках техносоциального подхода, несистематического обзора литературы.

Результаты: в исследовании отмечается, что в цифровом обществе технологии интегрируются в жизнь людей, включая сферы преступности, виктимизации и правосудия, стирая границы между онлайн-и офлайн-реальностью, создавая гибридный мир человека и технологий, где преступления происходят в виртуальных сетях. Показано, что искусственный интеллект обладает потенциалом для достижения целей социального благополучия и устойчивого развития, однако необходимо учитывать риски, связанные с нарушением прав человека. Обосновывается необходимость междисциплинарного подхода для обеспечения безопасного использования технологий, борьбы с неравенством в сфере образования, помощи в осуществлении правосудия и распознавании девиантного или преступного поведения в сети. Подчеркивается, что в контексте зарождающейся техноэтики пока отсутствует или, скорее, находится в процессе формирования идея о том, что эта неофициальная норма, основанная на обыденных представлениях, станет «опорным камнем» для характеристики опосредованного онлайн-поведения как девиантного или преступного.

© Спайропулос Ф., 2024

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

Научная новизна: в статье с точки зрения техноэтики выдвигается ряд подходов к феномену использования информационно-коммуникационных технологий в преступных целях под влиянием искусственного интеллекта. При этом отмечены социальные вызовы, возникающие в результате технологических сбоев (например, прогнозирование и предотвращение преступлений путем трансформации деятельности органов охраны правопорядка, усиления наблюдения и практики уголовного правосудия) в «цифровом обществе».

Практическая значимость: идеи, лежащие в основе данного исследования, могут быть использованы при разработке предложений по внесению изменений и дополнений в действующее уголовное законодательство, а также в педагогической деятельности, особенно при реализации образовательных курсов или модулей по проблемам преступности в контексте цифровой трансформации общества.

Для цитирования

Спайропулос, Ф. (2024). Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии. *Journal of Digital Technologies and Law*, 2(3), 636–656. <https://doi.org/10.21202/jdtl.2024.32>

Содержание

Введение

1. Искусственный интеллект: проблемы определения
2. Подходы к техноэтике
3. Достижения, пробелы и вызовы этики искусственного интеллекта
4. Задачи и перспективы криминологии в «гибридном» мире
 - 4.1. Терминология и типология ИИ-преступности
 - 4.2. Подход техноэтики к проблеме ИИ-преступности

Заключение

Список литературы

Введение

Многочисленные и разнообразные пути проникновения цифровых технологий в повседневную жизнь в последние годы позволяют сделать вывод о том, что теперь «жизнь стала цифровой». «Мы все больше становимся субъектами цифровых данных, нравится нам это или нет, согласны мы на это или нет» (Lupton, 2015b).

Более того, в цифровую эпоху мы наблюдаем все более широкое использование технологий и искусственного интеллекта (далее – ИИ) для решения различных задач, а также повышения производительности и эффективности. На протяжении десятилетий ученые в области компьютерных наук были настолько очарованы неограниченным потенциалом новых технологий, что негативные последствия этих систем, по всей видимости, преуменьшались, а зачастую и вовсе игнорировались (Hayward & Maas, 2020)¹. Этот подход, известный под названием «технооптимизм»

¹ Schneier, B. (2008, March 20). Inside the twisted mind of the security professional. *Wired*. <https://clck.ru/3CzSKg>

(Danaher, 2022), отличается неспособностью эффективно сбалансировать выгоды и риск, что отражалось в Кодексе Google с его прежним лозунгом «Не причини зла»².

Однако в последнее время ученые используют ряд новых исследовательских подходов, рассматривая возможные изменения преступности под воздействием того, что Greenfield (2017) выразительно назвал «радикально новыми технологиями и ИИ сетевой эры».

Специалисты в области технологий и криминалистики сегодня осознают, что системы искусственного интеллекта открывают множество новых возможностей для серьезной преступности, а также позволяют применять сомнительные методы работы полиции (Hayward & Maas 2020; Ionescu et al., 2020; Broadhurst et al., 2019). В частности, увеличение числа преступлений, совершаемых в цифровом мире, доказывает, что быстро развивающиеся технологии создают новые возможности для преступников и в то же время способствуют повышению уровня и сложности преступлений³ (Lee & Chua, 2023; Di Nicola, 2022). При этом еще не изучены многие социальные проблемы, возникающие в связи с технологическими изменениями (например, прогнозирование и предупреждение преступлений путем трансформации деятельности полиции, усиления наблюдения и практики уголовного правосудия) (Brown, 2006a; Hayward, 2012; Holt & Bossler, 2014).

1. Искусственный интеллект: проблемы определения

Дать определение понятию «искусственный интеллект» непросто; это явление кажется уже распространенным, но в то же время оно четко не определено. В популярной культуре и новостных репортажах об ИИ часто фигурируют причудливые сюжеты с участием пресловутых «роботов-убийц» или систем наблюдения, как в антиутопиях (Hayward & Maas, 2020). Однако в повседневной жизни ИИ действует на гораздо более прозаическом уровне, управляя всем – от «умных» телевизоров до приложений – переводчиков с иностранных языков. По словам К. Пайпера, «в разговорах об ИИ много путаницы, дезинформации, непонимания – во многом потому, что мы используем термин ИИ для обозначения множества различных понятий»⁴.

Граница между тем, что считается собственно ИИ, и другими технологиями размыта. Более того, термин «интеллект» в контексте парадигмы ИИ – это сложное и глубоко неоднозначное философское и научное понятие. О нем не упоминают, когда приводят философские и технические аргументы в спорах о том, удастся ли когда-нибудь разработать ИИ, обладающий сознанием и достаточно сложный, чтобы мы беспокоились о его нравственности и защищали ее (Boddington, 2017). Возможно, нас смущает именно общий и неопределенный характер этого явления; не в последнюю очередь это происходит потому, что каждый предполагаемый вариант будущего ИИ вызывает свой ряд вопросов, связанных с безопасностью, этикой, законностью и ответственностью.

² Mayer, D. (2016). Why Google Was Smart To Drop Its 'Don't Be Evil' Motto. Fast Company.

³ Ife, C. C., Davies, T., Murdoch, S. J., & Stringhini, G. (2019). Bridging information security and environmental criminology research to better mitigate cybercrime. arXiv preprint arXiv:1910.06380. <https://clck.ru/3CzSMo>

⁴ Piper, K. (2018). The case for taking AI seriously as a threat to humanity, Vox. <https://clck.ru/3CzSPd>

Так называемый аспект «двойного назначения» технологий – не новая проблема, когда речь идет о киберпреступности или (кибер-)безопасности. Хотя ИИ может использоваться для атак на государственные структуры, правительства также применяют его для расширения своих возможностей. Однако появляются новые уязвимости, так как возникают злоупотребления и злонамеренное использование технологий. Одно из законных применений ИИ – это системы для предотвращения и обнаружения преступлений (Dilek et al., 2015; Li et al., 2010; Lin et al., 2017; McClendon & Meghanathan, 2015), но существует также вероятность злоупотребления этой технологией и использования ее для незаконной деятельности (Kaloudi & Li, 2020; Sharif et al., 2016; Mielke & Chen, 2008; van der Wagen & Pieters, 2015). Важнейшей проблемой является использование злоумышленниками систем, не относящихся к искусственному сверхинтеллекту, для автоматизации, обеспечения и расширения масштабов киберпреступлений известных типов, а также появление совершенно новых возможностей для киберпреступлений.

Для того чтобы общество смогло решить эту проблему, необходимо дать четкие ответы на простые вопросы: «Что именно представляет собой ИИ?», «Каковы его возможности и пределы?» и «Каковы последствия его распространения и использования в обществе как в качестве инструмента для достижения преступных или незаконных целей, так и в качестве средства обеспечения безопасности и социального контроля?»

2. Подходы к техноэтике

Термин «техноэтика» был предложен в 1974 г. аргентино-канадским философом Mario Bunge (Bunge, 1977) для обозначения особой ответственности технологов и инженеров за развитие этики как отрасли технологии.

«Этику можно определить как кодекс или набор принципов, по которым живут люди. Этика говорит о том, что считается морально правильным и что считается неправильным. Когда люди выносят моральные суждения, они делают не описательные заявления о том, что сделано, а нормативные или предписывающие заявления о том, что должно быть сделано, о моральном долге и обязательствах. Таким образом, этическая теория или моральная философия – это учение о правилах или принципах, лежащих в основе моральных решений, обоснование моральных суждений. Применение этической теории может помочь пользователям, вплоть до определения того, как люди должны вести себя в различных областях применения технологий.

Соответственно, техноэтика – это междисциплинарная область, задача которой – определить соответствующее отношение или систему взглядов на применение технологий в реальных жизненных ситуациях. Среди ряда этических теорий, наиболее актуальных для сферы применения технологий, можно выделить последовательный, деонтологический и утилитарный подходы. Техноэтика занимается изучением влияния этики на технологии, технологические изменения, технологический прогресс и их прикладные аспекты. Это относится как к устоявшимся областям, таким как биоэтика, компьютерная этика или инженерная этика, так и к новым направлениям исследований, таким как нейроэтика (Heller, 2012).

Rosci Luppiciни подчеркивает: «...техноэтика основана на предпосылке, что крайне важно развивать диалог, направленный на определение этического использования технологий, защиту от их неправильного применения и разработку продуманных принципов, которые помогут направлять новые технологические достижения на благо общества в различных социальных контекстах и этических измерениях» (Luppiciни, 2008).

Следует сказать, что техноэтика – это быстро развивающаяся область этики, обусловленная стремительным развитием технологий и их интеграцией в повседневную жизнь. Она использует обширные знания из таких научных направлений, как информация и коммуникации, общественные науки, технические и естественно-научные дисциплины, прикладная этика и философия. Задача техноэтики – выявить этические преимущества технологий, защитить от их неправильного использования и наметить общие принципы, которые приведут за собой новые достижения в области развития и применения технологий на благо общества.

Отвечая на вопрос, зачем нам нужны техноэтика и технологическое сознание, можно сказать следующее. С развитием технологий искусственного интеллекта и машинного обучения мы, несомненно, столкнемся с технологиями, которые будут способны учиться и творить, иметь собственное сознание. Поэтому нам необходимо обратиться к вопросам технологического сознания и техноэтики, чтобы найти ответы на возникающие моральные дилеммы, связанные с технологиями, и направить эти развивающиеся технологии таким образом, чтобы они приносили пользу человечеству, ведь любой алгоритм можно использовать как во благо, так и во зло.

3. Достижения, пробелы и вызовы этики искусственного интеллекта

Технологический прогресс всегда находится в центре динамики экономической системы, прямо или косвенно влияя на все виды экономической и производственной деятельности. Происходящие значительные изменения вызывают соответствующие перемены в целом ряде видов производственной и экономической деятельности. В то же время они выступают мощным фактором возникновения дисбаланса, появления новых или воспроизводства существующих примеров неравенства и несправедливости как на уровне рынка труда, структуры занятости и экономики, так и на уровне социально-экономического развития экономик, секторов, регионов и стран на европейском и международном уровнях.

Вопросы, возникающие в связи с развитием технологий, и в частности, с развитием искусственного интеллекта, все больше занимают ученых, компании и государственные органы. Так, совместная работа исследовательского отдела компании Dell Technologies и Института будущего привела к выводу, что «зависимость людей от машин перерастет в отношения сотрудничества, в которые люди привнесут такие качества, как креативность, целеустремленность и предприимчивость»⁵.

Когда говорят об этических проблемах и вызовах, связанных с технологиями и искусственным интеллектом, обычно подразумевается, что речь идет о чем-то плохом с моральной точки зрения. И конечно, большая часть дебатов об ИИ вращается вокруг морально проблематичных эффектов, для которых необходимо найти решение. Однако стоит подчеркнуть, что технологии и новые достижения в области ИИ сулят многочисленные выгоды (Berendt, 2019)⁶. Во многих программных доку-

⁵ Barbaschow, A. (2019, October 8). Machines as consumers: The future according to Dell Technologies. ZDNET.

⁶ Faggella, D. (2020). Everyday examples of artificial intelligence and machine learning. Boston, MA: Emerj. <https://clck.ru/3CzSZw>

ментах, посвященных ИИ, основное внимание уделяется экономическим преимуществам ИИ, которые, как ожидается, будут обусловлены достижением более высоких уровней эффективности и производительности. Это этические ценности, поскольку они обещают увеличение благосостояния, что позволит людям жить лучше и, таким образом, будут способствовать или даже станут необходимыми для процветания человека (см. подробнее: Экспертная группа высокого уровня ЕС по ИИ⁷).

Однако в последнее время обещания повысить эффективность, снизить затраты и ускорить исследования и разработки сменились опасениями, что эти сложные, непрозрачные системы могут принести человечеству больше вреда, чем пользы. Этические проблемы ИИ неоднократно описывались; в основном такие работы развивают давнюю традицию обсуждения этики и ИИ в научной литературе (Coeckelbergh, 2019; Dignum, 2019; Müller, 2020), но все чаще рассматривают эту проблему также с точки зрения политики⁸. Самыми известными вопросами в области этики являются следующие: а) нарушение конфиденциальности данных; б) раскрытие чувствительной информации; в) дезинформация и дипфейки; г) отсутствие надзора и принятия ответственности; д) использование ИИ (распознавание лиц, потеря рабочих мест, отслеживание состояния здоровья, проверка достоверности данных, усиление существующих предубеждений, отсутствие объяснимости и интерпретируемости и т. д.).

Таким образом, важно подчеркнуть, что правовые и этические проблемы, с которыми сталкивается общество в связи с появлением искусственного интеллекта, включают аспекты соблюдения приватности, надзора, предвзятости и дискриминации, а также потенциально затрагивают философский вопрос о роли человеческого суждения. В результате использования новых цифровых технологий возникают опасения по поводу того, что они могут стать источником неточностей и утечек данных. Поэтому необходимо принимать фундаментальные решения, чтобы обеспечить защиту личных свобод и надлежащее использование данных.

Опасения (оправданные или неоправданные) возникают в связи с распространением машин с искусственным «суперинтеллектом». Но реальная опасность заключается не в доминировании сверхинтеллектуальных машин, а в том, что они еще недостаточно «умны», чтобы справиться с поставленными перед ними задачами. Интеллект машин будет продолжать совершенствоваться, но, по крайней мере, в обозримом будущем уровня человеческого интеллекта они не достигнут. В результате усилится потребность в человеческих навыках и ценностях, чтобы преодолеть разрыв и смягчить риски, создаваемые мощным искусственным интеллектом в современных сложных человеческих сообществах. Ключом к устранению таких рисков является инвестирование в человеческий капитал и его развитие, а также осуществление ответственного мониторинга искусственного интеллекта. Это позволит поддерживать доверие общества к этой технологии. Среди моральных ценностей машин с искусственным интеллектом человеческие ценности часто отсутствуют. Чтобы добиться их соответствия, человек должен владеть обеими, поставив первые (ценности машин) на службу вторым (человеческим

⁷ EU's High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. Brussels: European Commission. <https://clck.ru/3CzSbj>

⁸ Ibid.

ценностям). Не нужно обвинять ИИ в моральных промахах человечества. «Зеркало искусственного интеллекта» является полезным инструментом для диагностирования общества; с его помощью люди могут многое узнать о его слабостях и ограничениях, а также о новых открытиях и решениях, которые он предлагает. Будущее искусственного интеллекта и человеческого общества будет решаться не за людей, а людьми. ИИ и роботы не должны решать за человека, но человек должен решать, что правильно, а что нет.

В последнее время в общественных науках стало популярным понятие «цифровое общество». Это общество, характеризующееся беспрецедентно быстрым прохождением потока информации через глобальные сети. Но самая важная особенность цифрового общества заключается в том, что оно рассматривает эти технологии как неотъемлемую часть более крупной социальной структуры и признает, что цифровые технологии, медиа и сети включены в нашу повседневную жизнь (Lupton, 2015a, 2015b), в том числе в части совершения преступлений, виктимизации и правосудия. В частности, Baun (2015) отмечает, что отличительной чертой цифровых технологий является то, как они изменили взаимодействие людей друг с другом. Такое переплетение цифрового и социального также называют цифровизацией общества, при которой «технология – это общество, а общество невозможно понять или представить без его технологических инструментов» (Castells, 1996).

С другой стороны, цифровая криминология относится к быстро развивающейся научной области, которая применяет криминологические, социальные, культурологические теории, теорию технических систем и соответствующие методы исследования для изучения преступности, делинквентного/девиантного поведения и правосудия в цифровом обществе (Stratton et al., 2017). Более того, она заново пересматривает криминологические теории в поисках новых научных идей, бросая вызов классическим дихотомиям: Интернет против физического мира, виртуальное против реального – как для предотвращения, так и для противодействия преступности в цифровой среде, в Интернете, а также в целом в контексте новых технологий, в контексте развития техноэтики. Таким образом, цифровая криминология расширяет границы современной криминологической теории и исследований, а более широкое и непрерывное обсуждение технологий, социальности, преступности, девиантности и правосудия способствует формированию новых концептуальных основ и эмпирических направлений в киберпространстве и в картировании цифровой преступности.

4. Задачи и перспективы криминологии в «гибридном» мире

Хотя прошло уже более пятнадцати лет с начала широкого распространения социальных сетей, появления дополненной реальности и искусственного интеллекта, большая часть криминологических исследований по-прежнему традиционно фокусируется на информационных системах и интернет-технологиях, рассматривая их либо как объекты преступлений, либо как инструменты для совершения других традиционных преступлений (Hayward & Maas, 2020; Holt & Bossler, 2014). Более того, многие подходы основываются на внутреннем дуализме, т. е. киберпреступность по-прежнему рассматривается как зеркальная или сетевая версия своих аналогов в физическом мире, отличаясь от них средствами совершения и пространственными масштабами, но не сущностью и характером (Grabosky, 2001).

4.1. Терминология и типология ИИ-преступности

В попытке определить место ИИ в криминологии, в соответствующей научной литературе можно встретить такие термины, как «киберпреступность на основе ИИ» (Wang, 2020), «ИИ-киберпреступность» (Hoanca & Mock, 2020), «ИИ-преступность» (King et al., 2020), «вредоносный ИИ» (Hibbard, 2015; Johnson & Verdicchio, 2017), «злонамеренный ИИ»⁹, «злонамеренное использование и злоупотребление ИИ» (Blauth et al., 2022) и др.

По мнению большинства исследователей, использование ИИ может способствовать развитию существующих форм преступности («киберпреступность») или появлению новых форм преступности («киберзависимая преступность») (Akdemir & Lawless, 2020; Grabosky, 2001). ИИ потенциально позволяет совершать атаки, которые по своим масштабам и охвату превосходят те, которые ранее были возможны при использовании других технологий (Blauth, et al., 2022). Поэтому предпочтительнее использовать термин «преступление с использованием ИИ», поскольку такие возможности существуют как в сфере киберпреступности (пересекаясь с традиционными терминами кибербезопасности), так и в других сферах (причем некоторые из этих угроз возникают как продолжение существующей преступной деятельности, а другие являются новыми). Термин «ИИ-преступление», предложенный в работе King et al. (2020) для описания ситуации, когда ИИ-технологии используются для совершения действий, которые уже определены как преступные в соответствующем законодательстве, напротив, следует считать слишком узким для создания широкой типологии, которая не ограничивается деяниями, являющимися преступлением в любом государстве. Например, создание и распространение дезинформации или ложных сведений может расцениваться как нанесение вреда по некоторым национальным законам, но необязательно является уголовным преступлением. Поэтому понятие «злонамеренное использование и злоупотребление» ИИ (King et al., 2020)¹⁰ служит очень интересной альтернативой.

В рамках этого широкого спектра вариантов Hoanca & Mock (2020) разделяют киберпреступность с использованием ИИ на три крупные, слабо пересекающиеся области: использование ИИ для совершения киберпреступлений в Интернете, использование ИИ через новые каналы киберпреступности с выходом в физическое пространство и использование ИИ или знаний об ИИ для атаки на другие системы искусственного интеллекта путем искажения данных или алгоритмов. Эти области во многом пересекаются, и степень их пересечения будет расти. В то же время, пытаясь расширить криминологическую парадигму за счет учета «связи между технологиями и преступностью» Hayward и Maas (2020), квалифицируют использование термина «преступное использование ИИ» и выделяют три категории: (1) преступления с использованием искусственного интеллекта, (2) преступления по отношению к ИИ и (3) преступления, совершенные искусственным интеллектом. По их мнению, ИИ относится к первой категории «ИИ-преступности», являясь мощным инструментом

⁹ Yampolskiy, R. V. (2016). Taxonomy of pathways to dangerous AI. arXiv:1511.03246v2, 143–148. <https://clck.ru/3CzVKL>

¹⁰ Ciancaglini, V. (2020). Malicious uses and abuses of artificial intelligence. Trend Micro Research. United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol's European Cybercrime Centre (EC3). <https://clck.ru/3CzSmK>

для «злонамеренного» преступного использования путем внедрения новых угроз или изменения внутренних характеристик уже существующих. Современные угрозы могут распространяться в физической среде¹¹. Атаки, направленные на обман или «обход» системы ИИ, использующие уязвимости системы и проводя обратный инжиниринг, относятся ко второй категории «ИИ-преступности» – преступлениям «по отношению к ИИ». Уже давно существует возможность «испортить» данные, используемые для обучения системы. Известно, что, после того как пользователи завалили чат-бот «Тэй» от Microsoft Twitter¹² массой фраз правого толка, он за один день стал расистским¹³. В третьей категории «ИИ-преступности» – «преступления, совершенные искусственным интеллектом» – важнейшим аспектом является актуальный вопрос о правовом статусе ИИ и его потенциальном использовании в качестве «криминального прикрытия/пособника». Примером такой ситуации, по мнению Hayward & Maas (2020), является дело группы художников, которые в 2015 г. опубликовали в даркнете бота для совершения различных покупок; в результате бот стал покупать наркотики и был арестован швейцарской полицией¹⁴.

4.2. Подход техноэтики к проблеме ИИ-преступности

Понимание этических аспектов различных типов технологий затрудняется тем, что в академических кругах существует тенденция к созданию информационных групп в отдельных областях и дисциплинах. Техноэтика (далее – ТЭ) помогает объединить отдельные области знания вокруг общей темы (в нашем случае это технологии, а именно ИИ). Она является целостной по своей природе и представляет объединяющее понятие для всех областей прикладной этики, которые фокусируются на человеческой деятельности, связанной с технологиями, включая экономику, политику, глобализацию, здравоохранение и медицину, а также научные исследования и разработки. ТЭ предлагает изменить, в сущности, представление человека о себе и его взгляд на реальность. Здесь кроются самые глубокие причины провала технико-научной парадигмы, которая не учитывает ни природу человека, ни природу живых существ в целом. Мы должны отказаться от технонауки, которая подразумевает примат науки над технологией, и принять новую реляционную парадигму, основанную на постмодернизме. Техноэтика возникла из необходимости противостоять тенденции, присущей большей части технологий, а именно тенденции отделять технологии от свободы и вместо этого утвердить технологию как духовную деятельность, выдающийся продукт человеческого духа и признать ее движущей силой, а не просто реципиентом теоретических разработок в области этики. Можно сказать, что основной вклад техноэтики заключается в рассмотрении новых этических проблем.

¹¹ См. также Brundage, M., Avin, S., Clark, J. et al. (2018). The malicious use of artificial intelligence. <https://clck.ru/3CzSuH>

¹² Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

¹³ Gershgorn, D. (2016). Here's how we prevent the next racist chatbot. Popular Science. <https://clck.ru/3CzSxm>

¹⁴ См. также Kasperkevic, J. (2015). Swiss police release robot that bought ecstasy online. The Guardian. <https://clck.ru/3CzSzB>

Поэтому неудивительно, что многие современные дискуссии о технологическом прогрессе ведутся в рамках ТЭ. Таким образом, они неизбежно поднимают важные вопросы о соблюдении прав человека, неприкосновенности частной жизни, ответственности и рисках, и на эти вопросы необходимо дать надлежащий ответ. Более того, в отличие от традиционной прикладной этики, которая делает акцент на этическом отношении к живым существам, ТЭ является «биотехноцентричной».

В научных дискуссиях возможные преступления с использованием ИИ в основном подразделяются на три открытые категории в зависимости от связи между преступностью и ИИ:

- преступления против ИИ (например, взлом устройств, защищенных системой распознавания лиц);
- ИИ для предотвращения преступлений (например, выявление мошеннических операций на финансовых рынках);
- ИИ для совершения преступлений (например, шантаж людей с помощью дипфейков) (Caldwell et al., 2020).

Как в исследованиях в области искусственного интеллекта, так и в практике регулирования проявляется стремление достичь баланса между преимуществами инноваций и возможным нанесением вреда или нарушениями. В последнее время исследования в области ИИ переживают всплеск активности. Однако одним из непреднамеренных последствий этого процесса является потенциальная переориентация технологий ИИ на содействие преступным действиям, т. е. ИИ-преступность (иными словами, теоретическая возможность создания ИИ была осуществлена благодаря опубликованным экспериментам по автоматизации мошенничества по отношению к пользователям социальных сетей, а также демонстрации манипуляций ИИ на моделях рынка)^{15, 16} (Nguyen et al., 2015). Важность ИИ-преступности как отдельного явления еще не получила признания. Исследование этических и социальных последствий ИИ сосредоточивается на вопросах регулирования и контроля использования ИИ в гражданских целях, тогда как работы, касающиеся ИИ-преступности, делаются в рамках самых разных дисциплин, включая социально-правовые исследования, информатику, психологию, робототехнику и т. д. Недостаточное число работ, посвященных ИИ-преступности, подрывает возможности для формирования прогнозов и решений относительно новой области – преступной деятельности, совершаемой ИИ. Это касается возможности новых преступлений в категории «преступлений белых воротничков» (LoPucki, 2017), а также поднимает вопросы о правосубъектности ИИ и вызывает опасения по поводу использования таких машин в качестве «посредников», их уголовной ответственности. В частности, речь идет о тех случаях, когда ограничения моделей ответственности подрывают правовую определенность, т. е. когда агенты, искусственные или нет, совершают преступные действия или бездействие, но условия ответственности за конкретное преступление недостаточны для того, чтобы привести к уголовной ответственности (King et al., 2020; Bayern, 2016; Williams, 2017; McAllister, 2018).

¹⁵ Huang, S., Papernot, N., Goodfellow, I., Duan, Y., & Abbeel, P. (2017). Adversarial attacks on neural network policies. arXiv preprint arXiv:1702.02284. <https://clck.ru/3CzT6s>

¹⁶ Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. <https://clck.ru/3CzT8m>

Таким образом, техноэтический подход поднимает важнейшие проблемы и вопросы, требующие рассмотрения, а также опасения по поводу дестабилизации концепций. основополагающей концепцией уголовного права, которая подвергается дестабилизации, является идея уголовной ответственности. ИИ как «независимый» посредник в преступлении ставит серьезные вопросы о базовых правовых нормах, таких как намеренно совершенное преступление (*actus reus*), преступный умысел (*mens rea*) и различные вопросы о пороге осведомленности. Вторая концепция, которая, вероятно, подвергается пересмотру, – это важность социального контроля, идея демократических ценностей и пределы защиты государством прав человека. Речь идет о масштабируемом, всеобъемлющем, неизбежном наблюдении и потенциальном использовании ИИ и робототехники для обеспечения правопорядка¹⁷ (Zardiashvili et al., 2019), включая критический анализ того, как в рамках демократии обеспечить подотчетность прогностической деятельности полиции, основанной на машинном обучении. Концепция скрытого государственного управления включает повсеместное, но негласное наблюдение, беспилотники с ИИ и датчики «умных городов». Новые формы «широкого наблюдения» являются вездесущими, но при этом тонкими, негласными и скрытыми (Hayward & Maas, 2020). Концепция государства-оракула состоит в следующем: от обнаружения и ликвидации нарушений закона к их прогнозированию и предотвращению с помощью систем ИИ, которые должны улавливать тонкие закономерности и делать (предположительно) точные прогнозы будущего поведения, в том числе преступного (Danaher, 2022).

Однако, когда мы обращаем основное и исключительное внимание на киберпространство, непосредственно и однозначно ссылаясь на Интернет и технологии «виртуального или искусственного интеллекта» (категории киберпреступности, которые легко однозначно отличить от соответствующих категорий в «не-киберпространстве»), мы можем упустить из виду разнообразные проявления внутренней природы цифровых данных и коммуникаций (Jaishankar, 2008). В современных условиях сдвиги в цифровой среде являются результатом динамической взаимосвязи характеристик технологии и ее использования (Goldsmith & Brewer, 2014). «Стремление к репрезентации» девиантного «виртуального я» (Yar, 2012) тесно связано с более широкими тенденциями: как самосоздания субъектности с помощью новых коммуникационных платформ, так и искусственного интеллекта – способности машин думать, общаться и принимать решения способами, которые раньше были возможны только для человека (сетевая реальность, сетевая совместимость, сетевое содержание и др.)¹⁸.

В свете этих проблем S. Brown (2006a) предлагает создать цифровую криминологию, которая выходит за рамки традиционной и обращается к «техно-социальным теориям» (Latour, 1993; Lash, 2002; Haraway, 1987, 1991; Castells, 2001), поскольку одной из особенностей цифровых технологий является то, как они изменили способы взаимодействия между людьми (Baym, 2015). По ее мнению, важно отметить, что анализ киберпреступности, вероятно, чересчур нацелен на абсолютные различия между «виртуальной» и «воплощенной, реальной» преступностью, а понимание «новой»

¹⁷ Interpol and UNICRI. (2019). Artificial Intelligence and Robotics for Law Enforcement. <https://clck.ru/3CzTGP>

¹⁸ Institute for the Future (ITF). (2019). Future of connected living – augmented humans in a networked world: Research Report. <https://clck.ru/3CzTPY>

киберпреступности опирается почти исключительно на метафоры и «перенос» «старых» правовых и теоретических подходов (Aas, 2007; Hayward, 2012; Wood, 2016). В криминологии «нет видения критичности природы мира как гибрида человека и техники...» (Brown, 2006b), в котором все преступления происходят в сетях, отличающихся только степенью виртуальности/реальности (воплощения). Поэтому криминологи сегодня должны рассматривать преступление и преступность на стыке биологии и технологии, природы и общества, объекта и действующего субъекта, искусственного разума и человека. Не следует сводить изучение киберпреступности к технологиям и сетям как средствам распространения информации, расширяющим преступные возможности. Сегодня ученые предлагают «понимать цифровую/сетевую (преступную) деятельность как процессы, т. е. явления, находящиеся в постоянном диалоге и изменении с другими явлениями/технологиями в гибридном мире человека и технологий» (Brown, 2006a).

Заключение

Эпоха разрозненных подходов и дихотомий, вероятно, подходит к концу. Возможно, настало время для синергии, особенно на междисциплинарном уровне. Зачем цепляться за дихотомии, если мы можем гармонизировать подходы и перспективы? И все это в контексте «цифрового общества», которое признает технологии частью более широкой социальной структуры и допускает интеграцию цифровых технологий, медиа и сетей в жизнь человека, включая преступность, виктимизацию и правосудие.

В исследовании Байм (2015) подробно показано размывание границ между онлайн- и офлайн-реальностью; отмечается, что главной особенностью цифровых технологий является то, что они изменили способ взаимодействия людей друг с другом в сетевой реальности, в мире, который теперь воспринимается как гибрид человека и технологии (Brown, 2006a), где все преступления происходят в сетях, отличающихся только степенью виртуальности/воплощенности.

Более того, все вопросы, возникающие при использовании этой технологии, не являются чисто техническими, а затрагивают широкий спектр научных и ненаучных областей, и ее безопасное использование невозможно обеспечить без междисциплинарного подхода.

Искусственный интеллект обладает огромным потенциалом для использования в целях достижения социального благополучия и устойчивого развития. Несмотря на то, что он может решить многие важнейшие социальные проблемы человечества, его применение также вызывает беспокойство в связи с нарушением прав человека, таких как право на свободу выражения мнений, право на неприкосновенность частной жизни, защиту данных, отсутствие дискриминации. Технологии на основе ИИ открывают широкие возможности, если они разрабатываются с соблюдением универсальных норм, этики и стандартов, а также опираются на ценности, основанные на правах человека и принципах устойчивого развития. Например, надежный и прозрачный искусственный интеллект может стать эффективным средством для устранения неравенства в образовательном процессе, поскольку с его помощью можно создавать программы, адаптированные к потребностям учащихся, и повышать скорость обучения.

Кроме того, искусственный интеллект может сыграть важную роль в сфере правосудия, создавая автоматизированные судебные системы, а также в области юриспруденции в целом. Например, в сфере уголовного правосудия использование систем искусственного интеллекта для оказания помощи в проведении расследований и автоматизации процессов принятия решений уже применяется во многих судебных системах по всему миру.

В контексте зарождающейся техноэтики отсутствует (или, скорее, находится в процессе формирования) идея о том, что эта неофициальная норма, основанная на убеждениях людей, поможет квалифицировать действия в сети как девиантные или криминальные.

Моральные ценности машин с искусственным интеллектом слишком часто не соответствуют более широкому человеческим ценностям. Чтобы примирить их между собой, человек должен добиться господства над обеими и поставить первые (ценности машин) на службу вторым (человеческим ценностям). ИИ не может отвечать за моральное несовершенство человека. Через «зеркало искусственного интеллекта», которое является полезным диагностическим инструментом для общества, люди могут узнать больше о его недостатках и ограничениях, а также о новых открытиях и решениях, которые он предлагает. Будущее искусственного интеллекта и человеческого общества будет решаться не за людей, а самими людьми.

Список литературы

- Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.
- Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, 30(6), 1665–1687. <https://doi.org/10.1108/intr-10-2019-0400>
- Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, 7(1), 297–309. <http://dx.doi.org/10.1017/S1867299X00005729>
- Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.
- Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, 10, 44–65. <https://doi.org/10.1515/pjbr-2019-0004>
- Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, 10, 77110–77122. <https://doi.org/10.1109/access.2022.3191790>
- Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.
- Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.3407779>
- Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223–244. <https://doi.org/10.1177/1362480606063140>
- Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.
- Bunge, M. (1977). Towards a Technoethics. *Monist*, 60(1), 96–107.
- Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, 9(1), 1–13. <https://doi.org/10.1186/s40163-020-00123-8>
- Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.
- Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.
- Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, 2019, 31–34. <https://doi.org/10.26116/techreg.2019.003>
- Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, 35(54), 8. <https://doi.org/10.1007/s13347-022-00550-2>
- Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09457-y>

- Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
- Dilek, S., Cakir, H., & Aydin, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, 6(1), 21–39. <https://doi.org/10.5121/ijaia.2015.6102>
- Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, 19(1), 112–130. <https://doi.org/10.1177/1362480614538645>
- Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243–249. <https://doi.org/10.1177/a017405>
- Greenfield, A. (2017). *Radical Technologies*. London: Verso.
- Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, 2(4), 1–42. <https://doi.org/10.1080/08164649.1987.9961538>
- Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
- Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, 17(2), 1–25. <https://doi.org/10.1177/1741659020917434>
- Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, 52(3), 441–462. <https://doi.org/10.1093/bjc/azs008>
- Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, 3(1), 14–27. <https://doi.org/10.4018/jte.2012010102>
- Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
- Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
- Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20–40. <https://doi.org/10.1080/01639625.2013.822209>
- Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, 27(2), 55–61. <https://doi.org/10.1109/mmul.2020.2994403>
- Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
- Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, 27(4), 575–590. <https://doi.org/10.1007/s11023-017-9417-6>
- Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, 53(1), 1–34. <https://doi.org/10.1145/3372823>
- King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 26(1), 89–120. <https://doi.org/10.1007/s11948-018-00081-0>
- Lash, S. (2002). *Critique of Information*. London: Sage.
- Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
- Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, 70(9), 2250–2277. <https://doi.org/10.1177/00111287231180093>
- Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, 37(10), 7108–7119. <https://doi.org/10.1016/j.eswa.2010.03.004>
- Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. <https://doi.org/10.1109/iiiai-aaai.2017.46>
- LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities*. *Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
- Luppici, R. (2008). The Emerging Field of Technoethics. In R. Luppici, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. <https://doi.org/10.4018/9781605660226.ch001>
- Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, 17(4), 440–453. <https://doi.org/10.1080/13691058.2014.920528>
- Lupton, D. (2015b). *Digital Sociology*. 1st ed. London & New York: Routledge.
- McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, 101, 2527–2573.

- McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, 2(1), 1–12. <https://doi.org/10.5121/mlaij.2015.2101>
- Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. <https://doi.org/10.1109/isi.2008.4565058>
- Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.
- Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition*, 7–12 June, 427–436. <https://doi.org/10.1109/cvpr.2015.7298640>
- Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. <https://doi.org/10.1145/2976749.2978392>
- Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, 6(2), 17–33. <https://doi.org/10.5204/ijcjsd.v6i2.355>
- van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, 55(3), 578–595. <https://doi.org/10.1093/bjc/azv009>
- Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, 1533(3), 032014. <https://doi.org/10.1088/1742-6596/1533/3/032014>
- Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.
- Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's¹⁹ technological unconscious. *Theoretical Criminology*, 21(2), 1–18. <https://doi.org/10.1177/1362480616643382>
- Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, 8(3), 245–260. <https://doi.org/10.1177/1741659012443227>
- Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, 2(4), 179–185. <https://doi.org/10.21552/delphi/2019/4/7>

¹⁹ Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Сведения об авторе



Фотиос Спиropулос – научный сотрудник, PhD, доцент в области уголовного права и криминалистики, факультет права, Университет Филиппс; старший партнер юридической компании Spyropoulos Law Firm

Адрес: Кипр, 28008, г. Никосия, ул. Ламияс, 4-6; Греция, 11474, г. Афины, Александрас авеню, 81

E-mail: fspyropoulos@gmail.com

ORCID ID: <https://orcid.org/0000-0001-5950-3583>

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

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.81 / Криминология

Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 30 апреля 2024 г.

Дата одобрения после рецензирования – 15 мая 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:349.2:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.32>

New Approaches to Researching AI Crime: Institutionalization of Digital Criminology

Fotios Spyropoulos

Philips University, Nicosia, Cyprus

Spyropoulos Law Firm, Athens, Greece

Keywords

artificial intelligence,
crime,
criminal deed,
cybercrime,
digital criminology,
digital society,
digital technologies,
ethics,
law,
technoethics

Abstract

Objective: the article deals with modern scientific approaches to the “digital society”, identifies new criminological perspectives, such as that of digital criminology in an ever-changing hybrid world, in the scientific study of the potential use of AI by criminals, including what is referred to here as AI crime.

Methods: this article is an essay commonly used in humanities and social sciences, as the author aims to present provocative arguments to encourage readers to rethink AI issues in relation to criminality in the “hybrid world” based on a non-systematic literature review. The arguments should be supported by relevant references to “digital criminology” and its non-binary way of thinking in favour of a techno-social approach.

Results: the era of divided perspectives is coming to an end, and it's time for synergies, especially at the interdisciplinary level. The «mirror of artificial intelligence» can help identify flaws and solutions, ensuring the future of AI and human society is decided by the people. In a digital society, technology is integrated into people's lives, including crime, victimization, and justice. Digital technologies blur the boundaries between online and offline realities, creating a human-technological hybrid world where crimes occur in virtual networks. AI has potential for social good and Sustainable Development Goals, but concerns about human rights violations need to be addressed. Multidisciplinary approaches are needed to ensure safe use, address education inequalities, enhance justice, and identify online behavior as deviant or criminal. In the context of emerging technoethics, the idea that this unofficial norm, derived from a popular belief, will be the ‘touchstone’ for characterising online mediated behaviour as deviant/criminal, is missing - or rather in the process of being formed.

© Spyropoulos F., 2024

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 aims to provide some insightful thoughts on formulating the right questions and interesting reflections from a technoethical perspective on the phenomenon of the use of information and communication technologies for criminal purposes under the catalytic influence of AI, recognising the social challenges arising from technological disruption (e.g. prediction and prevention through the transformation of policing, increased surveillance and criminal justice practises) in “digital society”.

Practical significance: some of the initial ideas of this theoretical material can be used in the elaboration of proposals for amendments and additions to the current crime legislation, as well as in pedagogical activity, especially in the implementation of educational courses or modules on crime in the context of the digital transformation of society.

For citation

Spyropoulos, F. (2024). New Approaches to Researching AI Crime: Institutionalization of Digital Criminology. *Journal of Digital Technologies and Law*, 2(3), 636–656. <https://doi.org/10.21202/jdtl.2024.32>

References

- Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.
- Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, 30(6), 1665–1687. <https://doi.org/10.1108/intr-10-2019-0400>
- Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, 7(1), 297–309. <http://dx.doi.org/10.1017/S1867299X00005729>
- Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.
- Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, 10, 44–65. <https://doi.org/10.1515/pjbr-2019-0004>
- Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, 10, 77110–77122. <https://doi.org/10.1109/access.2022.3191790>
- Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.
- Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. <http://dx.doi.org/10.2139/ssrn.3407779>
- Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223–244. <https://doi.org/10.1177/1362480606063140>
- Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.
- Bunge, M. (1977). Towards a Technoethics. *Monist*, 60(1), 96–107.
- Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, 9(1), 1–13. <https://doi.org/10.1186/s40163-020-00123-8>
- Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.
- Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.
- Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, 2019, 31–34. <https://doi.org/10.26116/techreg.2019.003>
- Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, 35(54), 8. <https://doi.org/10.1007/s13347-022-00550-2>
- Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09457-y>

- Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
- Dilek, S., Cakir, H., & Aydin, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, 6(1), 21–39. <https://doi.org/10.5121/ijaia.2015.6102>
- Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, 19(1), 112–130. <https://doi.org/10.1177/1362480614538645>
- Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243–249. <https://doi.org/10.1177/a017405>
- Greenfield, A. (2017). *Radical Technologies*. London: Verso.
- Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, 2(4), 1–42. <https://doi.org/10.1080/08164649.1987.9961538>
- Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
- Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, 17(2), 1–25. <https://doi.org/10.1177/1741659020917434>
- Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, 52(3), 441–462. <https://doi.org/10.1093/bjc/azs008>
- Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, 3(1), 14–27. <https://doi.org/10.4018/jte.2012010102>
- Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
- Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
- Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20–40. <https://doi.org/10.1080/01639625.2013.822209>
- Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, 27(2), 55–61. <https://doi.org/10.1109/mmul.2020.2994403>
- Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
- Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, 27(4), 575–590. <https://doi.org/10.1007/s11023-017-9417-6>
- Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, 53(1), 1–34. <https://doi.org/10.1145/3372823>
- King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 26(1), 89–120. <https://doi.org/10.1007/s11948-018-00081-0>
- Lash, S. (2002). *Critique of Information*. London: Sage.
- Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
- Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, 70(9), 2250–2277. <https://doi.org/10.1177/00111287231180093>
- Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, 37(10), 7108–7119. <https://doi.org/10.1016/j.eswa.2010.03.004>
- Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. <https://doi.org/10.1109/iiiai-aaai.2017.46>
- LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities*. *Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
- Luppici, R. (2008). The Emerging Field of Technoethics. In R. Luppici, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. <https://doi.org/10.4018/9781605660226.ch001>
- Lupton, D. (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, 17(4), 440–453. <https://doi.org/10.1080/13691058.2014.920528>
- Lupton, D. (2015). *Digital Sociology*. 1st ed. London & New York: Routledge.
- McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, 101, 2527–2573.

- McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, 2(1), 1–12. <https://doi.org/10.5121/mlaij.2015.2101>
- Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. <https://doi.org/10.1109/isi.2008.4565058>
- Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.
- Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition*, 7–12 June, 427–436. <https://doi.org/10.1109/cvpr.2015.7298640>
- Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. <https://doi.org/10.1145/2976749.2978392>
- Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, 6(2), 17–33. <https://doi.org/10.5204/ijcjsd.v6i2.355>
- van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, 55(3), 578–595. <https://doi.org/10.1093/bjc/azv009>
- Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, 1533(3), 032014. <https://doi.org/10.1088/1742-6596/1533/3/032014>
- Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.
- Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's¹ technological unconscious. *Theoretical Criminology*, 21(2), 1–18. <https://doi.org/10.1177/1362480616643382>
- Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, 8(3), 245–260. <https://doi.org/10.1177/1741659012443227>
- Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, 2(4), 179–185. <https://doi.org/10.21552/delphi/2019/4/7>

¹ The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation

Author information



Fotios Spyropoulos – PostDoc, PhD, Associate Professor of Criminal Law & Criminology, Faculty of Law, Philips University; Senior Partner of Spyropoulos Law Firm

Address: 4-6 Lamias Street, 2001, P.O. Box 28008, Nicosia, Cyprus; Alexandras Avenue 81, 11474, Athens, Greece

E-mail: fspyropoulos@gmail.com

ORCID ID: <https://orcid.org/0000-0001-5950-3583>

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

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – April 30, 2024

Date of approval – April 15, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:343.9:004.4

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

DOI: <https://doi.org/10.21202/jdtl.2024.33>

Новостная криминология в XXI веке: формирование общественного мнения в новых реалиях

Валентина Андреевна Бабаева

Московский государственный институт международных отношений (университет)

Министерства иностранных дел Российской Федерации, Москва, Россия

Ключевые слова

Интернет,
криминология,
новостная криминология,
право,
правоохранительный орган,
правосудие,
преступность,
средство массовой
информации,
цифровые технологии,
цифровое общество

Аннотация

Цель: исследование концепции новостной криминологии и ее актуальности в современных условиях развития средств массовой информации.

Методы: методологическую основу работы составляют общенаучные, социальные, специально-юридические методы познания. Проведенное исследование основано на диалектическом методе (при определении общего направления исследования), методах формальной логики (анализ, синтез, индукция, дедукция, аналогия), системном методе (при сопоставлении и обобщении информации, собранной в процессе исследовательской деятельности).

Результаты: выявлены функции новостной криминологии в классическом ее проявлении, а также ее дополнительные функции при изучении медиа в интернет-пространстве. Высказано предположение, что с появлением Всемирной сети актуальность новостной криминологии повысилась: социальные сети, блоги и видеохостинги как альтернативные средства массовой информации имеют сильное влияние на общественное мнение, при этом в отличие от традиционных средств массовой информации доступ к генерации контента имеет неограниченный круг лиц. Многие государства понимают важность взаимодействия средств массовой информации и правоохранительных органов и активно внедряют свои методы реализации новостной криминологии в сети. Автор статьи указывает на риски, возникающие при освещении материалов о правоохранительных органах и преступности в СМИ. Одним из таких рисков является культура отмены, которая носит стихийный, непредсказуемый характер, при котором может пострадать качество жизни жертвы или деловая репутация и деятельность организаций.

© Бабаева В. А., 2024

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: определены функции, выполняемые новостной криминологией при изучении традиционных и альтернативных медиа. До настоящего времени такая доктрина не была исследована в достаточной мере с учетом современных форм массовой коммуникации. Проведен анализ примеров взаимодействия правоохранительных органов разных государств и средств массовой информации.

Практическая значимость: исследование вносит вклад в область понимания корреляции между криминологическими явлениями и современными медийными платформами. Интернет и социальные сети предоставляют новые каналы информационного обмена, которые существенно отличаются от традиционных средств массовой информации, таких как печать или телевидение.

Для цитирования

Бабаева, В. А. (2024). Новостная криминология в XXI веке: формирование общественного мнения в новых реалиях. *Journal of Digital Technologies and Law*, 2(3), 657–673. <https://doi.org/10.21202/jdtl.2024.33>

Содержание

Введение

1. Классическая новостная криминология

2. Новостная криминология в XXI веке

3. Культура отмены как криминологический феномен

Заключение

Список литературы

Введение

Взаимодействие между сотрудниками правоохранительных органов и средствами массовой информации (далее – СМИ) имеет амбивалентную природу и вызывает особый интерес для исследователей природы такого взаимоотношения с точки зрения криминологии. СМИ имеют колоссальное влияние на общественное мнение, что может как снизить уровень доверия правоохранительных органов среди населения и способствовать развитию стереотипов о том или ином преступном феномене, так и наоборот. Осуществляя сотрудничество, правоохранительные органы и средства массовой информации могут предоставлять общественности точную и достоверную информацию об инцидентах, расследованиях и деятельности правоохранительных органов, освещать вопросы общественной безопасности и повышать осведомленность о стратегиях предотвращения преступности. Такое сотрудничество играет ключевую роль для обеспечения общественной безопасности, установления доверия и облегчения эффективного общения с обществом, что в перспективе способствует укреплению позитивных отношений между правоохранительными органами и общественностью, обеспечивая при этом распространение точной и своевременной информации.

В 1988 г. Грегг Барак впервые ввел термин «новостная криминология». Данная научная доктрина изучает особенности взаимодействия правоохранительных органов и СМИ, влияние СМИ на общественное мнение о сотрудниках правоохранительных органов.

и криминогенной обстановке в стране. Новостная криминология является подвигом так называемой публичной криминологии – особого подхода к криминологии, в рамках которого ученые распространяют результаты своих исследований в данной сфере за пределы академических кругов для более широкой аудитории.

В данной статье рассматривается концепция новостной криминологии через призму современных правовых реалий. Эпоха цифровизации охватывает все сферы жизни общества, включая и средства массовой информации. Автор данной концепции рассматривал новостную криминологию, учитывая традиционные СМИ, т. е. радио, телевидение, газеты и т. д. Сообщество, сформировавшееся во Всемирной сети Интернет, стало новой формой средств массовой информации, взаимодействие с которыми стало намного более сложным процессом, чем предполагалось при взаимодействии с традиционными СМИ. Социальные процессы в сети Интернет являются более стихийными и непредсказуемыми, что имеет ряд определенных рисков.

1. Классическая новостная криминология

Криминологи часто критикуют средства массовой информации за эмоциональность повествования, искажение фактов и чрезмерное упрощение, которые они привносят в вопросы преступности и правосудия. Данный феномен вызван социальными и техническими достижениями СМИ: их способностью воспроизводить и создавать контент, а также их влиянием на многие аспекты социальной и культурной жизни. СМИ способны создавать общественное мнение, определять взгляды отдельных лиц и целых социальных групп (Сысоев, 2007). С этой точки зрения мощные формы коммуникации создают нереалистичные образы преступности и избегают рационального осмысления данных феноменов. Центральное место в этой критике занимает концепция медиа как процесса коммуникации и лежащих в его основе понятий (Arrigo & Bersot, 2015; Stout & Clamp, 2015; Gore et al., 2020; De Melo Bandeira, 2013; Cotee, 2004).

Новостная криминология – это сознательная деятельность криминологов по изучению репрезентации преступности и уголовного правосудия в СМИ, а также взаимодействие с представителями СМИ в целях формирования «достойного освещения» материалов о преступности и правосудии (Barak, 1988).

Несмотря на сходство терминов «новостная криминология» и «криминология СМИ», между ними присутствуют определенные отличия. Криминология средств массовой коммуникации является концепцией, направленной на анализ причин и закономерностей преступности в множестве массовых коммуникаций и информационного обмена в целом (Горшенков, 2003). Так, новостную криминологию можно отнести к подвидам криминологии СМИ.

Новостная криминология охватывает ряд проблем освещения процесса отправления правосудия в СМИ, что оказывает непосредственное влияние на представления граждан о правоохранительных органах или преступности в целом. Так, основоположник данной концепции указывает на отсутствие надлежащего уровня образования среди участников соответствующих программ, выполняющих просветительскую функцию. Например, в программы на тему экономики и политики приглашаются специалисты данных научных отраслей, тогда как криминологические передачи испытывают недостаток специалистов в этой сфере (Barak, 2007). Отсутствие экспертного мнения в этих материалах можно объяснить ограничениями

по времени и их информационно-развлекательным характером: немногие эксперты могут вывести обсуждение проблемы за рамки «звуковых фрагментов», «тезисов для обсуждения» в рамках повествования (Frost & Phillips, 2011). Новостная криминология движима морально-политической мотивацией информировать аудиторию СМИ и развеять заблуждения о преступности и правосудии (Richards et al., 2020).

Отношения между системой уголовного правосудия и системой СМИ были предметом исследований, спекуляций и комментариев на протяжении всего XX в. Такие отношения можно назвать симбиотическими: система уголовного правосудия является ценным ресурсом для системы СМИ, поскольку сведения о недавно совершенных преступлениях и ходе судебных разбирательств по таким делам пользуются спросом у аудитории. В поисках нового материала СМИ отслеживают новейшие тенденции в обществе на предмет реальных и потенциальных угроз индивидуальному и коллективному благополучию. Многие журналистские расследования и разоблачения способствуют выявлению латентных правонарушений, а своевременно обнародованные сведения позволяют предотвратить готовящиеся преступления (Шамаев, 2018). Взаимодействие средств массовой информации и правоохранительных органов является важным инструментом борьбы с преступностью. Оно позволяет влиять на различные сферы жизни общества. Так, новостная криминология ставит перед собой ряд функций (Ozkan, 2019).

Во-первых, аналитическая функция новостной криминологии заключается в изучении репрезентации преступности отправления уголовного правосудия в средствах массовой информации. Она анализирует содержание, оформление и наличие предвзятости в новостях, помогая выявить закономерности и тенденции в освещении преступности в СМИ.

Во-вторых, новостной криминологией исследуется формирование общественного мнения и восприятие целевой аудиторией преступности и процесса отправления уголовного правосудия. Новостная криминология изучает то, как повествование в СМИ влияет на общественное мнение, формирует страх или стереотипы относительно тех или иных феноменов или криминогенных факторов. Она также рассматривает более широкие социальные последствия репрезентации преступности и уголовного правосудия, например, как СМИ влияют на доверие общества к тем или иным социальным институтам и стигматизацию определенных групп и сообществ.

В-третьих, новостная криминология рассматривает этические последствия практики СМИ при освещении преступлений. Данная функция рассматривает такие аспекты, как дезинформация, неполное освещение всех фактов уголовного дела и т. д. Грегг Барак акцентировал внимание на репрезентации преступности средствами массовой информации в одномерном и искаженном формате. Так, до общественности доносятся лишь самые «интересные» материалы, которые в теории должны привлечь большую аудиторию и принести новостным телеканалам или газетам прибыль, в то время как другие социальные проблемы могут игнорироваться или искажаться.

В-четвертых, новостная криминология имеет просветительскую функцию. Специфика концепции новостной криминологии заключается не только во взаимодействии ученых-криминологов и сотрудников правоохранительных органов со СМИ, но и в выведении идей науки криминологии за предел академических кругов и становлении их более доступными для изучения. Целью просветительской функции является создание у общества более глубокого понимания проблем криминальной

сферы, развенчание мифов и заблуждений относительно отправления уголовного правосудия и способствование развитию медиаграмотности, что в свою очередь способствует снижению криминогенной обстановки.

Средства массовой информации имеют прямое влияние на общественное сознание, что может способствовать как снижению уровня преступности, так и его повышению (Мацкевич, 2013). К примеру, репрезентация сотрудников правоохранительных органов в СМИ как компетентных специалистов придает гражданам чувство защищенности и мотивирует на сотрудничество с правоохранительными органами (Гайдай, Грозин, 2020). Материалы, публикуемые СМИ, могут содержать так называемые кримино-репульсионные триггеры – аудиовизуальные материалы, вызывающие в человеке цепь переживаний, обладающих способностью подавить криминальную мотивацию (Токарев, Бодров, 2012). Такими триггерами могут быть сюжеты, напоминаящие потенциальному правонарушителю о неотвратимости наказания. Налаживание сотрудничества между правоохранительными органами и СМИ является одним из методов формирования положительного представления о работе правоохранительных органов среди граждан (Глухова и др., 2017).

Способность медиасистемы охватить широкую аудиторию граждан позиционирует ее как важный ресурс для системы уголовного правосудия и всех сопутствующих ей судебных и правоохранительных органов. Чтобы система уголовного правосудия работала эффективно, она должна иметь авторитет, основанный на готовности людей придать ей легитимность, и повествование в СМИ может повлиять на этот процесс.

Развлекательные СМИ также изучались и подвергались критике за их влияние на общественное мнение о людях и учреждениях, составляющих систему уголовного правосудия. Большое количество телевизионных программ (например, комедии, детективы, драмы, биографии, документальные фильмы) так или иначе сосредоточены на полиции, адвокатах, судьях, преступниках и жертвах преступлений. Влияние этих программ на общественное отношение и поведение привлекло значительное внимание исследователей. Журналисты могут повысить общую легитимность системы правосудия, освещая ее деятельность. Доверие общественности и уверенность в том, что сотрудники правоохранительных органов работают надлежащим образом, можно поддерживать за счет освещения преступлений в новостных источниках.

2. Новостная криминология в XXI веке

В эпоху до появления Интернета средства массовой информации обладали более жесткой системой цензуры. С появлением Всемирной сети, в частности социальных сетей, подвергать цензуре экспоненциально растущий поток информации стало сложнее. Концепция новостной криминологии была разработана в 80-х гг. XX в., следовательно, в тот временной период исследователи были сосредоточены на особенностях репрезентации отправления уголовного правосудия в традиционных СМИ, в частности, по радио, телевидению и в газетах. В широком смысле понимания термина «средства массовой информации» Интернет также можно назвать разновидностью СМИ (Суходолов, Бычкова, 2017). Так называемые альтернативные средства массовой информации (также известные как социальные медиа), видеохостинги, блоги и социальные сети представляют из себя более хаотичную систему

с глобальным охватом аудитории. Любой пользователь может поделиться своим субъективным мнением, которое, в зависимости от работы алгоритмов, может найти широкий отклик среди других пользователей со всего мира. Одно и то же суждение приобретает разный смысл и имеет разное влияние на общественное мнение в зависимости от личности автора. Данный факт обостряет актуальность новостной криминологии. Такие новые феномены киберпространства, как культура отмены, кибербуллинг, информационные войны и т. д., обращают внимание научного сообщества на необходимость в обновлении доктрины новостной криминологии.

В случае классических СМИ над созданием материала работают несколько человек в целях улучшения качества контента, исходный материал нацелен на аудиторию в рамках одного государства или его региона. Следовательно, методики, разработанные новостными криминологами при взаимодействии с традиционными формами СМИ, все еще могут применяться в сети Интернет, но их эффективность стала намного ниже, что говорит о необходимости поиска новых подходов к взаимодействию.

Согласно статистике, за последние годы наблюдаются серьезные изменения в предпочтениях относительно источников информации. Так, в Российской Федерации в 2010 г. 89 % опрошенных предпочитало телевидение как основной источник новостей, 13 % получало информацию из новостных сайтов в Интернете, 21 % – из печатной прессы, газет и журналов, 19 % узнавали новости по радио и всего 4 % опрошенных – из блогов, сайтов и социальных сетей. По состоянию на 2023 г. можно заметить, что за 13 лет динамика предпочтения зрителей изменилась в пользу альтернативных СМИ. Так, в 2023 г. процентное соотношение россиян, получающих информацию по телевидению, составило 62 %, из новостных сайтов – 42 %, из блогов и социальных сетей – 23 %. Показатели предпочтения радио и печатной прессы резко снизились и составили 8 и 7 % соответственно¹.

При этом рейтинг доверия новостным источникам также изменился: уровень доверия телевидению составил 43 % в 2023 г., тогда как в 2010-м он составлял 63 %. За этот временной отрезок уровень доверия к форумам, блогам и социальным сетям вырос с 4 до 13 %.

С появлением Интернета и альтернативных СМИ новостная криминология приобретает дополнительные функции. Так, теперь перед новостной криминологией также стоит задача изучить интернет-сообщества и субкультуры, как эти сообщества формируются и влияют на уровень преступности. В этой области основное внимание уделяется репрезентации образа сотрудника правоохранительных органов в онлайн-сообществе и среди представителей разных субкультур. Новостные криминологи могут изучить, как информация циркулирует в этих пространствах и как она коррелирует с поведением участников интернет-сообществ в реальной жизни.

Жанровые признаки записи в Интернете размыты, так как, с одной стороны, они имеют черты записи в личном дневнике, с другой – такая запись нацелена на прочтение широким кругом пользователей (Александрова, 2008). Субъективное мнение одного человека, основанное на эмоциях и спекулятивной оценке, в редких случаях подкрепленное фактами, может найти широкий отклик среди других пользователей и привести к общественному резонансу. Это говорит о персонифицированности

¹ Источники информации: предпочтения россиян. (2023, 14 февраля). Фонд «Общественное мнение». <https://clck.ru/3CgYy3>

альтернативных СМИ, при которой основу общественного мнения в Интернете может составить не только блогер, политик или другая медийная личность, но и любой пользователь Сети (Быков, Ахмедова, 2021).

В этой особенности альтернативных СМИ заключается еще одна новая функция новостной криминологии: современные условия позволяют представителям правоохранительных органов и криминологам создавать блоги и новостные страницы без необходимости взаимодействовать с представителями традиционных СМИ. Как было упомянуто выше, правоохранительные органы и представители традиционных СМИ зачастую преследуют разные цели, в связи с чем результат такого взаимодействия может негативно повлиять на качество и содержание материала, которое изначально хотели донести новостные криминологи. К примеру, в рамках изучения криминологии массовых коммуникаций Д. А. Шестаков выделил ряд методов обработки общественного мнения, применяемых традиционными СМИ, таких как прямая фальсификация фактов, создание иллюзии открытой дискуссии и дозирование информации (Шестаков, 2013). Специфика альтернативных СМИ заключается в том, что новостные криминологи могут взаимодействовать с аудиторией в Сети напрямую и самостоятельно выбирать контент для осуществления просветительской деятельности без необходимости взаимодействовать с иными лицами, как в случае с традиционными СМИ.

В этом аспекте любопытны подходы некоторых государств – участников БРИКС к вопросам взаимодействия правоохранительных органов и СМИ внутри государств. Так, Индия считает нежелательным взаимодействие правоохранительных органов с сотрудниками новостных каналов относительно освещения новостей об уголовных делах, по которым ведется расследование или не было оглашено решение суда, так как информация в перспективе может нанести моральный ущерб стороне защиты или стороне обвинения². Подход Индии также любопытен необычным экспериментом со стороны правоохранительных органов, в рамках которого региональные полицейские участки создают блоги и аккаунты в соцсетях³. К примеру, блог полиции Мумбаи имеет 4 млн подписчиков. В таких блогах полицейские делятся новостями о криминогенной обстановке в регионе, а также предлагают систему обратной связи. Так, граждане могут сообщить сотрудникам правоохранительных органов о подозрительных инцидентах, используя Твиттер⁴ или Ватсап.

В случае с Бразилией в интернет-сегменте данного государства присутствует противостояние между членами организованной преступности и правоохранительными органами ввиду того, что преступники используют соцсети для устрашения населения и продвижения своего незаконного бизнеса⁵. Правоохранительные органы Бразилии имеют схожую с Индией стратегию и используют соцсети для повышения

² Narendran, A. (2022, June 14). Police-Media relations: Should they be regulated? The Probe. <https://clck.ru/3CgZ4q>

³ Chaturvedi, A. (2019, July 27). Law enforcement agencies turn to social media for better outreach. The Economic Times. <https://clck.ru/3CgZ93>

⁴ Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации

⁵ Muggah, R. (2015, August 21). Gangsta's Paradise: How Brazil's Criminals (and Police) Use Social Media. Instituto Igarapé. <https://goo.su/IRgf>

своего рейтинга в глазах общественности и оптимизации процесса получения необходимой информации.

Новостные криминологи из ЮАР подчеркивают, что их ситуация касательно имиджа сотрудников правоохранительных органов схожа с ситуацией, наблюдаемой в Великобритании и США (Motsepe, 2020). Информация, освещаемая в альтернативных СМИ, заставляет полицию ЮАР (SAPS) выглядеть некомпетентной и непрофессиональной. Имидж этого органа был запятнан рядом опосредованных скандалов, в которых имели место такие действия со стороны сотрудников, как институциональный расизм, некомпетентное расследование преступлений (убийств) и повторяющаяся коррупция. Исторически сложилось так, что средства массовой информации в Южной Африке играли значительную роль в разоблачении злоупотреблений и неправомερных действий полиции (Potgieter, 2013). Так, уровень доверия общественности к полиции в ЮАР очень низкий.

3. Культура отмены как криминологический феномен

Усиливают актуальность влияния альтернативных СМИ на мнение граждан о правоохранительных органах возникновение и развитие такого феномена, как культура отмены, также известной как cancel culture. Причиной такой отмены может послужить публичное высказывание, которое считается неприемлемым с позиции представлений о добре и зле отдельных групп. Экспоненциальная скорость распространения негативной реакции в отношении того или иного высказывания может иметь непоправимые последствия для дальнейшей карьеры автора высказывания. При этом подвергнуться «отмене» могут не только отдельные лица, но и частные учреждения, государственные органы и даже отдельные государства, их культурное наследие и граждане.

Период развития культуры отмены пришелся на 2015–2020 гг. На сегодняшний день данный феномен наиболее распространен в англоговорящих странах, таких как США и Великобритания. Однако тенденции появления культуры отмены заметны и в других странах, например, во Франции, Южной Корее и Российской Федерации. В последнее время Российская Федерация, ее культура и граждане стали объектами отмены в зарубежных традиционных и альтернативных СМИ⁶. В российском обществе культура отмены зародилась совсем недавно, и на данный момент известно лишь несколько случаев «отмены» медийных личностей и руководителей компаний, однако, как показывает практика, в отличие от Запада последствия культуры отмены в России не оказывают серьезного влияния на карьеру и жизнь лиц, подвергаемых ей.

Культура отмены представляет собой особую форму остракизма, при которой индивид, совершивший тот или иной поступок, противоречащий представлениям о добре и зле отдельных групп, изгоняется из социальных или профессиональных кругов. Одной из причин возникновения и развития культуры отмены является резкий отказ пользователей Сети идти на компромисс с теми, чье мировоззрение идет вразрез с их идеалами, а также желание максимально отгородиться от неприятных

⁶ Акопов, П. (2022). Отмена России вышла на вселенский уровень. РИА Новости. <https://clck.ru/3CgZS4>

концепций (Lukianoff & Haidt, 2019). Любой, несмотря на ограниченный доступ к фактам, может определить и публично заявить, считает ли он человека виновным, а затем потребовать «отмены» этого человека. «Отмена» влечет за собой увольнение человека, разжигание повсеместной ненависти в отношении него, организации или даже сообщества. Общественные организации, которые стоят за инициированием «отмены», в зависимости от характера действий жертвы «отмены», также добиваются привлечения лица к уголовной ответственности. Широкий общественный резонанс, вызванный «отменой» лица в СМИ, подрывает принцип объективности и беспристрастности суда, ярким примером чего является судебное разбирательство по делу Харви Вайнштейна (Борзунова и др., 2020). Диктуя судебный процесс, широкая общественность фактически становится судьями и присяжными для жертвы «отмены» (Баранова, 2021).

Культура отмены имеет четыре характерные черты во всех случаях этого явления: (1) публичное порицание неприемлемого поведения; (2) ретроактивность, т. е. действие, допустимое в тот или иной период времени, спустя несколько лет может стать основанием для «отмены»; (3) отказ от поддержки жертвы «отмены», а также (4) желание увидеть, как жертва испытывает последствия или наказание (например, потерю работы и прибыли, получения тюремного заключения и даже совершение суицида).

Причиной для «отмены» гражданина может быть как действие, противоречащее общему понятию морали и нравственности (например, мошенничество, насильственные действия сексуального характера и т. д.), так и действие или высказывание, которое не соответствует жизненной позиции и политическим взглядам отдельной группы лиц. Тренд на «отмену» жертвы приобретает характер снежного кома, в результате чего жертва подвергается «отмене» со стороны граждан и учреждений, которые не относятся к оскорбленной социальной группе. Так, скандал, последовавший за высказыванием Джоан К. Роулинг об абсурдности концепции смены пола, вынудил многие компании, не имеющие никакого отношения к ЛГБТ-сообществу⁷, разорвать контракты с писательницей и отказать ей в сотрудничестве.

Возвращаясь к вопросу освещения правоохранительных органов в СМИ в целях формирования положительного общественного мнения, стоит отметить, что, ввиду субъективности оценки ситуации в материалах, выкладываемых в сети и сложности прогнозирования их влияния на общественность, новостная криминология сталкивается со сложностями, которые не предусматривались Греггом Баракком, автором данной концепции. Так, в рамках скандала, связанного с убийством Джорджа Флойда в 2020 г., в сети Интернет возникла неконтролируемая волна негативных суждений о полиции США в целом, что впоследствии повлекло массовые беспорядки. Учитывая непредсказуемость социокультурных явлений в сети Интернет, в долгосрочной перспективе подобные случаи могут повториться и в других государствах.

Согласно данным Национального центра статистики здравоохранения США, в 2020 г. годовой прирост количества убийств был самым большим с 1905 г.⁸ В 2020 г. в США на каждые 100 000 человек приходилось 7–8 убийств, по сравнению с шестью

⁷ Пропаганда нетрадиционных сексуальных отношений в Российской Федерации запрещена.

⁸ Crude death rates for All causes: United States, 2020-Quarter 3. (2020) National Center for Health Statistics. <https://clck.ru/3CgZcE>

убийствами на 100 000 человек годом ранее. Рост уровня убийств в стране в 2020 г. намного превысил 20-процентный рост, измеренный в 2001 г., который был вызван террористическими атаками 11 сентября. Одной из причин роста убийств в США в 2020 г. считают изменения в отношениях между полицией и общественностью после убийства Джорджа Флойда в Миннесоте⁹.

Инциденты, схожие с историей Д. Флойда, ранее имели место в уголовной практике США, однако никогда деятельность полиции данного государства не подвергалась столь острой стигматизации в глазах общественности на основе поведения одного сотрудника данного правоохранительного органа. Причиной такой острой реакции стала широкая огласка инцидента в СМИ. К примеру, в серьезных газетных изданиях США, таких как The New York Times, начали появляться статьи, призывающие к полной изоляции полиции от общества. Так, автор одной из таких статей предполагает, что полное упразднение полиции и перенаправление финансовых средств в другие общественные секторы, такие как образование, смогут не только снизить, но и уничтожить преступность в принципе, что тем самым сделает полицию неактуальной и устаревшей как социальный институт¹⁰.

Еще одним эффектом освещения преступлений в СМИ, который привлек значительное внимание исследователей, является влияние досудебной огласки на присяжных. Было отмечено, что большая часть освещения преступлений наносит ущерб обвиняемому. Разнообразные экспериментальные и квазиэкспериментальные исследования продемонстрировали последовательную поддержку гипотезы о том, что, по крайней мере, умеренная предвзятость против ответчика может быть результатом воздействия досудебной огласки.

Bruschke и Loges обнаружили, что количество обвинительных приговоров обвиняемых в федеральных убийствах, чьи дела не получили заметного освещения в печати, существенно не отличались от уровня обвинительных приговоров обвиняемых, чьи дела широко освещались в печати. Они обнаружили, что самый высокий уровень обвинительных приговоров наблюдался среди тех обвиняемых, по делу которых было написано от одной до пяти статей в СМИ. Обвиняемые с наибольшей огласки, получали значительно более длительные сроки тюремного заключения, чем те, кто мало или совсем не были известны в СМИ (Bruschke & Loges, 2003).

Несмотря на тот факт, что данное исследование было проведено в 2004 г., оно не теряет своей актуальности и сейчас, когда внедрение интернет-СМИ стало массовым явлением. Так, средства массовой информации, оказывая воздействие на общественное мнение, способствуют развитию предвзятости у потенциальных присяжных заседателей, что противоречит базовым правам обвиняемого в суде, в связи с чем правоведы вынуждены искать способы обеспечения права на беспристрастное судебное разбирательство, учитывая новые условия (Brown, 2013). Персонафицированность интернет-СМИ представляет собой новый аспект современных реалий, к которым необходимо адаптироваться с точки зрения новостной криминологии. Такие негативные проявления современных СМИ, как культура

⁹ Gramlich, J. (2021, October 27). What we know about the increase in US murders in 2020. <https://clck.ru/3CgZgE>

¹⁰ Kaba, M. (2020, June 12). Yes, we mean literally abolish the police because reform won't happen. The New York Times. <https://clck.ru/3CgZkz>

отмены, имеют колоссальные последствия для системы уголовного правосудия. Культура отмены по своей специфике является формой кибербуллинга, при котором происходит стигматизация отдельных лиц, учреждений и даже государств и их культурного наследия.

Заключение

Новостная криминология, разработанная в 80-х гг. XX в., не утратила своей актуальности, возникновение Всемирной сети и новых форм СМИ свидетельствует о необходимости проведения новых исследований в рамках данной подотрасли криминологии. Формы взаимодействия с традиционными формами СМИ не имеют эффективности в отношении интернет-СМИ. Возникновение таких комплексных социальных феноменов, как культура отмены, обостряют важность выработки контрмер по воздействию на общественное мнение. Укоренение в цифровом сообществе парадигм, дискредитирующих деятельность правоохранительных органов и предполагающих более высокую эффективность обычного пользователя в борьбе с преступностью, является потенциальным криминогенным фактором, при котором такая борьба может выйти за рамки киберпространства в повседневную жизнь.

Список литературы

- Александрова, И. Б. (2008). Моблоги и блоги: альтернативные СМИ? *Вестник Московского университета. Серия 10. Журналистика*, 4, 68–79. <https://elibrary.ru/jvvr0r>
- Баранова, М. В. (2021). Канселинг (cancel culture) как инновационный правокультурный феномен. *Юридическая техника*, 15, 123–128. <https://elibrary.ru/mjkmnp>
- Борзунова, Н. Ю., Максимова, К. Л., Цечоев, А. М. (2020). Принцип презумпции невиновности в уголовном судопроизводстве и проблемы его реализации. *Социология и право*, 4, 86–91. <https://doi.org/10.35854/2219-6242-2020-4-86-91>
- Быков, И. А., Ахмедова, Ю. Д. (2021). Культура отмены и персонификация политического дискурса. *Вестник Кабардино-Балкарского государственного университета: Журналистика. Образование. Словесность*, 1(1), 14–26. <https://doi.org/10.24334/KBSU.2021.1.1.002>
- Гайдай, М. К., Грозин, С. Ю. (2020). Роль СМИ в оценке деятельности полиции. *Юристъ-Правоведъ*, 3(94), 195–198. <https://elibrary.ru/bnfjvu>
- Глухова, А. А., Иудин, А. А., Шпилев, Д. А. (2017). Оценка гражданами уровня доверия полиции и защищенности от преступных посягательств. *Russian Journal of Economics and Law*, 3(43), 56–80. EDN: <https://elibrary.ru/zfnfbp>. DOI: <https://doi.org/10.21202/1993-047X.11.2017.3.56-80>
- Горшенков, Г. Н. (2003). *Криминология массовых коммуникаций*. Н. Новгород. <https://elibrary.ru/qvxufj>
- Мацкевич, И. М. (2013). Общественное сознание и преступность. *Schriften Zum Deutschen und Russischen Strafrecht*, 3, 167–178. (на нем.). <https://elibrary.ru/ozdolh>
- Суходолов, А. П., Бычкова, А. М. (2017). К вопросу о роли средств массовой информации в противодействии пропаганде суицида в социальных сетях. *Евразийское сотрудничество: гуманитарные аспекты*, 1, 111–127. <https://elibrary.ru/yrofay>
- Сысоев, А. М. (2007). Влияние средств массовой информации на формирование криминогенных установок. *Уголовно-исполнительное право*, 2, 32–34. <https://elibrary.ru/jxdzvn>
- Токарев, А. Л., Бодров, Н. Ф. (2012). Криминологический и судебно-экспертный подходы к изучению публикаций СМИ, стимулирующих антиобщественное поведение. *Актуальные проблемы российского права*, 2, 214–223. <https://elibrary.ru/zkpxqk>
- Шамаев, А. В. (2018). Криминология. Роль средств массовой информации в предупреждении преступности в России. *Проблемы науки*, 12(36), 69–71.
- Шестаков, Д. А. (2013). Правовая журналистика и криминология массовой коммуникации. *Платон*, 1, 40–41. <https://elibrary.ru/ywylwh>
- Arrigo, B. A., & Bersot, H. Y. (2015). Critical criminology. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 244–250). <https://doi.org/10.1016/b978-0-08-097086-8.45053-1>

- Barak, G. (1988). Newsmaking criminology: Reflections of the media, intellectuals, and crime. *Justice Quarterly*, 5(4), 565–587. <https://doi.org/10.1080/07418828800089891>
- Barak, G. (2007). Doing newsmaking criminology from within the academy. *Theoretical Criminology*, 11(2), 191–207. <https://doi.org/10.1177/1362480607075847>
- Brown, K. R. (2013). Somebody poisoned the jury pool: Social media's effect on jury impartiality. *Texas Wesleyan Law Review*, 19, 809. <https://doi.org/10.37419/twlr.v19.i3.6>
- Bruschke, J., & Loges, W. E. (2003). *Free press vs. fair trials: Examining publicity's role in trial outcomes*. Routledge.
- Cottee, S. (2004). The idea of a critical criminology: irony, scepticism and commitment. *International Journal of the Sociology of Law*, 32(4), 363–376. <https://doi.org/10.1016/j.ijsl.2004.08.001>
- De Melo Bandeira, G. C. S. (2013). "Corruption" and social and economic criminal law: Criminology, criminal policy, political science and law & economics – A new idea about criminal liability of legal entities. *Tékhne*, 11(2), 105–113. <https://doi.org/10.1016/j.tekhne.2013.10.002>
- Frost, N. A., & Phillips, N. D. (2011). Talking heads: Crime reporting on cable news. *Justice Quarterly*, 28(1), 87–112. <https://doi.org/10.1080/07418820903173336>
- Gore, M. L., Hübschle, A., Botha, A. J., Coverdale, B. M., Garbett, R., Harrell, R. M., Krüger, S. C., Mullinax, J. M., Olson, L. J., Ottinger, M. A., Smit-Robinson, H., Shaffer, L. J., Thompson, L. J., Van Den Heever, L., & Bowerman, W. W. (2020). A conservation criminology-based desk assessment of vulture poisoning in the Great Limpopo Transfrontier Conservation Area. *Global Ecology and Conservation*, 23, e01076. <https://doi.org/10.1016/j.gecco.2020.e01076>
- Lukianoff, G., & Haidt, J. (2019). *The coddling of the American mind: How good intentions and bad ideas are setting up a generation for failure*. Penguin.
- Motsepe, L. L. (2020). The impact of news media on the SAPS's public image: 30 years in democratic policing. In *Proceedings of the 11th International Conference on Social Sciences* (pp. 167–181).
- Ozkan, T. (2019). Criminology in the age of data explosion: New directions. *The Social Science Journal*, 56(2), 208–219. <https://doi.org/10.1016/j.soscij.2018.10.010>
- Potgieter, P. J. (2013). Exploring the public image of the police in a post-apartheid South Africa. *Acta Criminologica: African Journal of Criminology & Victimology*, 26(2), 147–169.
- Richards, I., Wood, M. A., & Iliadis, M. (2020). Newsmaking criminology in the twenty-first century: an analysis of criminologists' news media engagement in seven countries. *Current Issues in Criminal Justice*, 32(2), 125–145. <https://doi.org/10.1080/10345329.2019.1696442>
- Stout, B., & Clamp, K. (2015). Applied Criminology and Criminal Justice. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 832–838). <https://doi.org/10.1016/b978-0-08-097086-8.10512-4>

Сведения об авторе



Бабаева Валентина Андреевна – аспирант кафедры уголовного права, уголовного процесса и криминалистики, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации

Адрес: 119454, Россия, г. Москва, проспект Вернадского, 76

E-mail: tina.babaeva.a@gmail.com

ORCID ID: <https://orcid.org/0000-0001-8298-4960>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1162866

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.81 / Криминология

Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 29 февраля 2024 г.

Дата одобрения после рецензирования – 20 марта 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:343.9:004.4

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

DOI: <https://doi.org/10.21202/jdtl.2024.33>

Newsmaking Criminology in the 21st Century: Forming the Public Opinion under the New Reality

Valentina A. Babaeva

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs
of the Russian Federation, Moscow, Russia

Keywords

cancel culture,
crime,
digital technologies,
discrimination,
Internet,
law,
mass media,
newsmaking criminology,
social network,
social relations

Abstract

Objective: to study the concept of newsmaking criminology and its relevance in the current conditions of mass media development.

Methods: the methodological basis of the work consists of general scientific, social, and special-legal methods of cognition. The conducted research is based on the dialectical method (in determining the general direction of the study), methods of formal logic (analysis, synthesis, induction, deduction, analogy), system method (in comparing and generalizing the information collected for the research).

Results: the functions of newsmaking criminology in its classical manifestation, as well as its additional functions in the study of mass media in the Internet, were revealed. It is suggested that with the emergence of the World Wide Web, the relevance of newsmaking criminology has increased: social networks, blogs and video hosting as alternative media have a strong influence on public opinion, while an unlimited number of people have access to content generation, contrary to traditional media. Many states understand the importance of interaction between mass media and law enforcement agencies and are actively implementing their methods of promoting newsmaking criminology online. This article points out the risks that arise in media coverage of law enforcement and crime. One of such risks is the cancel culture, which is spontaneous, unpredictable in nature, and may jeopardize the quality of life of the victim or business reputation and activity of organizations.

© Babaeva V. A. , 2024

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 functions performed by newsmaking criminology in the study of traditional and alternative media were identified. So far, such doctrine has not been sufficiently researched taking into account modern forms of mass communication. Examples of interaction between law enforcement agencies of different states and the media were analyzed.

Practical significance: the study contributes to understanding the correlation between criminological phenomena and modern media platforms. The Internet and social networks provide new channels of information exchange that differ significantly from traditional media such as printed media or television.

For citation

Babaeva, V. A. (2024). Newsmaking Criminology in the 21st Century: Forming the Public Opinion under the New Reality. *Journal of Digital Technologies and Law*, 2(3), 657–673. <https://doi.org/10.21202/jdtl.2024.33>

References

- Aleksandrova, I. B. (2008). Moblogs and blogs: alternative mass media? *Vestnik Moskovskogo universiteta. Ser. 10. Zhurnalistika*, 4, 68–79. (In Russ.).
- Arrigo, B. A., & Bersot, H. Y. (2015). Critical criminology. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 244–250). <https://doi.org/10.1016/b978-0-08-097086-8.45053-1>
- Barak, G. (1988). Newsmaking criminology: Reflections of the media, intellectuals, and crime. *Justice Quarterly*, 5(4), 565–587. <https://doi.org/10.1080/07418828800089891>
- Barak, G. (2007). Doing newsmaking criminology from within the academy. *Theoretical Criminology*, 11(2), 191–207. <https://doi.org/10.1177/1362480607075847>
- Baranova, M. V. (2021). Cancel culture as an innovative legal and cultural phenomenon. *Juridical Techniques*, 15, 123–128. (In Russ.).
- Borzunova, N. Yu., Maksimova, K. L., & Tsechoev, A. M. (2020). The Principle of Presumption of Innocence in Criminal Proceedings and Problems of Its Implementation. *Sociology and Law*, 4, 86–91. (In Russ.). <https://doi.org/10.35854/2219-6242-2020-4-86-91>
- Brown, K. R. (2013). Somebody poisoned the jury pool: Social media's effect on jury impartiality. *Texas Wesleyan Law Review*, 19, 809. <https://doi.org/10.37419/twlr.v19.i3.6>
- Bruschke, J., & Loges, W. E. (2003). *Free press vs. fair trials: Examining publicity's role in trial outcomes*. Routledge.
- Bykov, I. A., & Akhmedova, Yu. D. (2021). Cancel culture in the political discourse of modern Russia. *Vestnik Kabardino-Balkarskogo gosudarstvennogo universiteta: Zhurnalistika. Obrazovaniye. Slovesnost*, 1(1), 14–26. (In Russ.). <https://doi.org/10.24334/KBSU.2021.1.1.002>
- Cottee, S. (2004). The idea of a critical criminology: irony, scepticism and commitment. *International Journal of the Sociology of Law*, 32(4), 363–376. <https://doi.org/10.1016/j.ijsl.2004.08.001>
- De Melo Bandeira, G. C. S. (2013). "Corruption" and social and economic criminal law: Criminology, criminal policy, political science and law & economics – A new idea about criminal liability of legal entities. *Tékhne*, 11(2), 105–113. <https://doi.org/10.1016/j.tekhne.2013.10.002>
- Frost, N. A., & Phillips, N. D. (2011). Talking heads: Crime reporting on cable news. *Justice Quarterly*, 28(1), 87–112. <https://doi.org/10.1080/07418820903173336>
- Gaidai, M. K., & Grozin, S. Yu. (2020). The role of the media in police performance assessment. *Yurist-Pravoved*, 3(94), 195–198. (In Russ.).
- Glukhova, A. A., Iudin, A. A., & Shpilev, D. A. (2017). Assessment by citizens of the level of confidence of police and protection from criminal entry. *Actual Problems of Economics and Law*, 11(3), 56–80. (In Russ.). <https://doi.org/10.21202/1993-047X.11.2017.3.56-80>

- Gore, M. L., Hübschle, A., Botha, A. J., Coverdale, B. M., Garbett, R., Harrell, R. M., Krüger, S. C., Mullinax, J. M., Olson, L. J., Ottinger, M. A., Smit-Robinson, H., Shaffer, L. J., Thompson, L. J., Van Den Heever, L., & Bowerman, W. W. (2020). A conservation criminology-based desk assessment of vulture poisoning in the Great Limpopo Transfrontier Conservation Area. *Global Ecology and Conservation*, 23, e01076. <https://doi.org/10.1016/j.gecco.2020.e01076>
- Gorshenkov, G. N. (2003). *Criminology of mass communications*. (In Russ.).
- Lukianoff, G., & Haidt, J. (2019). *The coddling of the American mind: How good intentions and bad ideas are setting up a generation for failure*. Penguin.
- Matskevich, I. M. (2013). Mass consciousness and crime. *Schriften zum deutschen und russischen Strafrecht*, 3, 167–178. (In German).
- Motsepe, L. L. (2020). The impact of news media on the SAPS's public image: 30 years in democratic policing. In *Proceedings of the 11th International Conference on Social Sciences* (pp. 167–181).
- Ozkan, T. (2019). Criminology in the age of data explosion: New directions. *The Social Science Journal*, 56(2), 208–219. <https://doi.org/10.1016/j.soscij.2018.10.010>
- Potgieter, P. J. (2013). Exploring the public image of the police in a post-apartheid South Africa. *Acta Criminologica: African Journal of Criminology & Victimology*, 26(2), 147–169.
- Richards, I., Wood, M. A., & Iliadis, M. (2020). Newsmaking criminology in the twenty-first century: an analysis of criminologists' news media engagement in seven countries. *Current Issues in Criminal Justice*, 32(2), 125–145. <https://doi.org/10.1080/10345329.2019.1696442>
- Shamaev, A. V. (2018). Criminology. The role of mass media in preventing crime in Russia. *Problems of Science*, 12(36), 69–71. (In Russ.).
- Shestakov, D. A. (2013). Legal journalism and criminology of mass communication. *Platon*, 1, 40–41. (In Russ.).
- Stout, B., & Clamp, K. (2015). Applied Criminology and Criminal Justice. In *International Encyclopedia of the Social & Behavioral Sciences* (2d Ed., pp. 832–838). <https://doi.org/10.1016/b978-0-08-097086-8.10512-4>
- Sukhodolov, A. P., Bychkova, A. M. (2017). On the role of mass media in countering the propaganda of suicide in social networks. *Evroaziatskoe sotrudnichestvo: gumanitarnye aspekty*, 1, 111–127. (In Russ.).
- Sysoyev, A. M. (2007). Influence of mass media on formation of criminogenic attitude. *Ugolovno-ispolnitel'noe pravo*, 2, 32–34 (In Russ.).
- Tokarev, A. A., & Bodrov, N. F. (2012). Criminological and forensic approaches to the study of mass-media publications which provoke deviant behavior. *Actual Problems of Russian Law*, 2, 214–223. (In Russ.).

Author information



Valentina A. Babaeva – post-graduate student, Department of Criminal Law, Criminal Procedure and Criminology, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation

Address: 76 prospekt Vernadskogo, 119454 Moscow, Russia

E-mail: tina.babaeva.a@gmail.com

ORCID ID: <https://orcid.org/0000-0001-8298-4960>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1162866

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – February 29, 2024

Date of approval – Март 20, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:341:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.34>

Нарушение воздушного пространства страны беспилотными летательными аппаратами (дронами) с точки зрения международного права

Милад Каши Камиджани

Университет Кума, Кум, Иран

Ключевые слова

беспилотный летательный аппарат,
воздушное пространство,
вооруженный конфликт,
дрон,
международная конвенция,
международное
гуманитарное право,
международное право,
права человека,
право,
цифровые технологии

Аннотация

Цель: на примере использования беспилотными летательными аппаратами (дронами) воздушного пространства показать вызовы международному праву и недостатки действующего регулирования, обусловленные стремительным развитием беспилотных технологий.

Метод: исследование построено прежде всего на совокупности способов толкования положений международного права, позволяющих проанализировать положения в области использования беспилотных летательных аппаратов (дронов).

Результаты: в статье на основе международного воздушного и гуманитарного права рассматриваются вопросы использования беспилотными летательными аппаратами (дронами) воздушного пространства. Проводится анализ основных источников права в этой сфере, которыми служат, в частности, положения международного воздушного права, особенно Парижской, Мадридской, Гаванской и Чикагской конвенций. Предпринимается попытка ответить на возникающие в связи с развитием беспилотных технологий вопросы о том, какие нормы международного права распространяются на их использование и способно ли действующее международное право на них эффективно реагировать. Показано современное представление о правовом статусе воздушного пространства над территорией государства. Автор задается вопросом, не является ли исключительной область беспилотных летательных аппаратов, автоматических и автономных видов вооружений, объединяющей научные и военные достижения с новыми технологиями. В этой связи затрагивается проблема использования беспилотных летательных аппаратов в международных конфликтах в качестве универсального оружия. Делается вывод о том, что при использовании интеллектуального, управляемого и роботизированного оружия, способного автоматически принимать решения,

© Камиджани М. К., 2024

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.

такого как беспилотники, необходимо пересмотреть существующие конвенции или установить новые правовые стандарты в отношении этого вида оружия. Такие беспилотники предлагается рассматривать как военные воздушные суда особого типа.

Научная новизна: международно-правовая ответственность государств за военное применение беспилотных летательных аппаратов не получила в доктрине однозначной оценки, вместе с тем многое в данном вопросе зависит от юридического толкования важнейших международно-правовых категорий, а дальнейшая разработка данной проблематики непосредственно связана с развитием вопросов международной ответственности и концепцией суверенитета государства над воздушным пространством.

Практическая значимость: развитие на современном этапе беспилотной авиации демонстрирует несовершенство сформированной правовой базы, которая призвана регулировать указанные отношения. В связи с исследованием общемировой тенденции в контексте действующего международного права, выявление недостатков положений последнего имеет значение прежде всего для дальнейшей их модернизации с учетом современных достижений науки и развития концепции суверенитета страны над ее воздушным пространством.

Для цитирования

Камиджани, М. К. (2024). Нарушение воздушного пространства страны беспилотными летательными аппаратами (дронами) с точки зрения международного права. *Journal of Digital Technologies and Law*, 2(3), 674–689. <https://doi.org/10.21202/jdtl.2024.34>

Содержание

Введение

1. Суверенное воздушное пространство и статус беспилотных летательных аппаратов (дронов)
2. Чикагская конвенция и ее роль в организации воздушного движения летательных аппаратов
3. Международный режим воздушного пространства и ответственность за его нарушение
4. Концепция и принцип суверенитета страны над ее воздушным пространством
5. Использование вооруженных дронов и вопросы международного гуманитарного права
6. Международная ответственность стран, допускающих нарушения

Заключение

Список литературы

Введение

Некоторые ученые считают, что новые цифровые технологии в целом и беспилотники в частности бросают вызов действующему международному праву, которое и возникло в связи с появлением новых технологий и нового оружия; что международное

право достигло своего низшего уровня, будучи не в состоянии ответить на потребности, возникающие в связи с новыми технологиями; что это привело к необходимости сформулировать новые законы, соответствующие новым технологиям и способные их контролировать (Bace et al., 2024).

Сегодня во многих войнах инициатива принадлежит стране, обладающей превосходством в воздухе, и в значительной степени агрессия сверхдержав против более слабых стран осуществляется с помощью воздушных ударов, поскольку это дорогое стратегическое оружие проще и надежнее других видов вооружений (Niu et al., 2024; Ambos, 2008).

Gilley утверждает, что «беспилотные летательные аппараты могут соответствовать современным правовым стандартам»¹, и сравнивает атаку дрона с атакой пилотируемого самолета. По его мнению, если атака последнего недопустима, то она недопустима и для дрона (беспилотника, беспилотного летательного аппарата (далее – БПЛА)). Со временем использование БПЛА расширилось в нескольких областях гражданского и военного применения (Siddiqi et al., 2022).

Таким образом, наличие пилота не влияет на применение законодательства, а потому нет необходимости в новом законе об использовании беспилотников; новым потребностям вполне отвечает существующее законодательство. По словам Gilley, «закон есть закон»²; он должен применяться независимо от «платформы», и для беспилотников не требуется новое законодательство³.

Действующее международное право и существующие нормы предусматривают меры в рамках гуманитарного права, права в условиях вооруженных конфликтов, а также мягкого права. Они позволяют разработать соответствующие правила в области новых технологий и нового оружия без необходимости внесения изменений в существующее законодательство. Таким образом, нужно либо создавать новое законодательство, либо признать действующее международное право неэффективным и игнорировать его (Majd et al., 2021).

Итак, рассмотрим вопросы экспортного производства и использования новых технологий в сфере вооружений с учетом существующих норм и попытаемся найти решение для выхода из тупиковой ситуации, сложившейся под лозунгом «никаких ограничений в области нового оружия» (Ishiwatari, 2024).

1. Суверенное воздушное пространство и статус беспилотных летательных аппаратов (дронов)

Полный и исключительный суверенитет государства в границах его воздушного пространства закреплен в ст. 1 Чикагской конвенции. Согласно ст. 2 Конвенции, воздушный суверенитет государства включает пространство над сушей и водами территории, прилегающей к его границам, которые официально определены Чикагской конвенцией (Clarke, 2014; Ishiwatari, 2024).

Нужно отметить, что при обсуждении вопросов БПЛА и Чикагской конвенции в основном затрагивается тема БПЛА, а другие вопросы, такие как суверенитет, не упоминаются. Такая ситуация сложилась потому, что по умолчанию считается,

¹ EU-OSHA. (2023, September 11). Unmanned aerial vehicles: implications for occupational safety and health. <https://clck.ru/3EGYKv>

² Там же.

³ Там же.

что государство, использующее беспилотник, получило согласие правительства другой страны и не нарушает принципы невмешательства и неприменения силы, либо такое использование основано на просьбе страны о помощи; поэтому в любом случае на основе согласия или просьбы страны использование беспилотников разрешено (Clarke & Moses, 2014).

Под суверенитетом здесь понимается независимость воздушного и космического пространства каждой страны от других стран. Статья 1 Чикагской конвенции гласит, что «договаривающееся государство обладает полным и исключительным суверенитетом над воздушным пространством над своей территорией»⁴, а ст. 8 Чикагской конвенции прямо запрещает полеты беспилотников без предварительного согласия других государств.

Следует также отметить, что статус БПЛА во многом зависит от того, как государство их использует, то есть не определен заранее, а определяется целью его использования. Беспилотник может использоваться для военной операции, а затем для оказания гуманитарной помощи (Tatsidou et al., 2019), поэтому характер использования играет важную роль в соответствующих законах и правилах. Беспилотники не подпадают под какой-либо абсолютный и специально предусмотренный запрет в законе (Abeyratne, 2010).

2. Чикагская конвенция и ее роль в организации воздушного движения летательных аппаратов

Впервые определение самолета было дано в Парижской конвенции по авиации 1919 г., согласно которому «самолетом является любое устройство, способное взлетать или перемещаться в воздухе»⁵. В 1944 г. на Международной конференции по гражданской авиации в Чикаго присутствовало более 50 стран. Именно тогда США предложили по окончании Второй мировой войны создать правовой институт для развития национальной авиации.

Непосредственное участие человека-пилота в управлении летательным аппаратом не является критерием определения летательного аппарата. Поэтому определения и правила Парижской конвенции и Международной организации гражданской авиации (International Civil Aviation Organization, ИКАО) от 1967 г. в определенной степени относятся и к беспилотникам (Ishiwatari, 2024).

В рамках Чикагской конвенции страны – члены ИКАО обязались соблюдать ее принципы, важнейшим из которых является полный суверенитет стран-участниц над воздушным пространством своей территории. Нет сомнений, что суверенитет государства над своим воздушным пространством является одним из важнейших положений современного международного права. Нарушение воздушного пространства стран иностранными самолетами противоречит международному праву и не раз становилось причиной крупных аварий (Vogel, 2011).

Статья 8 Конвенции – единственная, где упоминаются беспилотные летательные аппараты и указано, что их полеты могут осуществляться только по специальному

⁴ International Civil Aviation Organization. (2000). Convention on International Civil Aviation (8th Ed.). <https://clck.ru/3EGYe5>

⁵ The 1919 Paris Convention: The starting point for the regulation of air navigation. The postal history of icao. <https://clck.ru/3EGfbC>

разрешению страны, над которой пролетает дрон. Таким образом, беспилотник как летательный аппарат в определенной степени подпадает под правовой режим Чикагской конвенции, и разрешение на его эксплуатацию на территории других стран зависит от согласия этих стран.

Статья 3 Конвенции постулирует различие между летательными аппаратами национального и государственного подчинения. Согласно этой статье, государственный летательный аппарат стран-участниц не имеет права пролетать или приземляться в другой стране без ее разрешения. Однако, как представляется, обязательной силы этих двух статей недостаточно для легализации многочисленных видов деятельности беспилотников. Необходимы другие правила, особенно в области нарушений воздушного пространства, суверенитета государств, а также гуманитарных норм и прав человека (Vogel, 2011).

3. Международный режим воздушного пространства и ответственность за его нарушение

На заседании № 2319 14 декабря 1974 г. Генеральная Ассамблея ООН без голосования, на основе консенсуса членов, утвердила определение агрессии. Утвержденная резолюция и приложение к ней определяют посягательство следующим образом.

Согласно ст. 1, агрессия означает применение вооруженной силы каким-либо государством против суверенитета, территориальной целостности или политической независимости другого государства или ее использование иным образом, противоречащим Уставу Организации Объединенных Наций. В ст. 2 о преимущественном праве государства на применение вооруженных сил говорится, что Совет Безопасности имеет право, согласно Уставу ООН, подтвердить факт нарушения по таким основаниям, как недостаточная интенсивность принятых мер или несогласие с их результатами (Vogel, 2011).

Парижская конвенция как первый международный документ в области воздушных прав гласит, что каждая из сторон, подписавших конвенцию, признает за собой полный и исключительный суверенитет над воздушным пространством над своей территорией.

Это общее мнение стран-участниц повторялось и уточнялось в последующих договорах и конвенциях. Так, Мадридская конвенция 1926 г., Гаванская конвенция 1928 г. и, что важнее всего, Чикагская конвенция 1944 г. подчеркивают исключительную юрисдикцию государств над воздушным пространством над их территорией. Очевидно, что еще до начала Первой мировой войны такое представление о правовом статусе воздушного пространства над территорией было общепринятым. В качестве примера можно привести протесты голландского правительства перед началом войны против полета немецких самолетов над территорией этой страны без получения предварительного разрешения.

Нарушения в этой сфере имеют существенное отличие от других преступлений, подпадающих под юрисдикцию Международного уголовного суда, а именно геноцида, преступлений против человечности и военных преступлений, и служат основой для совершения этих преступлений.

Ряд стран – постоянных членов Совета Безопасности, используя право вето, легко допускают полеты этого типа летательных аппаратов в пространстве других стран и нарушают их суверенную территорию, несмотря на все протесты.

В случае с беспилотными летательными аппаратами, как и в случаях с автоматическим оружием или задокументированным дистанционным управлением, в принципе отсутствует пилот, который был бы подсуден и нес ответственность за нарушение. При этом в целом ответственность несет наземный диспетчер и учитывается человеческий фактор в этой ситуации (Nelson & Gorichanaz, 2019; Bassi, 2019).

Таким образом, согласно международным нормам, ответственность за все события несут исполнители Hedayad Behbad и связанные с ними лица. Поскольку они находятся за тысячи километров от поля боя, операторы дронов избегают ответственности за невыполнение таких обязанностей, как необходимые прогнозы при атаках и гарантия разделения и пропорциональности (Vogel, 2011).

4. Концепция и принцип суверенитета страны над ее воздушным пространством

Что касается прав на воздушное пространство и прав в воздушном пространстве, то наиболее ярким универсалистом в этой сфере выступил Ю. Колосов. В 1977 г. в Праге он выдвинул концепцию исключительного и полного суверенитета любой страны над воздушным пространством территории этой страны. Оно определяется как «то, что находится над сухопутной и водной территорией страны»⁶. Этот воздушный слой простирается до границы атмосферы, а после этого начинается область за пределами атмосферы, или космос.

Статья 1 Парижской конвенции от 13 октября 1919 г. закрепляет абсолютный и исключительный суверенитет государств над их территориальным воздушным пространством и территориальными водами. Чикагская конвенция от 7 декабря 1944 г. подтверждает этот принцип. Статья 2 Женевской конвенции от 1958 г. также устанавливает, что указанный суверенитет включает в себя поверхность и дно территориальных морских вод. Согласно ст. 3 Закона о гражданской авиации, утвержденного в 1338 г. хиджры [1919 г. – Прим. пер.], государство обладает абсолютным и исключительным суверенитетом над прибрежными водами.

В случае несанкционированного захода беспилотного летательного аппарата в воздушное пространство другой страны его могут перехватить в целях идентификации, вынудить покинуть воздушное пространство по установленному воздушному маршруту или направить на землю для проведения расследования или судебного преследования. Право летать или приземляться на территории другой страны может возникнуть только через заключение договора и соблюдение его условий. Существуют и другие серьезные нарушения международного права с участием БПЛА.

Согласно международному воздушному праву, каждая страна имеет право ограничить или запретить полеты самолетов других государств на части своей территории по соображениям военного характера или безопасности. Кроме того, страны должны уважать суверенитет других государств при использовании фотооборудования. Каждая договаривающаяся сторона может запретить или ограничить использование фотооборудования над своей территорией (Vogel, 2011).

Эти принципы запрещают использование самолетов-шпионов над территориями других стран и подтверждают незаконность и аморальность этого действия.

⁶ Материалы семинара по космическому праву в XXI веке. <https://clck.ru/3EPvCk>

Увеличение частоты этих нарушений свидетельствует о наглом и чудовищном пренебрежении общепринятыми нормами.

Согласно ст. 8 Чикагской конвенции, полеты беспилотных летательных аппаратов над территорией любой страны не допускаются без получения специального разрешения и соблюдения пунктов, содержащихся в этом разрешении. Страны-участницы согласились осуществлять полеты беспилотников в зонах, объявленных свободными для национальных самолетов, под необходимым контролем и наблюдением для предотвращения возможных опасностей для национальных самолетов.

5. Использование вооруженных дронов и вопросы международного гуманитарного права

Изначально дроны создавались как разведывательные самолеты. При этом вопросы о гуманитарных правах и правах человека были менее изучены. Однако в определенный момент к беспилотным системам начали присоединять и использовать боевые ракеты (Sopha et al., 2024; Rainer, 2014).

С тех пор дискуссии о гуманитарных правах ведутся более серьезно, чем раньше. Принимаются новые законы и нормы в области использования современных технологий, в том числе беспилотников; обсуждаются гуманитарные последствия таких технологий и позиции международного права, особенно международного гуманитарного права, в этой сфере (Sopha et al., 2024).

Использование вооруженных дронов вызвало серьезные вопросы в области международного права, и в частности международного гуманитарного права, прав человека и применения силы. Если обнаруживается, что государства в определенных обстоятельствах нарушают свои обязательства в рамках международного права, то встает вопрос и о правительстве этих государств. Все сильнее ощущается необходимость обратить внимание на базовые принципы и основы гуманитарных прав в этой области, ведь дроны атакуют людей без объявления войны или в отсутствие вооруженного конфликта. Если же такой конфликт существует, то в нем обязательно используют беспилотники.

В небоевых ситуациях использование беспилотников в качестве вооружения также должно быть ограничено в рамках гуманитарных прав и правозащитных норм. Что касается легитимности использования дронов, то здесь следует обратить внимание на некоторые моменты. В первую очередь беспилотники должны рассматриваться как оружие, инструмент для запуска ракет и бомб. При этом необходимо следовать стандартам прав человека.

Сегодня принято считать, что во время вооруженных конфликтов должны соблюдаться гуманитарные права и права человека. Это касается не только Женевских конвенций, но и стандартов в области прав человека. Любое применение силы, в том числе с помощью беспилотников, должно осуществляться с гарантией соблюдения минимальных человеческих стандартов.

6. Международная ответственность стран, допускающих нарушения

Международный суд неоднократно подчеркивал, что принцип неприменения силы является обязательной нормой международного права. Важнейшим источником при определении агрессии является соответствующая резолюция Генеральной

Ассамблеи ООН. Согласно этой резолюции, ввод военной техники в страну сам по себе считается агрессией и нарушает принцип неприменения силы. Согласно ст. 51 Устава ООН, применение агрессии законно только в случае обороны против вооруженного нападения, но не признается законным в качестве защиты от других форм агрессии (Sopha et al., 2024).

Беспилотники не относятся ни к государственным, ни к гражданским государственным воздушным судам, но их можно рассматривать как военные воздушные суда особого типа. Таким образом, несанкционированный заход дронов в воздушное пространство страны будет являться примером агрессии и последует международная ответственность государств, которым принадлежат эти дроны.

Поскольку перед вооруженным нападением дрона прибегать к законной защите не имеет смысла, а применение дронов-шпионов в принципе не является вооруженным нападением, вопрос о законной защите от дронов-шпионов подниматься не будет.

С другой стороны, государство-жертва может ответить, конфисковав БПЛА в мирное время или изъяв его в военное время.

В этом случае такое государство не понесет международную ответственность. Шпионаж с помощью военных беспилотников внутри другой страны, не только нарушает ряд положений Чикагской конвенции, но и противоречит таким принципам, как запрет на вмешательство во внутренние дела страны и неприменение силы. Ответственность стран, с территории которых осуществлялась эта акция, также очевидна с точки зрения международного права. Ведь молчание правительств свидетельствует о том, что такая ситуация их устраивает (Chen & Wang, 2009).

Подача исков против государства в связи с международными нарушениями, допущенными этой страной в результате отправки беспилотников-шпионов в воздушное пространство другой страны, – вопрос, не имеющий достаточных и целесообразных правовых оснований (Wang et al., 2024).

Представляется, что лучшим способом компенсировать вторжение иностранных беспилотников является их остановка и конфискация, чего пока удастся добиться благодаря современным информационным технологиям. Помимо этих действий, ИКАО также рекомендует подать жалобу в Секретариат ООН и в Совет по безопасности гражданской авиации (Askerbekov et al., 2024; Wang et al., 2024; Dolata & Schwabe, 2023).

Главным международным органом по рассмотрению жалоб и исков для предотвращения любого рода угроз и актов агрессии является Совет Безопасности ООН. Пострадавшее государство должно предпринять юридические действия, подав жалобу в Совет Безопасности по поводу проникновения военных беспилотников враждебной страны (Li & Dang, 2024).

Что касается судебного разбирательства, то следует сказать, что в первом случае остановки беспилотников ни один международный судебный орган не имеет полномочий рассматривать этот вопрос. Только если стороны согласятся на судебное разбирательство, дело может рассмотреть Международный суд, что очень маловероятно в связи с текущей ситуацией. Поскольку летательные аппараты считаются принадлежащими государству, то к ним не относятся положения Чикагской конвенции. Соответственно, механизмы и средства разрешения споров, предусмотренные этой конвенцией, здесь неприменимы (Dolata & Schwabe, 2023).

Международный суд является инстанцией, которая рассматривает правовые претензии между странами, а не такие вопросы, как посягательство. Конечно, было бы хорошо, если бы Совет Безопасности изменил свою политику и разрешил эту ситуацию. Но если Совет Безопасности ООН медлит с решением вопроса юридическим путем, то естественно, что этим хочет заняться соответствующее государство через Международный суд ([Zègre-Hemsey et al., 2024](#)).

Однако в суде может быть рассмотрен только правовой аспект этого вопроса. Эта ситуация имеет два измерения, одно из которых политическое, а другое – юридическое, и Международный суд может рассматривать только юридический аспект. Конечно, вопрос в определенной степени сложный, но в то же время необходимо учитывать интересы другой стороны. Невозможно передать дело в Международный суд, не получив согласия или заявления о подтверждении юрисдикции суда сторонами спора. Это возможно, только если правительства данных стран уже признали эту юрисдикцию или в ходе событий обе стороны или стороны, участвующие в споре, договорились о том, что дело должно быть передано в суд. Другими словами, подача иска в Международный суд зависит от согласия сторон, участвующих в споре. В любом случае нарушение воздушного пространства страны считается угрозой миру и безопасности, и государство, которому угрожает опасность, может обратиться в Совет Безопасности ООН.

Заключение

Использование беспилотных летательных аппаратов в международных конфликтах в качестве универсального оружия – очень сложная проблема. Беспилотные летательные аппараты являются оружием, но к ним не применяются положения, регулирующие контроль над вооружениями. В результате в контексте закона о военных действиях эти самолеты используются как боевые или иные средства в соответствии с методом ведения войны.

По этой причине международное сообщество настаивает на том, что использование беспилотников должно регулироваться в соответствии с положениями Устава ООН и международного права. Использование этого типа летательных аппаратов должно осуществляться в соответствии с фундаментальными положениями международного гуманитарного права, включая принципы разделения, достоинства, пропорциональности и осторожности. Следует также учитывать вопросы территориальной целостности, суверенитета государства и воздушного пространства страны.

В данной статье мы рассмотрели проблему нарушения воздушного пространства стран беспилотниками с точки зрения международного права. Основными источниками в этой сфере служат положения международного воздушного права, особенно Чикагской конвенции, и международное гуманитарное право с такими важными положениями, как запрет на бессмысленные жертвы и принцип пропорциональности. Существуют также многосторонние меры экспортного контроля, ограничения, регулирующие беспилотники в различных областях применения (международное воздушное право и отношения между суверенными государствами, международное гуманитарное право и защита гражданского населения).

Все это помогает лучше понять текущую ситуацию с БПЛА в международном праве.

Таким образом, при использовании интеллектуального, управляемого и роботизированного оружия, способного автоматически принимать решения, такого как беспилотники, в связи с неоднозначностью соблюдения принципов разделения и пропорциональности необходимо пересмотреть существующие конвенции или установить новые правовые стандарты в отношении этого вида оружия.

Кроме того, сложнее, чем для классического оружия, решается и вопрос индивидуальной уголовной ответственности в случае совершения международных преступлений странами, владеющими этим вооружением. Однако не подлежит сомнению, что ответственность за созданные ситуации несут исполнительные агенты и операторы дистанционного управления этими видами оружия.

Список литературы

- Abeyratne, R. I. (2010). *Aviation Security Law*. Springer Berlin, Heidelberg. <https://doi.org/10.1007/978-3-642-11703-9>
- Ambos, K. (December 14, 2011). Article 25: *Individual Criminal Responsibility: Commentary on the Rome statute of the International Criminal Court*, Second edition (pp. 743–770), O. Triffterer, ed., München, 2008.
- Askerbekov, D., Garza-Reyes, J. A., Ghatak, R. R., Joshi, R., Kandasamy, J., & De Mattos Nascimento, D. L. (2024). Embracing drones and the Internet of drones systems in manufacturing – An exploration of obstacles. *Technology in Society*, 78, 102648. <https://doi.org/10.1016/j.techsoc.2024.102648>
- Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. *Telecommunications Policy*, 48(4), 102739. <https://doi.org/10.1016/j.telpol.2024.102739>
- Bassi, E. (2019). European drones regulation: today's legal challenges. In *International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 443–450). <https://doi.org/10.1109/icuas.2019.8798173>
- Chen, H., & Wang, Y. Li (2009). A survey of autonomous control for UAV. In *International Conference on Artificial Intelligence and Computational Intelligence*, Shanghai, China. 2009 (pp. 267–271). <https://doi.org/10.1109/AICI.2009.147>
- Clarke, R. (2014). The regulation of civilian drones' impacts on behavioural privacy. *Computer Law & Security Report*, 30(3), 286–305. <https://doi.org/10.1016/j.clsr.2014.03.005>
- Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Report*, 30(3), 263–285. <https://doi.org/10.1016/j.clsr.2014.03.007>
- Dolata, M., & Schwabe, G. (2023). Moving beyond privacy and airspace safety: Guidelines for just drones in policing. *Government Information Quarterly*, 40(4), 101874. <https://doi.org/10.1016/j.giq.2023.101874>
- Ishiwatari, M. (2024). Leveraging drones for effective disaster management: A comprehensive analysis of the 2024 Noto Peninsula earthquake case in Japan. *Progress in Disaster Science*, 23, 100348. <https://doi.org/10.1016/j.pdisas.2024.100348>
- Li, X., & Dang, A. (2024). Spatial Patterns of Drone Adoption: Insights from Communities in Southern California. *Technological Forecasting & Social Change*, 203, 123391. <https://doi.org/10.1016/j.techfore.2024.123391>
- Majd, N., Savari, H., & Fakheri, N. (2021). Legal Rules Governing the Flying of Drones in Air Warfare from the Perspective of International Law. *Public Law Studies Quarterly*, 51(3), 1203–1221. <https://doi.org/10.22059/jplsq.2019.283487.2042>
- Nelson, J., & Gorichanaz, T. (2019). Trust as an ethical value in emerging technology governance: The case of drone regulation. *Technology in Society*, 59, 101131. <https://doi.org/10.1016/j.techsoc.2019.04.007>
- Niu, B., Zhang, J., & Xie, F. (2024). Drone logistics' resilient development: impacts of consumer choice, competition, and regulation. *Transportation Research. Part A: Policy and Practice*, 185, 104126. <https://doi.org/10.1016/j.tra.2024.104126>
- Rainer, D. (2014). Rules, regulations and codes for drones, unmanned aerial vehicle, NextGen Air Transportation, unmanned air systems. *Journal of Chemical Health & Safety*, 21(6), 34–35. <https://doi.org/10.1016/j.jchas.2014.09.003>

- Siddiqi, M. A., Iwendi, C., Jaroslava, K., & Anumbe, N. (2022). Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. *Mathematical Biosciences and Engineering*, 19(3), 2641–2670. <https://doi.org/10.3934/mbe.2022121>
- Sopha, B. M., Asih, A. M. S., & Agriawan, J. I. (2024). Adopters and non-adopters of drones in humanitarian operations: An empirical evidence from a developing country. *Progress in Disaster Science*, 21, 100314. <https://doi.org/10.1016/j.pdisas.2024.100314>
- Tatsidou, E., Tsiamis, C., Karamagioli, E., Boudouris, G., Pikoulis, A., Kakalou, E., & Pikoulis, E. (2019). Reflecting upon the humanitarian use of unmanned aerial vehicles (drones). *Swiss Medical Weekly*, 149(1314), w20065. <https://doi.org/10.4414/smw.2019.20065>
- Vogel, R. J. (2011). Drone Warfare and the Law of Armed Conflict. *Denver Journal of International Law and Policy*, 39(1), 101–138.
- Wang, S., Zheng, C., & Wandelt, S. (2024). Policy challenges for coordinated delivery of trucks and drones. *Journal of the Air Transport Research Society*, 2, 100001. <https://doi.org/10.1016/j.jatrs.2024.100001>
- Zègre-Hemsey, J. K., Cheskes, S., Johnson, A. M., Rosamond, W. D., Cunningham, C. J., Arnold, E., Schierbeck, S., & Claesson, A. (2024). Challenges & barriers for real-time integration of drones in emergency cardiac care: Lessons from the United States, Sweden, & Canada. *Resuscitation Plus*, 17, 100554. <https://doi.org/10.1016/j.resplu.2024.100554>

Сведения об авторе



Милад Каши Камиджани – магистр в области публичного права, факультет права, Университет Кума

Адрес: Иран, 3716146611, г. Кум, бульвар Аль-Гадир

E-mail: Mkk1377@gmail.com

ORCID ID: <https://orcid.org/0009-0008-1640-3230>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/ISU-4107-2023>

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

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.87 / Международное право

Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 13 октября 2023 г.

Дата одобрения после рецензирования – 1 ноября 2023 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:341:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2024.34>

Violation of the Airspace of Countries by Unmanned Aerial Vehicles (Drones) from the Perspective of International Law

Milad Kashi Kamijani

University of Qom, Qom, Iran

Keywords

airspace,
armed conflict,
digital technologies,
drone,
human rights,
humanitarian law,
international convention,
international law,
law,
unmanned aerial vehicle

Abstract

Objective: to illustrate the challenges to international law and the shortcomings of current regulation caused by the rapid development of drone technology, by the example of using unmanned aerial vehicles (drones) in airspace.

Methods: the study is based primarily on a set of methods for interpreting the provisions of international law, which allow analyzing the provisions in the field of using unmanned aerial vehicles (drones).

Results: based on international air law and humanitarian law, the article examines the issues of unmanned aerial vehicles (drones) using airspace. The main sources of law in this area are analyzed, including the provisions of international air law, especially the Paris, Madrid, Havana and Chicago Conventions. An attempt is made to answer the questions arising from the development of unmanned technologies as to which rules of international law apply to their use and whether existing international law is capable of responding effectively to them. The article shows the current understanding of the legal status of airspace over the territory of a state. The author puts forward the question whether the sphere of unmanned aerial vehicles, automatic and autonomous weapons, which combines scientific and military achievements with new technologies, is exceptional. In this regard, the problem of using unmanned aerial vehicles as a universal weapon in international conflicts is touched upon. A conclusion is made that the use of intelligent, guided and robotic weapons capable of automatic

© Kamijani M. K., 2024

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.

decision-making, such as drones, requires the revision of existing conventions or the establishment of new legal standards for these weapons. It is proposed to consider such drones as military aircraft of a special type.

Scientific novelty: international legal responsibility of states for the military use of drones has not received an unambiguous assessment in the doctrine. However, much in this issue depends on the legal interpretation of the most important international legal categories. Further development of this issue is directly related to the issues of international responsibility and the concept of state sovereignty over airspace.

Practical significance: the development of unmanned aviation at the present stage demonstrates the imperfection of the existing legal framework, which is designed to regulate these relations. With regard to the study of the global trend in the current international law, the identification of the shortcomings in the provisions of the latter is important primarily for their further modernization, taking into account modern scientific achievements and the development of the concept of a state sovereignty over its airspace.

For citation

Kamijani, M. K. (2024). Violation of the Airspace of Countries by Unmanned Aerial Vehicles (Drones) from the Perspective of International Law. *Journal of Digital Technologies and Law*, 2(3), 674–689. <https://doi.org/10.21202/jdtl.2024.34>

References

- Abeyratne, R. I. (2010). *Aviation Security Law*. Springer Berlin, Heidelberg. <https://doi.org/10.1007/978-3-642-11703-9>
- Ambos, K. (December 14, 2011). Article 25: *Individual Criminal Responsibility: Commentary on the Rome statute of the International Criminal Court*, Second edition (pp. 743–770), O. Triffterer, ed., München, 2008.
- Askerbekov, D., Garza-Reyes, J. A., Ghatak, R. R., Joshi, R., Kandasamy, J., & De Mattos Nascimento, D. L. (2024). Embracing drones and the Internet of drones systems in manufacturing – An exploration of obstacles. *Technology in Society*, 78, 102648. <https://doi.org/10.1016/j.techsoc.2024.102648>
- Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. *Telecommunications Policy*, 48(4), 102739. <https://doi.org/10.1016/j.telpol.2024.102739>
- Bassi, E. (2019). European drones regulation: today's legal challenges. In *International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 443–450). <https://doi.org/10.1109/icuas.2019.8798173>
- Chen, H., & Wang, Y. Li (2009). A survey of autonomous control for UAV. In *International Conference on Artificial Intelligence and Computational Intelligence*, Shanghai, China. 2009 (pp. 267–271). <https://doi.org/10.1109/AICI.2009.147>
- Clarke, R. (2014). The regulation of civilian drones' impacts on behavioural privacy. *Computer Law & Security Report*, 30(3), 286–305. <https://doi.org/10.1016/j.clsr.2014.03.005>
- Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Report*, 30(3), 263–285. <https://doi.org/10.1016/j.clsr.2014.03.007>
- Dolata, M., & Schwabe, G. (2023). Moving beyond privacy and airspace safety: Guidelines for just drones in policing. *Government Information Quarterly*, 40(4), 101874. <https://doi.org/10.1016/j.giq.2023.101874>
- Ishiwatari, M. (2024). Leveraging drones for effective disaster management: A comprehensive analysis of the 2024 Noto Peninsula earthquake case in Japan. *Progress in Disaster Science*, 23, 100348. <https://doi.org/10.1016/j.pdisas.2024.100348>
- Li, X., & Dang, A. (2024). Spatial Patterns of Drone Adoption: Insights from Communities in Southern California. *Technological Forecasting & Social Change*, 203, 123391. <https://doi.org/10.1016/j.techfore.2024.123391>

- Majd, N., Savari, H., & Fakheri, N. (2021). Legal Rules Governing the Flying of Drones in Air Warfare from the Perspective of International Law. *Public Law Studies Quarterly*, 51(3), 1203–1221. <https://doi.org/10.22059/jplsq.2019.283487.2042>
- Nelson, J., & Gorichanaz, T. (2019). Trust as an ethical value in emerging technology governance: The case of drone regulation. *Technology in Society*, 59, 101131. <https://doi.org/10.1016/j.techsoc.2019.04.007>
- Niu, B., Zhang, J., & Xie, F. (2024). Drone logistics' resilient development: impacts of consumer choice, competition, and regulation. *Transportation Research. Part A: Policy and Practice*, 185, 104126. <https://doi.org/10.1016/j.tra.2024.104126>
- Rainer, D. (2014). Rules, regulations and codes for drones, unmanned aerial vehicle, NextGen Air Transportation, unmanned air systems. *Journal of Chemical Health & Safety*, 21(6), 34–35. <https://doi.org/10.1016/j.jchas.2014.09.003>
- Siddiqi, M. A., Iwendi, C., Jaroslava, K., & Anumbe, N. (2022). Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. *Mathematical Biosciences and Engineering*, 19(3), 2641–2670. <https://doi.org/10.3934/mbe.2022121>
- Sopha, B. M., Asih, A. M. S., & Agriawan, J. I. (2024). Adopters and non-adopters of drones in humanitarian operations: An empirical evidence from a developing country. *Progress in Disaster Science*, 21, 100314. <https://doi.org/10.1016/j.pdisas.2024.100314>
- Tatsidou, E., Tsiamis, C., Karamagioli, E., Boudouris, G., Pikoulis, A., Kakalou, E., & Pikoulis, E. (2019). Reflecting upon the humanitarian use of unmanned aerial vehicles (drones). *Swiss Medical Weekly*, 149(1314), w20065. <https://doi.org/10.4414/smw.2019.20065>
- Vogel, R. J. (2011). Drone Warfare and the Law of Armed Conflict. *Denver Journal of International Law and Policy*, 39(1), 101–138.
- Wang, S., Zheng, C., & Wandelt, S. (2024). Policy challenges for coordinated delivery of trucks and drones. *Journal of the Air Transport Research Society*, 2, 100001. <https://doi.org/10.1016/j.jatrs.2024.100001>
- Zègre-Hemsey, J. K., Cheskes, S., Johnson, A. M., Rosamond, W. D., Cunningham, C. J., Arnold, E., Schierbeck, S., & Claesson, A. (2024). Challenges & barriers for real-time integration of drones in emergency cardiac care: Lessons from the United States, Sweden, & Canada. *Resuscitation Plus*, 17, 100554. <https://doi.org/10.1016/j.resplu.2024.100554>

Author information



Milad Kashi Kamijani – Master of Public Law, Faculty of Law, University of Qom

Address: Al-Ghadir Boulevard, after Quds Town, 3716146611 Qom, Iran

E-mail: Mkk1377@gmail.com

ORCID ID: <https://orcid.org/0009-0008-1640-3230>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/ISU-4107-2023>

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

Conflict of interests

The author declares no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – October 13, 2023

Date of approval – November 1, 2023

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научная статья

УДК 34:004:341:004.4

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

DOI: <https://doi.org/10.21202/jdtl.2024.35>

Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений

Валентина Петровна Талимончик

Российский государственный университет правосудия, Санкт-Петербург, Россия

Ключевые слова

интеграционные объединения,
международное право,
право,
правосудие,
разрешение споров,
спор,
суд,
Суд Евразийского
экономического союза,
судья,
цифровые технологии

Аннотация

Цель: проведение анализа компетенции и процедуры рассмотрения дел судами интеграционных объединений, позволяющих им разрешать споры, связанные с информационными технологиями, и определение перспектив рассмотрения этой категории споров судами интеграционных объединений.

Методы: использованы основные методы исследования – анализ, синтез и проблемно-теоретический метод.

Результаты: выявлены основные особенности категории «споры, связанные с цифровыми технологиями» применительно к специфике разрешения споров с участием частных лиц судами интеграционных объединений, а также потенциальные возможности для ряда судов интеграционных объединений разрешать споры, связанные с информационными технологиями, которые обеспечиваются особенностями компетенции судов, допускающей обращение частных лиц, а также процедуры разрешения споров, включающей привлечение экспертов. Доказано изменение категории «споры, связанные с цифровыми технологиями» как связанной не только с технологиями, но и информационно-коммуникационными системами, посредством анализа международных договоров и практики судов интеграционных объединений; в результате собственных суждений автора выявлено содержание споров, связанных с цифровыми технологиями, в отношении судов интеграционных объединений.

Научная новизна: в работе выявлены особенности категории «споры, связанные с цифровыми технологиями» в отношении судов интеграционных объединений и перспективы разрешения споров, связанных с информационными технологиями, судами интеграционных объединений.

Практическая значимость: выводы, данные в статье, могут быть использованы при совершенствовании практики судов интеграционных объединений.

© Талимончик В. П., 2024

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

Талимончик, В. П. (2024). Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений. *Journal of Digital Technologies and Law*, 2(3), 690–710. <https://doi.org/10.21202/jdtl.2024.35>

Содержание

Введение

1. Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений на Африканском континенте
 - 1.1. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости общего рынка Восточной и Южной Африки
 - 1.1.1. Особенности компетенции Суда справедливости общего рынка Восточной и Южной Африки
 - 1.1.2. Особенности процедуры Суда КОМЕСА, позволяющие разрешать споры, связанные с цифровыми технологиями
 - 1.2. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости Восточноафриканского сообщества
 - 1.2.1. Анализ наличия компетенции Суда справедливости Восточноафриканского сообщества по рассмотрению споров, связанных с цифровыми технологиями
 - 1.2.2. Особенности процедуры Суда справедливости Восточноафриканского сообщества, позволяющие разрешать споры, связанные с цифровыми технологиями
 - 1.3. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости Западноафриканского экономического и валютного сообщества
 - 1.3.1. Анализ наличия компетенции Суда справедливости Западноафриканского экономического и валютного сообщества по рассмотрению споров, связанных с цифровыми технологиями
 - 1.3.2. Особенности процедуры Суда ЭКОВАС, позволяющие разрешать споры, связанные с цифровыми технологиями
 - 1.4. Проблема возможности разрешения споров, связанных с цифровыми технологиями, судами иных интеграционных объединений на Африканском континенте
 - 1.4.1. Проблема возможности разрешения споров, связанных с цифровыми технологиями, Трибуналом сообщества развития Южной Африки
 - 1.4.2. Проблема возможности разрешения споров, связанных с цифровыми технологиями, Судом справедливости Центральноафриканского экономического и валютного сообщества

2. Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений Южной Америки
 - 2.1. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости Андского сообщества
 - 2.1.1. Анализ наличия компетенции Суда справедливости Андского сообщества по рассмотрению споров, связанных с цифровыми технологиями
 - 2.1.2. Особенности процедуры Суда справедливости Андского сообщества, позволяющие разрешать споры, связанные с цифровыми технологиями
 - 2.2. Проблема возможности разрешения споров, связанных с цифровыми технологиями, в рамках иных интеграционных объединений Южной Америки
 - 2.2.1. Проблема возможности разрешения споров, связанных с цифровыми технологиями, Судом справедливости Карибского сообщества
 - 2.2.2. Проблема возможности разрешения споров, связанных с цифровыми технологиями, в рамках Меркосур
 3. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом Евразийского экономического союза
 - 3.1. Анализ наличия компетенции Суда Евразийского экономического союза по рассмотрению споров, связанных с цифровыми технологиями
 - 3.2. Особенности процедуры Суда Евразийского экономического союза, позволяющие разрешать споры, связанные с цифровыми технологиями
- Заключение
- Список литературы

Введение

Традиционно вопрос разрешения споров, связанных с технологиями, относится к деятельности Комиссии ООН по праву международной торговли (далее – ЮНСИТРАЛ). 12–16 февраля 2024 г. в Нью-Йорке прошла 79-я сессия Рабочей группы II ЮНСИТРАЛ¹.

На 80-ю сессию, планировавшуюся 30 сентября – 4 октября 2024 г. в Вене, представлен определенный итоговый документ². ЮНСИТРАЛ уже пришла к определенным результатам применительно к деятельности международных коммерческих арбитражей.

¹ Рабочая группа II Комиссии ООН по праву международной торговли (ЮНСИТРАЛ) «Урегулирование споров» приняла документ «Урегулирование споров, связанных с технологиями, и адьюдикация: типовые оговорки и пояснительные тексты».

² Проект типовых оговорок ЮНСИТРАЛ об экспресс-урегулировании споров на основании заключения специалиста (СпецЭУС).

Во-первых, разработана категория спора, связанного с технологиями. Она включает самые различные категории, обусловленные «высокими» технологиями, во всех отраслях промышленности и сферы услуг. Информационные технологии отдельно не выделены.

Во-вторых, подготовлены общие типовые оговорки. Например, оговорка применительно к арбитражу содержит применение Правил ускоренного арбитража ЮНСИТРАЛ с изменениями об ускоренном назначении арбитра компетентной институцией, ускоренном проведении консультаций со сторонами, удобном месте и языке разбирательства.

В-третьих, ведется работа над оговоркой о заключении специалиста. Предлагается оговорка о назначении независимых технических консультантов. Для отбора технического консультанта арбитраж проводит консультации в отношении области специализации и круга ведения для специалиста. Стороны вправе высказывать замечания относительно разъяснений, данных техническим консультантом.

В целом ЮНСИТРАЛ близка к завершению формирования системы разрешения споров, связанных с технологиями, возникающих из международных сделок.

С 2021 г. Всемирная организация интеллектуальной собственности (далее – ВОИС) занимается передовыми технологиями³. Центр ВОИС по арбитражу и посредничеству рассматривает споры, связанные с ИКТ, и потенциально может решать вопросы, касающиеся информационно-коммуникационных систем. В отличие от ЮНСИТРАЛ, которая занимается разрешением споров, связанных с технологиями, международными коммерческими арбитражами, Центр ВОИС предложил эффективное досудебное урегулирование такого рода споров.

С 1 июля 2021 г. действует новая редакция Правил экспертного заключения ВОИС. Заключение понимается как решение, вынесенное экспертом в соответствии со ст. 17 Правил по вопросу, отнесенному к экспертному исследованию. Статья 17 Правил устанавливает, что эксперт может принять решение на основе, без ограничений: 1) любой информации, представленной сторонами; 2) компетентности эксперта; 3) любой другой информации, которую эксперт сочтет относящейся к делу. Эксперт может после консультаций со сторонами принять временное или частичное решение.

Компетенция ЮНСИТРАЛ и ВОИС не может касаться международных судебных учреждений. Международные судебные учреждения характеризуются отдельной правовой основой их деятельности, узкой компетенцией и не составляют систему.

В настоящее время активно действуют международные судебные учреждения по разрешению споров между государствами и частными лицами. Суды различных интеграционных объединений потенциально могут рассматривать споры, связанные с технологиями.

³ Они охватывают цифровые технологии (интернет вещей (IoT), блокчейн, метавселенные, искусственный интеллект (ИИ), включая генеративный ИИ (GenAI), большие данные и облачные вычисления) и физические технологии (автономное вождение, 3D-печать и аппаратные инновации).

Весьма многочисленны суды интеграционных объединений на Африканском континенте⁴. В практике судов интеграционных объединений можно использовать признаки споров, связанных с технологиями, разработанные ЮНСИТРАЛ⁵.

Споры, связанные с информационными технологиями, рассматриваемые в рамках интеграционных объединений, исследованы неполно. Практике Суда ЕС посвящено исследование Томаса Шоу (Shaw, 2016).

Фундаментальные исследования Криса Рида и Джона Энджела (Reed & Angel, 2007), Эндрю Мюррея (Murray, 2010), Томаса Смедингхоффа (Smedinghoff, 2000), Дайаны Ровланд и Элизабет Макдоналд (Rowland & Macdonald, 2005), Дайаны Ровланд, Уты Кёхл и Эндрю Чарльзуорта (Rowland et al., 2017) по праву информационных технологий содержат разделы о коммерческих доменных спорах.

Тщательный анализ судебной практики, преимущественно национальной, мы находим у Дина Армстронга, Фергюса Маккомби и Кери Дэвис (Armstrong et al., 2021).

В исследовании Фэй Фанфэй Вана (Wang, 2014) специальный раздел посвящен электронным коммерческим спорам.

Исследования по правовому регулированию «передовых» технологий Т. Хьерена и Б. Колани (Hoeren & Kolany, 2018), М. Бурри (Burri, 2021), Шин-и Пенга, Шин-фу Лина и Т. Стрейнза (Peng et al., 2021), С. Честермана (Chesterman, 2021), М. Компангуччи (Compagnucci, 2020), М. Ковач (Kovac, 2020), Н. Ребе (Rebe, 2021) не касаются деятельности судов интеграционных объединений.

Достаточно обширная научная литература по правовым аспектам блокчейна также не затрагивает проблему разрешения споров, связанных с технологиями, судами интеграционных объединений, так как интеграционная политика в этой области только формируется (Cappiello & Carullo, 2021; Herian, 2018; Stabile & Prior, 2020; Bambara & Allen, 2018; Fox & Green, 2019; Barker, 2020).

Поскольку практика Суда ЕС, в том числе связанная с цифровыми технологиями, всегда подвергается тщательному доктринальному анализу, в настоящем исследовании основное внимание будет уделено интеграционным объединениям Африки и Южной Америки. Анализ будет проводиться по двум вопросам: 1) позволяет ли компетенция судов интеграционных объединений рассматривать споры, связанные с цифровыми технологиями; 2) учитывают ли процессуальные правила судов интеграционных объединений особенности такого рода споров, а именно сокращенные процессуальные сроки и участие специалистов.

⁴ Суд справедливости общего рынка Восточной и Южной Африки; Суд справедливости Восточно-Африканского сообщества; Суд справедливости Центрально-Африканского экономического и валютного сообщества; Суд справедливости Западно-Африканского экономического и валютного сообщества; Трибунал сообщества развития Южной Африки.

⁵ В Проектах положений об урегулировании споров, связанных с технологиями, подготовленных ЮНСИТРАЛ, приведены примеры споров, возникающих в различных отраслях: аэрокосмической промышленности, аудиотехнологиях, автомобилестроении или средств обеспечения мобильности, в сфере искусственного интеллекта, биотехнологий, производства компьютеров, электроники, информационных технологий, медицинских приборов, военных/оборонных нанотехнологий, ядерной физики, фотоники, робототехники, полупроводников, телекоммуникаций, фармацевтических и финансовых технологий. Все эти споры неразрывно связаны с экономической интеграцией.

1. Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений на Африканском континенте

1.1. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости общего рынка Восточной и Южной Африки

1.1.1. Особенности компетенции Суда справедливости общего рынка Восточной и Южной Африки

Для определения компетенции Суда справедливости общего рынка Восточной и Южной Африки (далее – Суд КОМЕСА) по рассмотрению определенной категории споров следует обратиться к Договору КОМЕСА⁶. Также для определения компетенции Суда КОМЕСА по рассмотрению споров, связанных с цифровыми технологиями, следует определить категорию «цифровые технологии».

В настоящее время термин «технологии» в словосочетании «цифровые технологии» является условным. Наряду с устоявшимся термином «информационно-коммуникационные технологии» (далее – ИКТ) в него должны быть включены информационно-коммуникационные системы⁷.

Характерно, что ИКТ и информационно-коммуникационные системы (далее – ИКС) непосредственно разрабатываются частными субъектами, которые вступают в разного рода контрактные отношения. ИКТ сопровождают информацию на всем протяжении ее «жизненного цикла», который связан с разнообразными спорами. При создании информации споры касаются прав на интеллектуальную собственность⁸. При введении ИКТ в оборот заключаются различные контракты услуг (на внедрение, техническую поддержку)⁹. Споры могут быть связаны не только с контрактами, но и с использованием ИКТ без разрешения разработчика.

Для информационно-коммуникационных систем также характерно понятие жизненного цикла¹⁰. Как и в отношении ИКТ, использование

⁶ Treaty establishing the Common market for Eastern and Southern Africa. <https://clck.ru/3DsBHS>

⁷ Искусственный интеллект, большие данные, нейронные сети, распределенные реестры и иные системы, которые относительно автономны от человека.

⁸ Если программное обеспечение, база данных или технология в виде секрета производства создаются по заказу.

⁹ ИКТ как инструмент используются для поиска, получения, распространения, передачи, хранения, преобразования, систематизации, уничтожения информации и доступа к ней, для чего оператор поисковой системы, владелец сайта, лицо, с которым связана информация, вступают в правоотношения, по которым могут возникать споры.

¹⁰ Резолюция Генеральной конференции Организации Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) «Рекомендация об этических аспектах искусственного интеллекта», принятая на 41-й сессии, проходившей в Париже с 9 по 24 ноября 2021 г., определяет понятие жизненного цикла искусственной интеллектуальной системы: вся совокупность этапов, начиная с этапов исследования, проектирования и создания и заканчивая этапами развертывания и использования, к которому относятся техническое обслуживание, эксплуатация, сбыт, финансирование, мониторинг и оценка эффективности, контроль работоспособности, вывод из эксплуатации, демонтаж и утилизация.

информационно-коммуникационных систем опосредуется различными контрактами. Например, на этапе исследования, проектирования и создания информационно-коммуникационной системы это трудовые и подрядные контракты либо также инвестиционные. При развертывании информационно-коммуникационной системы могут потребоваться агенты и дистрибьюторы, поэтому использование ИКС связано с различными контрактами услуг¹¹. После развертывания такой системы не исключены различные виды деликтов, включая недобросовестную конкуренцию.

Следует констатировать, что споры, связанные с цифровыми технологиями, возникают преимущественно в сфере международного частного права. В публично-правовую сферу они переносятся, если: 1) международное публичное право допускает обращение частных лиц в международное судебное учреждение; 2) международный договор, определяющий круг ведения международного судебного учреждения, затрагивает вопросы, связанные с ИКТ и информационно-коммуникационными системами.

Анализ Раздела 5 Договора КОМЕСА позволяет выделить категории дел, по которым в Суд КОМЕСА могут обращаться частные лица. Во-первых, любое лицо, имеющее место жительства или место нахождения в государстве-члене, может обратиться в Суд КОМЕСА за обжалованием актов органов КОМЕСА при исчерпании национальных средств защиты. Во-вторых, Суд КОМЕСА выполняет также функцию арбитража по частным контрактам.

Договор КОМЕСА определяет общие¹² и специальные цели и задачи Общего рынка. Специальные цели сформулированы для отдельных областей сотрудничества. В сфере коммуникаций предполагается развивать такое сотрудничество, которое способствовало бы производству товаров и облегчало торговлю товарами и услугами, а также передвижение людей. В области промышленности поставлены цели устранить жесткость в структурах производства, с тем чтобы обеспечить высокое качество товаров и услуг, конкурентоспособных на Общем рынке, а также создать надлежащие благоприятные условия для участия частного сектора в экономическом развитии и сотрудничестве в рамках Общего рынка, осуществлять сотрудничество в области промышленного развития. Сотрудничество в информационной сфере отдельно не выделено. Вопросы поддержки передовых технологий могут быть решены в рамках промышленного развития.

¹¹ Контракты на услуги по техническому обслуживанию, обеспечению эксплуатации, мониторингу и оценке эффективности, контролю работоспособности, а также выводу из эксплуатации, демонтажу и утилизации.

¹² К общим целям, в частности, относятся: 1) достижение устойчивого роста и развития государств-членов путем содействия более сбалансированному и гармоничному развитию их производственных и маркетинговых структур; 2) содействие совместному развитию во всех областях экономической деятельности и совместному принятию макроэкономической политики и программ для повышения уровня жизни своих народов и укрепления более тесных отношений между своими государствами-членами; 3) сотрудничество в создании благоприятных условий для иностранных, трансграничных и внутренних инвестиций, в том числе совместное поощрение исследований в целях развития; 4) укрепление отношений между Общим рынком и остальным миром и выработка общих позиций на международных форумах. Эти цели сформулированы настолько широко, что не требуют адаптации к потребностям развития информационно-коммуникационных систем.

1.1.2. Особенности процедуры Суда КОМЕСА, позволяющие разрешать споры, связанные с цифровыми технологиями

Правила процедуры Суда КОМЕСА 2016 г.¹³ учитывают возможность участия эксперта в судебном разбирательстве. Они предусматривают специальную просьбу заявителя о назначении экспертизы. Предусмотрено особое правило для опроса эксперта: если он уведомляет Секретаря Суда по крайней мере за пятнадцать дней до слушания о том, что он или она не в состоянии адекватно изъясняться на одном из языков Суда КОМЕСА, Суд может разрешить эксперту давать свои показания на английском или другом языке и должен обеспечить устный перевод. В случае если какое-либо лицо вызвано для дачи показаний в качестве эксперта, Секретарь может назначить разумное вознаграждение за время, затраченное как на дачу показаний, так и на выполнение любой работы по делу. Характерно, что процедура экспертизы отдельно не урегулирована, статус эксперта аналогичен статусу свидетеля.

Правила процедуры Суда КОМЕСА 2016 г. объективно не могут учитывать сокращенные сроки разбирательств по спорам, связанным с информационными технологиями, поскольку не выделяют отдельно данную категорию споров¹⁴. В целом объем дел, рассмотренных Судом КОМЕСА с участием юридических лиц, незначителен.

1.2. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости Восточноафриканского сообщества

1.2.1. Анализ наличия компетенции Суда справедливости Восточноафриканского сообщества по рассмотрению споров, связанных с цифровыми технологиями

Раздел 8 Договора о создании Восточноафриканского сообщества 1999 г.¹⁵ регулирует статус Суда справедливости Восточноафриканского сообщества, который является судебным органом, который обеспечивает соблюдение права при толковании, применении и соблюдении положений Договора 1999 г.

Применительно к участию частных лиц Суд справедливости Восточноафриканского сообщества рассматривает обращения: 1) частных лиц о правомерности любого акта государства-участника на том основании, что оно нарушает договор; 2) сторон коммерческих контрактов, если в их соглашениях содержится арбитражная оговорка, предоставляющая юрисдикцию Суду.

Целью Сообщества является разработка политики и программ, направленных на расширение и углубление сотрудничества между государствами-членами в политической, экономической, социальной и культурной областях, исследованиях и технологиях, обороне, безопасности, а также в правовой и судебно-правовой сферах для их взаимной выгоды. Как следствие, исследования и технологии выделены в отдельное направление сотрудничества.

¹³ COMESA Court of Justice. <https://clck.ru/3DsBdr>

¹⁴ В качестве примеров дел, рассмотренных Судом КОМЕСА с участием юридических лиц, можно привести: *Malawi Mobile Limited vs COMESA*; *Malawi Mobile Limited Vs Government of the Republic of Malawi & Malawi Communication Regulatory Authority*.

¹⁵ East African Court of Justice. (1999). The Treaty. <https://clck.ru/3DsBez>

Для достижения общей цели Сообщество, в частности, обеспечивает: 1) устойчивый рост и развитие региона; 2) учет гендерной проблематики во всех его начинаниях и повышение роли женщин в культурном, социальном, политическом, экономическом и технологическом развитии; 3) укрепление партнерских отношений с частным сектором и гражданским обществом в целях достижения устойчивого социально-экономического и политического развития. Восточноафриканское сообщество отличается четкая ориентированность на развитие, что способствует расширению компетенции Суда этого интеграционного объединения.

1.2.2. Особенности процедуры Суда справедливости Восточноафриканского сообщества, позволяющие разрешать споры, связанные с цифровыми технологиями

Суд справедливости Восточноафриканского сообщества работает очень активно. Коллегия первой инстанции рассмотрела на текущий момент 179 дел, Апелляционная коллегия – 53 дела, из которых дела по обращениям физических и юридических лиц – наиболее частые. Например, в деле *Chester House Limited v. the Attorney General of the Republic of Uganda & 3 others* рассматривался вопрос защиты иностранных инвестиций.

Договором 1999 г., Правилами процедуры Суда справедливости Восточноафриканского сообщества 2019 г.¹⁶ установлены определенные нормы для обращений частных лиц. Договор 1999 г. устанавливает краткий срок для обращения частных лиц: разбирательство должно быть начато в течение двух месяцев с момента вступления в силу, публикации, директивы, решения или действия, на которые подана жалоба, или со дня, когда об этом стало известно заявителю жалобы. Стороны могут быть представлены адвокатом, имеющим право предстать перед верховным судом любого из государств-членов.

Главы VII и XII Правил процедуры устанавливают порядок рассмотрения дел. Предусмотрено участие эксперта. Стороны могут ознакомиться с заключением эксперта в Секретариате и получить копии за свой счет. В случае с любым лицом, вызванным Судом для дачи показаний в качестве эксперта, Секретарь может назначить разумное вознаграждение за время, затраченное как на дачу показаний, так и на выполнение любой работы по делу. Детально процедура привлечения эксперта не регламентируется. Эксперта привлекает не Суд, а заинтересованные стороны.

1.3. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости Западноафриканского экономического и валютного сообщества

1.3.1. Анализ наличия компетенции Суда справедливости Западноафриканского экономического и валютного сообщества по рассмотрению споров, связанных с цифровыми технологиями

Суд справедливости Западноафриканского экономического и валютного сообщества (далее – Суд ЭКОВАС) принимает к рассмотрению индивидуальные жалобы с 2005 г.

¹⁶ East African Court of Justice. (2019). Rules of procedures 2019. <https://clck.ru/3DsBoz>

Договор об экономическом сообществе западноафриканских государств (ЭКОВАС) 1975 г.¹⁷ включал мандат Суда Сообщества на рассмотрение споров, связанных с толкованием и действием Договора. Правила функционирования Суда были установлены Протоколом о Суде Сообщества 1991 г. Суд начал функционировать в декабре 2000 г.

Дополнительный протокол ЭКОВАС 2005 г.¹⁸ установил правила приемлемости заявлений, включив в них споры между частными лицами и их собственными государствами-членами. Суд ЭКОВАС включал следующие подразделения: административный трибунал ЭКОВАС, суд по правам человека, арбитражный суд и межгосударственный трибунал по разрешению споров.

Согласно ст. 4 Протокола 2005 г., право на обращение в Суд ЭКОВАС имеют физические и юридические лица. Для обращения в Суд ЭКОВАС нет необходимости в исчерпании внутренних средств правовой защиты.

Договор ЭКОВАС определяет общую цель объединения без ее конкретизации¹⁹. Он определяет также средства достижения цели, которые могут способствовать и развитию информационно-коммуникационных систем в регионе²⁰.

ЭКОВАС уделяет основное внимание экономической интеграции, но выделяет сферу информации в отдельную область сотрудничества.

1.3.2. Особенности процедуры Суда ЭКОВАС, позволяющие разрешать споры, связанные с цифровыми технологиями

Согласно Правилам процедуры Суда ЭКОВАС, вступившим в силу с 1 января 2022 г.²¹, Суд может использовать заключение эксперта. В постановлении о назначении эксперта должна быть определена его задача и установлен срок, в течение которого он должен подготовить свое заключение.

¹⁷ ECOWAS. <https://clck.ru/3DsBxo>

¹⁸ Supplementary Protocol A/SP.1/01/05 amending the preamble and articles 1, 2, 9 AND 30 of Protocol A/P.1/7/91 relating to the community Court of Justice and article 4 paragraph 1 of the english version of the Said Protocol. <https://clck.ru/3DsByp>

¹⁹ Целью ЭКОВАС является содействие сотрудничеству и интеграции, ведущих к созданию экономического союза в Западной Африке для повышения уровня жизни ее народов, а также для поддержания и укрепления экономической стабильности, укрепления отношений между государствами-членами и содействия прогрессу и развитию Африканского континента.

²⁰ В числе средств достижения цели названы: 1) гармонизация и координация национальной политики и содействие интеграционным программам, проектам и мероприятиям, в том числе в областях промышленности и связи, а также информации, науки, технологий; 2) содействие созданию совместных производственных предприятий; 3) устранение в отношениях между государствами-членами препятствий для свободного передвижения людей, услуг и капитала; 4) создание экономического союза; 5) содействие созданию совместных предприятий предприятиями частного сектора и другими экономическими операторами; 6) гармонизация стандартов; 7) поощрение распространения информации, особенно среди сельского населения, женских и молодежных организаций и социально-профессиональных объединений, таких как ассоциации средств массовой информации, деловых мужчин и женщин, работников и профсоюзов.

²¹ Community Court of Justice, ECOWAS (The Economic Community of West African States) rules of the Community Court of Justice of the Economic Community of West African States (ECOWAS). <https://clck.ru/3DsBzs>

Эксперт должен получить копию постановления Суда вместе со всеми документами, необходимыми для выполнения его исследования. Он должен находиться под наблюдением судьи-докладчика, который может присутствовать при его исследовании и который должен быть проинформирован о ходе выполнения им своей задачи. Суд может потребовать от сторон или одной из них внести обеспечение расходов на заключение эксперта. После того как эксперт сделает свое заключение, Суд может распорядиться о его допросе, предварительно уведомив стороны о необходимости его присутствия. Перед выполнением своей задачи эксперт должен принести следующую присягу в письменной форме или в суде: «Я клянусь или заявляю, что буду добросовестно и беспристрастно выполнять свою задачу». Если одна из сторон возражает против эксперта на том основании, что он не является компетентным или надлежащим лицом для выполнения функций эксперта, или по любой другой причине, или если эксперт отказывается давать показания, приносить присягу, данный вопрос должен быть разрешен судом.

Таким образом, Правила процедуры Суда ЭКОВАС, вступившие в силу с 1 января 2022 г., наиболее полно отражают специфику споров, связанных с цифровыми технологиями.

1.4. Проблема возможности разрешения споров, связанных с цифровыми технологиями, судами иных интеграционных объединений на Африканском континенте

1.4.1. Проблема возможности разрешения споров, связанных с цифровыми технологиями, Трибуналом сообщества развития Южной Африки

Трибунал САДК учрежден в соответствии со ст. 9 Договора о САДК²². Ранее он рассматривал споры с участием частных лиц. Дела, переданные на рассмотрение Трибунала САДК, затрагивали экспроприацию частной собственности государствами. В деле Mike Campbell (Pvt) LTD и другие против Зимбабве, дело № SADC (T) 2/2007, Основное решение от 28 ноября 2008 г., права заявителя были нарушены в результате экспроприации его частной собственности без компенсации. При рассмотрении дела Трибунал САДК руководствовался принципами международного права в области прав человека, а не применял какой-либо конкретный договор по правам человека.

После решений, вынесенных им против правительства Зимбабве по этому делу и связанным с ним делам, деятельность Трибунала была приостановлена. Далее последовал процесс пересмотра его компетенции. Новый протокол 2014 г. о Трибунале призван пересмотреть мандат Трибунала, ограничив его рассмотрением споров только с участием государств. Как следствие, Трибунал САДК был лишен возможности рассмотрения споров с участием частных субъектов, связанных с цифровыми технологиями.

²² Southern African Development Community. (2021). SADC Treaty. <https://clck.ru/3DsFEk>

1.4.2. Проблема возможности разрешения споров, связанных с цифровыми технологиями, Судом справедливости Центральноафриканского экономического и валютного сообщества

Статья 5 Договора об учреждении Центральноафриканского экономического и валютного сообщества (СЕМАК) 1994 г.²³ устанавливает, что судебная палата Суда СЕМАК обеспечивает толкование Договора СЕМАК и последующих конвенций.

В отношении потенциальной возможности разрешения споров с участием частных лиц Суд обеспечивает правомерность решений, директив и нормативных актов институтов Сообщества, отдельно обращения частных лиц не выделены.

Полномочия по рассмотрению других споров могут быть предоставлены Суду решениями, принятыми Конференцией глав государств и правительств.

2. Перспективы рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений Южной Америки

2.1. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом справедливости Андского сообщества

2.1.1. Анализ наличия компетенции Суда справедливости Андского сообщества по рассмотрению споров, связанных с цифровыми технологиями

Компетенция Суда справедливости Андского сообщества определена Соглашением о создании Суда справедливости Андского сообщества 1996 г.²⁴ Она включает споры с участием частных лиц²⁵.

Иск о признании недействительным акта Андского сообщества должен быть подан в течение двух лет с даты его вступления в силу. Если этот срок истек, любая из сторон судебного разбирательства, переданного национальным судам, может обратиться к национальному суду с ходатайством о признании решения органа Андского сообщества неприменимым к конкретному делу.

Картахенское соглашение 1969 г.²⁶ определяло общую цель Андского сообщества²⁷. Были предусмотрены механизмы и меры по достижению цели интеграции, в том числе: 1) принятие совместных программ, реализация промышленных программ и средств промышленной интеграции; 2) осуществление программ в области услуг и либерализация внутрирегиональной торговли услугами; 3) принятие

²³ Traite instituant la Communauté Économique et Monétaire de l'Afrique Centrale (Texte authentique). <https://clck.ru/3DsFJE>

²⁴ Treaty creating the court of justice of the andean community. <https://clck.ru/3DsFL7>

²⁵ Физические или юридические лица могут подать иск о признании недействительными решений, принятых Андским Советом министров иностранных дел или Комиссией Андского сообщества, резолюций Генерального секретариата или соглашений, которые затрагивают их субъективные права или законные интересы.

²⁶ Andean Subregional Integration Agreement (Cartagena Agreement). <https://clck.ru/3DsFMs>

²⁷ Содействие сбалансированному и гармоничному развитию государств-участников на равноправных условиях посредством интеграции и социально-экономического сотрудничества; ускорение их экономического роста; содействие их участию в процессе региональной интеграции с перспективой постепенного формирования Латиноамериканского общего рынка.

и реализация программ содействия научно-техническому развитию. Последняя мера позволяет Андскому сообществу функционировать в условиях развития передовых технологий.

2.1.2. Особенности процедуры Суда справедливости Андского сообщества, позволяющие разрешать споры, связанные с цифровыми технологиями

Привлечение экспертов весьма ограничено регламентируется Статутом Суда справедливости Андского сообщества²⁸. Стороны с предварительного разрешения Трибунала могут участвовать в слушании через экспертов только в тех случаях, когда речь идет о выяснении вопросов технического характера. В ходе слушания председатель и судьи могут допросить экспертов. Таким образом, экспертов привлекают стороны.

Вместе с тем в Андском сообществе создана региональная система охраны интеллектуальной собственности, что повлекло активную деятельность Суда справедливости Андского сообщества по разрешению подобного рода споров. В базе WIPO Lex находится 117 решений Суда справедливости Андского сообщества по вопросам интеллектуальной собственности. Например, в 2024 г. Суд справедливости Андского сообщества выступил в качестве последней инстанции в спорах по защите авторского права *Carlos Alberto Massó Vasco vs Caracol Televisión S.A., Entidad de Gestión Colectiva de Derechos de Productores Audiovisuales de Colombia vs IA TRIP S.A.S. (propietaria del establecimiento hotelero Hotel Picasso Inn)*. Учитывая опыт Суда справедливости Андского сообщества в отношении «традиционных» телекоммуникаций, споры в сфере интеллектуальной собственности и передовых технологий вряд ли вызовут существенные затруднения.

2.2. Проблема возможности разрешения споров, связанных с цифровыми технологиями, в рамках иных интеграционных объединений Южной Америки

2.2.1. Проблема возможности разрешения споров, связанных с цифровыми технологиями, Судом справедливости Карибского сообщества

Договор об учреждении Карибского сообщества (далее – КАРИКОМ) 1973 г.²⁹ не предусматривал создание Суда сообщества. Впоследствии Договор был пересмотрен.

Созданный в 2001 г. Суд справедливости Карибского сообщества обладает юрисдикцией как суда первой инстанции, так и апелляционной. В рамках своей апелляционной юрисдикции Суд выступает в качестве суда последней инстанции по гражданским и уголовным делам для тех государств, которые признали его апелляционную юрисдикцию. Как суд первой инстанции он применяет нормы международного права в отношении толкования и применения пересмотренного Чагуарамасского договора. Соглашение об учреждении Карибского суда 2001 г.³⁰ не предусматривает обращений частных лиц, однако Суд справедливости Карибского сообщества

²⁸ Estatuto del Tribunal de Justicia de la Comunidad Andina. <https://clck.ru/3DsFTt>

²⁹ Treaty Establishing the Caribbean Community. <https://clck.ru/3DsFVu>

³⁰ Agreement establishing the Caribbean Court of Justice. <https://clck.ru/3DsFXT>

в 2008 г. в деле двух юридических лиц против Гайаны сам признал такого рода свою компетенцию.

Несмотря на отсутствие четких договорных положений, позволяющих установить компетенцию Суда справедливости Карибского сообщества по рассмотрению споров, касающихся цифровых технологий, его правила в значительной степени приспособлены к рассмотрению такого рода споров. В частности, Правила первоначальной юрисдикции Карибского суда 2021 г.³¹ регулируют ряд вопросов экспертизы: важнейшую обязанность эксперта в суде – помогать Суду беспристрастно решать вопросы, имеющие отношение к компетенции эксперта; порядок осуществления этой обязанности; содержание заключения эксперта; право эксперта обращаться в суд за указаниями; полномочия суда по ограничению экспертного заключения; полномочия суда назначать одного эксперта; последствия непредоставления заключения эксперта. В целом столь подробная регламентация привлечения эксперта не только способствует разрешению споров, связанных с информационными технологиями, но могла бы быть учтена и в работе ЮНСИТРАЛ по этой тематике.

2.2.2. Проблема возможности разрешения споров, связанных с цифровыми технологиями, в рамках Меркосур

Договор о создании Общего рынка между Аргентинской Республикой, Федеративной Республикой Бразилией, Республикой Парагвай и Восточной Республикой Уругвай (Асунсьонский договор) 1991 г.³² не предусматривал возможности участия частных лиц в механизме разрешения споров в рамках Меркосур. Государства-участники путем заключения Асунсьонского договора приняли решение о создании Общего рынка до 31 декабря 1994 г. Общий рынок должен был включать в том числе свободное перемещение услуг, координацию макроэкономической и отраслевой политики государств-участников в области промышленности, услуг и любых других сферах, которые могут быть согласованы. Как следствие, сфера информации, телекоммуникаций, включая ИКТ, не была выделена в структуре общего рынка и отдельно не регулировалась.

Бразильский и Оливосский протоколы устанавливали процедуры по разрешению споров, касающихся толкования, применения или несоблюдения Асунсьонского договора или любого из его протоколов, решений органов Меркосур. Однако механизм рассмотрения обращений юридических и физических лиц не был разработан. Физические лица могут подавать жалобы только в Национальные отделения Группы Общего рынка того государства-участника, в котором они проживают. Отсутствие единого механизма разрешения споров в рамках Меркосур препятствует разрешению споров, связанных с информационными технологиями.

³¹ Caribbean Court of Justice. Original Jurisdiction Rules 2021. <https://clck.ru/3DsFdd>

³² Treaty Establishing a Common Market between the Argentine Republic, the Federal Republic of Brazil, the Republic of Paraguay and the Eastern Republic of Uruguay (Treaty of Asuncion). <https://clck.ru/3DsFeY>

3. Перспективы рассмотрения споров, связанных с цифровыми технологиями, Судом Евразийского экономического союза

3.1. Анализ наличия компетенции Суда Евразийского экономического союза по рассмотрению споров, связанных с цифровыми технологиями

Суд Евразийского экономического союза (далее – Суд ЕАЭС) обладает компетенцией по разрешению споров с участием частных лиц – хозяйствующих субъектов в отношении актов ЕЭК, которые в том числе могут быть связаны с информационными технологиями.

Возможность рассмотрения споров, связанных с информационными технологиями, определена спецификой компетенции ЕЭК³³. Потенциал по разрешению споров, связанных с информационно-коммуникационными системами, вытекает из ряда актов ЕАЭС³⁴.

Кроме того, ряд «услуг информационного общества» вошел в перечень секторов, в которых обеспечивается свобода движения услуг и единая политика³⁵. Потенциально споры, связанные с данными категориями услуг, могут разрешаться Судом ЕАЭС.

Специальные виды услуг регулируются общими положениями о едином рынке услуг (Консультативное заключение Суда ЕАЭС от 10 июля 2020 г.). Специальные нормы в отношении «услуг информационного общества» в праве ЕАЭС отсутствуют.

3.2. Особенности процедуры Суда Евразийского экономического союза, позволяющие разрешать споры, связанные с цифровыми технологиями

Статут Суда ЕАЭС предусматривает Специализированные экспертные группы только для разрешения споров, касающихся поддержки сельского хозяйства, промышленных субсидий, специальных торговых мер. Споры, связанные с цифровыми технологиями, не выделены в отдельную категорию споров, требующих создания Специализированных групп.

Для этих трех категорий споров выделены требования к экспертам: 1) высокая квалификация, знания и опыт в отношении предмета спора; 2) независимость; 3) отсутствие конфликта интересов.

³³ Комиссия, в частности, осуществляет деятельность в следующих сферах: 1) конкурентная политика; 2) взаимная торговля услугами и инвестиции; 3) интеллектуальная собственность. Во всех этих сферах могут возникать вопросы, связанные с использованием информационных технологий.

³⁴ Технологии искусственного интеллекта включены в Перечень приоритетных видов экономической деятельности для промышленного сотрудничества государств – членов ЕАЭС, утвержденный Решением Евразийского межправительственного совета от 27 ноября 2018 г. № 9, а также Перечень «отраслей будущего», утвержденный Распоряжением Евразийского межправительственного совета от 7 марта 2017 г. № 2.

³⁵ Согласно Решению Высшего Евразийского экономического совета от 23 декабря 2014 г. № 110, в перечень секторов единого рынка услуг, в частности, вошли: 1) услуги, связанные с базами данных, в том числе предоставления информации на веб-сайтах; предоставления услуг по поиску данных и другой информации из информационных ресурсов; 2) услуги предоставления помощи по поддержанию компьютерных систем в рабочем состоянии; их технического обслуживания, улучшения программ.

Вместе с тем правила судопроизводства в Суде ЕАЭС допускают участие экспертов, включая экспертов Специализированных групп, а также специалистов. Но только экспертам Специализированных групп предоставляются иммунитеты.

Эксперт или специалист обладают рядом прав³⁶. Они представляют письменное заключение по поставленным вопросам. Эксперт, специалист не могут участвовать в рассмотрении спора, в котором они ранее участвовали в ином качестве.

Общий срок для вынесения решения в Суде ЕАЭС составляет не позднее 90 дней со дня поступления заявления, ввиду чего Суд ЕАЭС может оперативно разрешать споры, связанные с цифровыми технологиями.

Заключение

По итогам проведенного исследования можно сделать следующие выводы.

Термин «споры, связанные с цифровыми технологиями» сложносоставной и охватывает не только споры, связанные с ИКТ, но и споры, связанные с информационно-коммуникационными системами в целом.

Эта категория споров включает споры, связанные с цифровыми технологиями, возникающие из международных контрактов и внедоговорных отношений между частными субъектами, рассматриваемые национальными судами в соответствии с правилами международной подсудности, а также международными коммерческими арбитражами, и споры, рассматриваемые международными судебными учреждениями, одной из сторон в которых могут являться частные лица. Потенциально возможно возникновение споров, связанных с цифровыми технологиями, в межгосударственных отношениях.

Суды ряда интеграционных объединений (за исключением Трибунала сообщества развития Южной Африки, Суда справедливости Центральноафриканского экономического и валютного сообщества и Меркосур) потенциально могут рассматривать споры, связанные с цифровыми технологиями, а Суд справедливости Андского сообщества активно рассматривает споры по защите интеллектуальной собственности, в том числе в связи с ИКТ. Возможность рассмотрения споров, связанных с цифровыми технологиями, судами интеграционных объединений обеспечивается особенностями их компетенции, допускающей обращение частных лиц, а также процедуры разрешения споров, включающей привлечение экспертов. Однако принцип транспарентности их деятельности не позволяет соблюдать конфиденциальность такого рода разбирательств, а вопрос сокращения сроков рассмотрения споров, связанных с цифровыми технологиями, может быть решен только в весьма отдаленной перспективе.

Список литературы

- Armstrong, D., McCombie, F., & Davis, C. (2021). *Cyber Litigation: The Legal Principles*. New York: Bloomsbury Professional Ltd.
- Bambara, J., & Allen, P. (2018). *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw-Hill Education.

³⁶ Знакомиться с материалами дела, относящимися к предмету экспертизы; задавать вопросы другим лицам, участвующим в споре; заявлять ходатайства о предоставлении дополнительных материалов для дачи заключения.

- Barker, R. (Ed.) (2020). *The Law and Governance of Decentralised Business Models: Between Hierarchies and Markets*. London: Routledge.
- Burri, M. (2021). *Big Data and Global Trade Law*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108919234>
- Cappiello, B., & Carullo, G. (Eds.) (2021). *Blockchain, Law and Governance*. London: Springer. <https://doi.org/10.1007/978-3-030-52722-8>
- Chesterman, S. (2021). *We, the Robots?: Regulating Artificial Intelligence and the Limits of the Law*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781009047081>
- Compagnucci, M. C. (2020). *Big Data, Databases and "Ownership" Rights in the Cloud*. London: Springer. <https://doi.org/10.1007/978-981-15-0349-8>
- Fox, D., & Green, S. (Eds.) (2019). *Cryptocurrencies in Public and Private Law*. Oxford: Oxford University Press.
- Herian, R. (2018). *Regulating Blockchain: Law, Technology and the Ethics of Political Economy*. London: Routledge. <https://doi.org/10.4324/9780429489815>
- Hoeren, T., & Kolany, B. (Eds.) (2018). *Big Data in Context Legal, Social and Technological Insights*. London: Springer. <https://doi.org/10.1007/978-3-319-62461-7>
- Kovac, M. (2020). *Judgement-Proof Robots and Artificial Intelligence A Comparative Law and Economics Approach*. London: Springer/Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-53644-2>
- Murray, A. (2010). *Information Technology Law: the law and society*. Oxford: Oxford University Press.
- Peng, S-Y., Lin, C-F., & Streinz, T. (Eds.) (2021). *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108954006>
- Rebe, N. (2021). *Artificial Intelligence: Robot Law, Policy and Ethics*. Leiden: Brill – Nijhoff. <https://doi.org/10.1163/9789004458109>
- Reed, C., & Angel, J. (Eds.) (2007). *Computer Law: the Law and Regulation of Information Technology*. Oxford: Oxford University Press.
- Rowland, D., Kohl, U., & Charlesworth, A. (2017). *Information Technology Law* (5th ed.). London: Routledge.
- Rowland, D., & Macdonald, E. (2005). *Information technology law* (3rd ed.). Abingdon: Cavendish Publishing Ltd.
- Shaw, T. J. (2016). *Information and Internet Law: Global Practice*. Createspace Independent Publishing Platform.
- Smedinghoff, T. J. (2000). *Online Law*. New York: Pearson Education Corporation.
- Stabile, D., & Prior, K. (2020). *Digital Assets and Blockchain Technology: U.S. Law and Regulation*. Cheltenham: Edward Elgar Publishing Limited.
- Wang, F. F. (2014). *Law of Electronic Commercial Transactions. Contemporary Issues in the EU, US and China*. New York: Routledge. <https://doi.org/10.4324/9780203628812>

Сведения об авторе



Талимончик Валентина Петровна – доктор юридических наук, доцент, профессор кафедры общетеоретических правовых дисциплин, Северо-Западный филиал Российского государственного университета правосудия

Адрес: 197046, Россия, г. Санкт-Петербург, Александровский парк, 5

E-mail: talim2008@yandex.ru

ORCID ID: <https://orcid.org/0000-0002-5302-460X>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57190001688>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/H-1253-2013>

Google Scholar ID: <https://scholar.google.com/citations?user=7EluYwgAAAAJ>

РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=447740

Конфликт интересов

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

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.87 / Международное право

Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 10 июня 2024 г.

Дата одобрения после рецензирования – 1 июля 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Research article

UDC 34:004:341:004.4

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

DOI: <https://doi.org/10.21202/jdtl.2024.35>

Prospects of Handling Digital Technology Disputes by Courts of Integration Associations

Valentina P. Talimonchik

Russian State University of Justice, Saint Petersburg, Russia

Keywords

Court of the Eurasian Economic Union, court, digital technologies, dispute resolution, dispute, integration associations, international law, judge, justice, law

Abstract

Objective: to analyze the competence and procedure of case handling by the courts of integration associations, allowing them to resolve disputes related to information technologies, and to identify the prospects of handling of this category of disputes by the courts of integration associations.

Methods: the main research methods were analysis, synthesis, and problem-theoretical method.

Results: the article identified the main features of the “disputes related to digital technologies” category in relation to resolving disputes involving individuals by the courts of integration associations. It reveals opportunities for some courts of integration associations to resolve disputes related to information technologies. The said opportunities are provided by the courts competence, allowing the appeal of individuals, as well as by the dispute resolution procedure involving experts. By analyzing international treaties and practice of courts of integration associations, the author proves that the changes in the category of “disputes related to digital technologies” are related not only to technologies, but also to information and communication systems. By own judgments, the author reveals the content of disputes related to digital technologies in the courts of integration associations.

Scientific novelty: the paper reveals the peculiarities of the category “disputes related to digital technologies” in relation to the courts of integration associations and the prospects of resolving disputes related to information technologies by the courts of integration associations.

Practical significance: the conclusions provided in the article can be used to improve the practice of courts of integration associations.

© Talimonchik V. P., 2024

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

Talimonchik, V. P. (2024). Prospects of Handling Digital Technology Disputes by Courts of Integration Associations. *Journal of Digital Technologies and Law*, 2(3), 690–710. <https://doi.org/10.21202/jdtl.2024.35>

References

- Armstrong, D., McCombie, F., & Davis, C. (2021). *Cyber Litigation: The Legal Principles*. New York: Bloomsbury Professional Ltd.
- Bambara, J., & Allen, P. (2018). *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw-Hill Education.
- Barker, R. (Ed.) (2020). *The Law and Governance of Decentralised Business Models: Between Hierarchies and Markets*. London: Routledge.
- Burri, M. (2021). *Big Data and Global Trade Law*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108919234>
- Cappiello, B., & Carullo, G. (Eds.) (2021). *Blockchain, Law and Governance*. London: Springer. <https://doi.org/10.1007/978-3-030-52722-8>
- Chesterman, S. (2021). *We, the Robots?: Regulating Artificial Intelligence and the Limits of the Law*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781009047081>
- Compagnucci, M. C. (2020). *Big Data, Databases and "Ownership" Rights in the Cloud*. London: Springer. <https://doi.org/10.1007/978-981-15-0349-8>
- Fox, D., & Green, S. (Eds.) (2019). *Cryptocurrencies in Public and Private Law*. Oxford: Oxford University Press.
- Herian, R. (2018). *Regulating Blockchain: Law, Technology and the Ethics of Political Economy*. London: Routledge. <https://doi.org/10.4324/9780429489815>
- Hoeren, T., & Kolany, B. (Eds.) (2018). *Big Data in Context Legal, Social and Technological Insights*. London: Springer. <https://doi.org/10.1007/978-3-319-62461-7>
- Kovac, M. (2020). *Judgement-Proof Robots and Artificial Intelligence A Comparative Law and Economics Approach*. London: Springer/Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-53644-2>
- Murray, A. (2010). *Information Technology Law: the law and society*. Oxford: Oxford University Press.
- Peng, S-Y., Lin, C-F., & Streinz, T. (Eds.) (2021). *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108954006>
- Rebe, N. (2021). *Artificial Intelligence: Robot Law, Policy and Ethics*. Leiden: Brill – Nijhoff. <https://doi.org/10.1163/9789004458109>
- Reed, C., & Angel, J. (Eds.) (2007). *Computer Law: the Law and Regulation of Information Technology*. Oxford: Oxford University Press.
- Rowland, D., Kohl, U., & Charlesworth, A. (2017). *Information Technology Law* (5th ed.). London: Routledge.
- Rowland, D., & Macdonald, E. (2005). *Information technology law* (3rd ed.). Abingdon: Cavendish Publishing Ltd.
- Shaw, T. J. (2016). *Information and Internet Law: Global Practice*. Createspace Independent Publishing Platform.
- Smedinghoff, T. J. (2000). *Online Law*. New York: Pearson Education Corporation.
- Stabile, D., & Prior, K. (2020). *Digital Assets and Blockchain Technology: U.S. Law and Regulation*. Cheltenham: Edward Elgar Publishing Limited.
- Wang, F. F. (2014). *Law of Electronic Commercial Transactions. Contemporary Issues in the EU, US and China*. New York: Routledge. <https://doi.org/10.4324/9780203628812>

Author information



Valentina P. Talimonchik – Dr. Sci. (Law), Associate Professor, Professor of the Department of General Theoretical Legal Disciplines, North-West branch of the Russian State University of Justice

Address: 5 Aleksandrovskiy park, 197046 Saint Petersburg, Russia

E-mail: talim2008@yandex.ru

ORCID ID: <https://orcid.org/0000-0002-5302-460X>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57190001688>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/H-1253-2013>

Google Scholar ID: <https://scholar.google.com/citations?user=7EluYwgAAAAJ>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=447740

Conflict of interests

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

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – June 10, 2024

Date of approval – July 1, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024



Научный обзор

УДК 34:004:347.211:004.383.8.032.26

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

DOI: <https://doi.org/10.21202/jdtl.2024.36>

Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии

Ян Корнехо

Независимый исследователь, Гуаякиль, Эквадор

Ключевые слова

законодательство,
нейроправа,
нейротехнологии,
неприкосновенность
частной жизни,
персональные данные,
права человека,
право,
психологическая автономия,
цифровые технологии,
этика

Аннотация

Цель: представить результаты проведенного систематического обзора исследований влияния нейротехнологий на юридические концепции и нормативную правовую базу, направленные на решение этических и социальных проблем, связанных с защитой индивидуальных прав, неприкосновенности частной жизни и психологической автономии.

Методы: систематический обзор литературы проводился по методологии, предложенной известным британским ученым – почетным профессором Университета Кила Барбарой Китченхэм, отличающейся гибкостью и эффективностью в получении результатов. Поиск осуществлялся на англо- и испаноязычных сайтах по ключевым словам («нейротехнологии», «персональные данные», «психологическая конфиденциальность», «нейроправа», «нейротехнологические вмешательства» и «нейротехнологическая дискриминация») с использованием таких поисковых систем, как Google Scholar и Redib, а также баз данных Scielo, Dialnet, Redalyc, Lilacs, Scopus, Medline и Pubmed. Фокус данного исследования – библиометрические данные – характеризуется как неэкспериментальный, кросс-секционный и описательный с применением контент-анализа на основе модели PRISMA.

Результаты: в представленном исследовании подчеркивается необходимость установления четких этических принципов, защищающих права личности и способствующих ответственному использованию нейротехнологий; выявлен ряд проблем психологической автономии, таких как ненадлежащее обращение с информацией, отсутствие гарантий юридической безопасности, нарушение прав и свобод на примере отношений в медицинской сфере. Исследование показывает необходимость адаптации существующей нормативной правовой базы для решения этических и социальных проблем, возникающих в связи с появлением новых нейротехнологий. Отмечается, что широкое исследование вопросов в сфере нейротехнологий будет способствовать защите прав человека.

© Ан Корнехо Я., 2024

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: предложено расширенное понимание пяти нейроправ в рамках Всеобщей декларации прав человека; нейроправа представлены как новая категория прав, направленных на защиту психологической целостности от неправомерного использования нейротехнологий; обосновано принятие таких принципов технократии, как личная идентичность, свобода воли, психологическая конфиденциальность, равноправный доступ и защита от предвзятости.

Практическая значимость: полученные результаты имеют значение для понимания современных юридических концепций, связанных с нейроправами, адаптации существующих нормативных правовых актов для решения этических и социальных проблем, возникающих в связи с появлением новых технологий, защиты нейроправ человека и ответственности за их нарушение. Исследование данной проблемы имеет ключевое значение для обеспечения дальнейшего ответственного развития и применения нейротехнологий.

Для цитирования

Корнехо, Я. (2024). Нейроправа, нейротехнологии и персональные данные: обзор проблем психологической автономии. *Journal of Digital Technologies and Law*, 2(3), 711–728. <https://doi.org/10.21202/jdtl.2024.36>

Содержание

Введение

1. Нейроправа, нейротехнологии, их этические и правовые последствия

1.1. Нейроправа

1.2. Нейротехнологии

1.3. Этические и правовые проблемы

1.3.1. Психологическая конфиденциальность

1.3.2. Психологическая целостность

1.3.3. Личная идентичность

1.3.4. Когнитивная свобода

2. Методология

2.1. Критерии включения и исключения

2.2. Популяция и выборка

3. Результаты исследования

3.1. Сбор и анализ данных

3.2. Обсуждение результатов

Заключение

Список литературы

Введение

Стремительное развитие нейротехнологий открыло беспрецедентные возможности для понимания и улучшения функционирования человеческого мозга. Однако этот прогресс также породил значительные этические и социальные проблемы, связанные с защитой прав личности, неприкосновенности частной жизни и психологической автономии.

В связи с этим возникает необходимость создания концептуальной и практической основы для ответственного развития и применения этих технологий. По определению Moisés Barrio, нейроправа – это цифровые права граждан, которые могут осуществляться с одинаковой эффективностью как в цифровой среде, так и за ее пределами (Arellano, 2024; Parlatino, 2023; Fukushi, 2024).

В Испании Хартия цифровых прав является основополагающим элементом для признания прав в цифровой среде, которые не заменяют основные права, также известные как права человека или индивидуальные гарантии. Важно отметить, что концепция нейроправ не создает новых основных прав, а скорее описывает и уточняет изменяющуюся природу цифровой среды, предлагая тем самым признать новые права человека, чтобы адаптироваться к этим изменениям (González, 2021; Hsu, 2024).

В этико-правовой сфере Goering et al. (2021) определяют нейроправа как «концептуальную и практическую основу для ответственного развития и применения нейротехнологий», подчеркивая необходимость установления четких этических принципов, защищающих права личности и способствующих ответственному использованию нейротехнологий (Gómez, 2021).

В то же время Filirova (2022) описывает их как «развивающуюся область, которая изучает этические и правовые проблемы, связанные с разработкой и применением нейротехнологий», подчеркивая важность надежной нормативной базы для обеспечения ответственного развития и применения этих технологий (López & Cáceres, 2022).

Обеспокоенность потенциальными этическими рисками, связанными с нейротехнологиями, разделяют многие авторы. Создание карты активности мозга (Brain Activity Map, BAP) вызвало дискуссии о психологической конфиденциальности, ответственности за наши действия в связи с достижениями в области нейротехнологий, а также о стигматизации и дискриминации, связанных с неврологическими показателями. В этом контексте искусственный интеллект, алгоритмическая предвзятость и свидетельства нейробиологии приобретают актуальность в правовой и судебной сферах (Fernández, 2023; López-Silva & Madrid, 2022; Cáceres et al., 2021; Clausen et al., 2017; Cornejo-Plaza et al., 2024).

Нейротехнологии открыли мир возможностей для понимания и улучшения функционирования человеческого мозга, но при этом ставят этические и социальные проблемы, связанные с защитой индивидуальных прав, неприкосновенности частной жизни и психологической автономии. Отсюда проблема нашего исследования: как адаптировать существующие нормативные правовые акты для решения этических и социальных проблем, возникающих в связи с появлением новых нейротехнологий? Этот вопрос имеет ключевое значение для обеспечения ответственного развития и применения нейротехнологий на благо общества.

Цель данного исследования – провести библиометрический анализ влияния нормативной правовой базы на этические и социальные проблемы, возникающие в связи с появлением новых нейротехнологий для блага человечества.

1. Нейроправа, нейротехнологии, их этические и правовые последствия

1.1. Нейроправа

Область нейроправ возникает в ответ на стремительное развитие нейротехнологий, которые способны изменить наше понимание человеческого мозга и взаимодействие с ним. Однако эти технологии также создают значительные этические и социальные проблемы, связанные с защитой индивидуальных прав, неприкосновенности частной жизни и психологической автономии (Moreu, 2022).

Первые дебаты о нейроправах начались в 1990-х гг., когда такие авторы, как Джуди Иллес (Judy Illes), начали изучать этические последствия новых методов работы с мозгом (Borbón & Borbón, 2022). В 2002 г. Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) провела конференцию по нейроэтике, на которой обсуждались проблемы и возможности нейротехнологий и отмечалась необходимость разработки этических рамок для их развития и применения.

В этом контексте концепция нейроправ становится теоретической и практической основой для решения этих проблем. Термин «нейроправа» представляет новую категорию прав, направленных на защиту психологической целостности от неправомерного использования нейротехнологий¹.

Тем не менее вызывает беспокойство тот факт, что не существует специального международного регулирования для борьбы с возможными нарушениями жизни, неприкосновенности и свободы слова в результате деятельности транснациональных корпораций, торгующих нейротехнологиями (Parlatino, 2023).

López-Silva и Madrid (2022) продемонстрировали тесную связь между терминами «умственный» и «психический», объединив их в «психологический». Кроме того, они предлагают использовать «церебральный» вместо «нейронный», учитывая сильную связь между этими двумя терминами. В этом смысле термин «умственный» тесно связан с понятием «психологической конфиденциальности», которое обычно используется для обозначения конфиденциальности нейронной информации. Однако важно понимать, что в зависимости от области применения и историко-культурного контекста эта сложная проблема может расцениваться по-разному.

По данным латиноамериканского парламента (Parlatino, 2023), система нейроправ, также известных как права мозга, – это новый международный правовой подход, который делает акцент на защите мозга и его функций в дополнение к уже установленным правам человека. Эти права включают в себя право на самоидентичность, психологическую конфиденциальность и индивидуальность. Кроме того, система содержит законодательно установленные гарантии для устранения растущих опасностей, связанных с развитием и использованием нейротехнологий применительно к людям (Moreu, 2022).

Исследования в области нейробиологии, терапевтическая практика и развитие технологий – это лишь некоторые из многочисленных областей, имеющих отношение к нейроправам (Parlatino, 2023).

¹ Universidad Santiago de Chile. (2021). Cambalache, 4. (In Spain). <https://clck.ru/3Ct9Wi>

1.2. Нейротехнологии

Нейротехнологии определяются как технологии, направленные на изучение возможностей совершенствования нервной системы человека. В настоящее время исследования и разработки позволяют выявить, какие области нервной системы нуждаются в реабилитации или помощи из-за потери функций, а также достичь реабилитации в самых основных ее функциях, например, при двигательных нарушениях (Barrios et al., 2017).

Эксперты отмечают, что термин «нейротехнологии» относится к широкому спектру методов и инструментов, которые работают совместно с мозгом и нервной системой в целом, осуществляя пассивный мониторинг или изменяя их деятельность (Andorno, 2023). Тот же автор утверждает, что преимущества нейротехнологий изучаются применительно к трудовой деятельности путем передачи мыслей на экраны без использования клавиатуры, и выражает обеспокоенность из-за существования скрытых рисков нарушения неприкосновенности частной жизни, свободы воли и человеческого достоинства.

Согласно исследованию ЮНЕСКО, нейротехнологии изучаются только в 10 странах Латинской Америки. Эта ситуация вызывает беспокойство из-за возможности неравноправного доступа к знаниям и возникновения неравенства в области здравоохранения, исследований и инноваций на благо человека².

Исследования в области работы мозга и нейротехнологий затрагивают важные проблемы. Это касается и правовых реформ, направленных на защиту нейроправ (Ruiz & Cayón, 2021), так как нейротехнологии используют методы и инструменты для связи с нервной системой.

Использование нейротехнологий предполагает не только их терапевтическое применение, но и их способность стимулировать расширение возможностей человека (Reguera & Cayón, 2021). Основной проблемой нейротехнологий является их интеграция с ИИ, поскольку это может затронуть саму сущность человека.

Кроме того, нейротехнологии могут раскрыть интимные мысли, эмоции, проявления подсознания, а также нейронной активности (Reguera & Cayón, 2021). При этом вновь возникает проблема уважения человеческого достоинства, прав и основных свобод. В большинстве стран мира уже внедрено законодательство о защите персональных данных, а также о конфиденциальности психологических данных, личной идентичности, свободе мысли.

Фактически нейротехнологии, связанные с нейроправами, рассматриваются с двух сторон: психологической конфиденциальности и права на частную жизнь, где особое внимание уделяется человеческой индивидуальности. Поэтому крайне важно, чтобы они рассматривались властями на региональном и международном уровнях (Andorno, 2023).

Таким образом, нейротехнологии выходят за рамки медицины, поскольку показывают нам возможности и проблемы когнитивных процессов, позволяя

² UNESCO. (2021). Report of the International Bioethics Committee of UNESCO (IBC) on ethical issues of neurotechnology. <https://clck.ru/3Ct9sj>

разрабатывать профилактические и терапевтические диагнозы. В этом смысле нейротехнологии получили развитие в странах Латинской Америки и Карибского бассейна, где со стороны ЮНЕСКО был проведен ряд исследований в области генома человека с участием искусственного интеллекта.

В последнее время нейротехнологии достигли больших успехов: благодаря технологии больших данных обрабатываются огромные объемы информации, а при участии искусственного интеллекта можно получить результаты в короткие сроки. Это позволяет выявлять паттерны нейронной активности или чтения мыслей, при этом этико-правовой подход применим к двум областям: отображение работы мозга (нейровизуализация) и интерфейсы «мозг – компьютер» (ICC, BCI) (Andorno, 2023).

1.3. Этические и правовые проблемы

Цель нейротехнологий – изучать неврологические механизмы психической деятельности и поведения человека, чтобы влиять на них. Это приводит к этическим и правовым ситуациям, когда они могут регулироваться в соответствии с определенными ценностями и принципами (Andorno, 2023). По этой причине ЮНЕСКО выражает обеспокоенность в отношении групп, которые требуют создания новых нейроправ или подрывают существующие.

В число нейроправ включают психологическую конфиденциальность, психологическую целостность, личную идентичность и когнитивную свободу. Рассмотрим их по отдельности.

1.3.1. Психологическая конфиденциальность

Данная область ближе других примыкает к проблеме доступа к психологическим данным. Это привело к созданию нейротехнологий, направленных на защиту от несогласованного доступа третьих лиц, будь то рекламные компании, страховщики, работодатели, государственные и другие компании, к данным о вашем мозге, а также от распространения таких данных.

Эта защита предусмотрена международными стандартами в области прав человека, включая конфиденциальность персональных данных, согласно которым не допускается произвольное вмешательство в частную жизнь, семью, жилище, честь или репутацию любого лица (ст. 12), а также поддерживается Американской конвенцией о правах человека 1969 г. (известной как Пакт Сан-Хосе-де-Коста-Рика) (Andorno, 2023).

Однако высказываются опасения, что по причинам юридического толкования законы не обеспечивают защиту психологических данных. Поэтому положения этих законов нуждаются в уточнении, чтобы обеспечить конфиденциальность указанных данных и тем самым избежать противоречий во мнениях юристов (Reguera & Cayón, 2021; Hertz, 2022; Makin et al., 2020).

Наконец, вызывает обеспокоенность то, что психологическая информация может быть использована в качестве биометрических данных, идентифицирующих человека, а в будущем – для выявления проблем с психическим здоровьем и когнитивными способностями в целях дискриминации (Arellano, 2024).

1.3.2. Психологическая целостность

Конфиденциальность психологических данных, связанных с применением нейротехнологий, имеет отношение к психологической целостности из-за ущерба, который может быть нанесен психологическим аспектам человека. Потенциальная простота электрической стимуляции с намеренным изменением ее параметров может привести к манипуляциям с устройствами интерфейса «мозг – компьютер» (Hertz, 2022; Alharbi, 2023).

Наряду с негативными последствиями есть и положительные. Например, дисциплина, называемая инженерией памяти, используется для лечения таких заболеваний, как болезнь Альцгеймера или посттравматический стресс, когда можно удалить воспоминания ради улучшения психологического здоровья пациента.

1.3.3. Личная идентичность

Личная идентичность связана с психологической целостностью индивида, который сохраняет свои характеристики с течением времени, чтобы узнавать себя и отличать от других, т. е. сохранять свою сущность (Hertz, 2022).

Лечебные процедуры или процедуры, меняющие психологическое состояние человека, могут привести к изменениям в поведении, в том числе из-за ненадлежащего или неправомерного использования устройств для стимуляции мозга. Поэтому каждый человек является субъектом прав, защищенных международными стандартами.

1.3.4. Когнитивная свобода

Эта категория связана с психологическим самоопределением, т. е. с выбором и осуществлением контроля над собственными психическими состояниями, которые могут быть изменены или обусловлены третьими лицами без их согласия (Hertz, 2022).

В этом контексте термин «свобода» был впервые использован Wrye Sententia в 2004 г. (Sententia, 2004). По мнению этого автора, право и свобода определяются собственной совестью и мыслями человека. Однако, по мнению Bublitz (Bublitz, 2013), это право изменять и улучшать собственные психические состояния, а также отказываться от использования устройств, которые могут манипулировать ими (Parlatino, 2023; Hertz, 2022).

Когнитивная свобода связана со свободой мысли, постулированной в правах человека; однако необходимо уточнить, что эта свобода включает также внутреннее измерение психологической деятельности (Andorno, 2023; Hertz, 2022).

2. Методология исследования

Цель нашего исследования – проанализировать научную литературу в области этических и социальных вопросов, связанных с нейроправами в нейротехнологиях будущего (рис. 1). Тщательный поиск проводился с использованием таких поисковых систем, как Google Scholar и Redib, а также баз данных Scielo, Dialnet, Redalyc, Lilacs, Scopus, Medline и Pubmed.

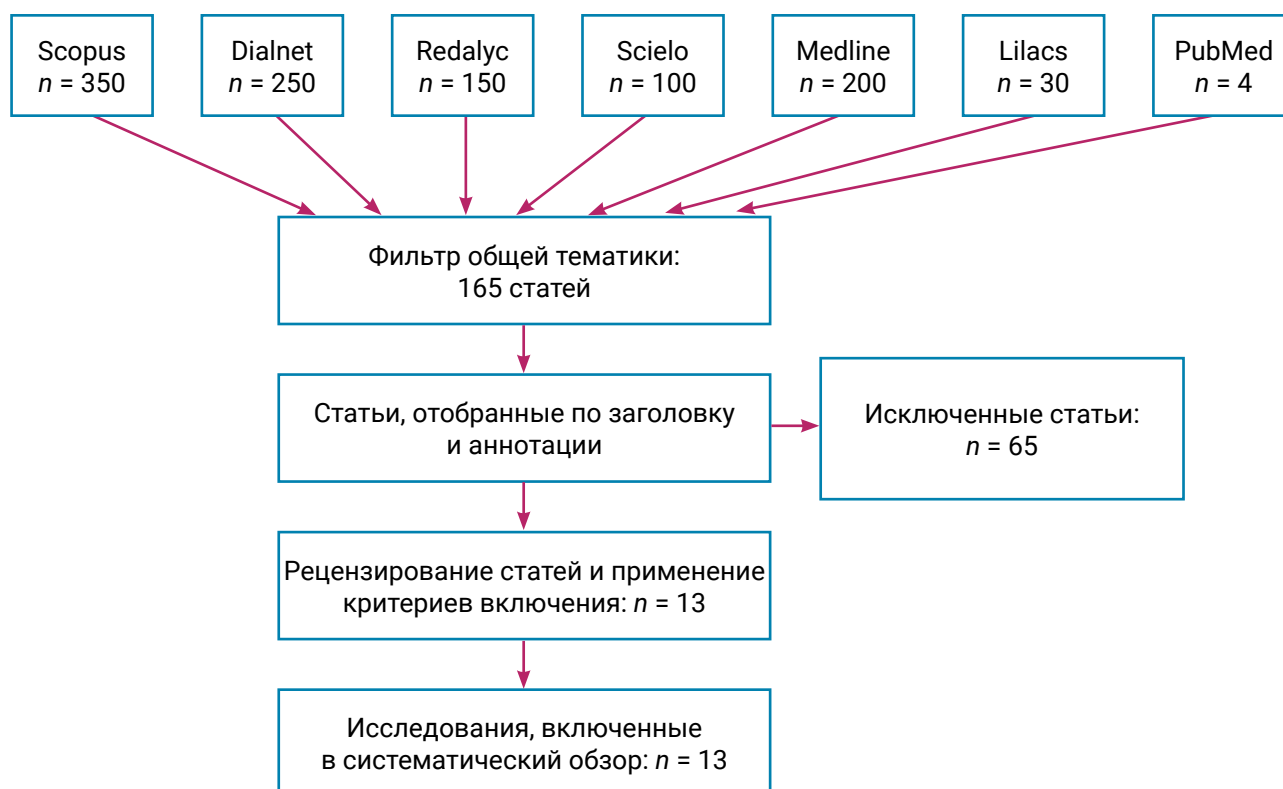


Рис. 1. Авторская разработка на основе модели PRISMA – COCHRANE

Поиск осуществлялся на англо- и испаноязычных сайтах по ключевым словам: «нейротехнологии», «персональные данные», «психологическая конфиденциальность», «нейроправа», «нейротехнологические вмешательства» и «нейротехнологическая дискриминация». Систематический обзор литературы проводился по методологии, предложенной известным британским ученым – почетным профессором Университета Кила Барбарой Китченхэм³, которая отличается гибкостью и эффективностью в получении результатов для публикации.

2.1. Критерии включения и исключения

Для оценки качества доказательств рассматривались только статьи и обзоры, написанные на английском или испанском языках (табл. 1) с участием организаций, исследователей и лиц, связанных с исследованием нейроправ. Для ответа на вопрос исследования применялся метод контент-анализа. Исключались дубликаты статей, редакционные комментарии, пресс-релизы, новости, мнения и клинические рекомендации. Были отобраны наиболее релевантные рукописи и рассмотрены полные тексты научных работ, связанных с нейроправами пациентов.

2.2. Популяция и выборка

В качестве анализируемой популяции использовались отобранные научные статьи, отвечающие критериям включения и исключения, установленным на этапе разработки, как показано в табл. 1.

³ <https://goo.su/PmZdwXj>

Таблица 1. Исследования в области нейрправ и нейротехнологий

№	Автор(ы)	Тематика	Год
1	E. Cáceres, J. Diez, E. García	Нейроэтика и нейроправа	2021
2	A. R. González	«Нейроправа», доказательства в области нейробиологии и гарантии независимости судебной власти	2021
3	M. Ienca	О нейроправах	2021
4	M. Ienca, R. Andorno	Подходы к новым правам человека в эпоху нейронауки и нейротехнологий	2021
5	S. Ruiz, V. Ramos, R. Concha, et al., C. Caneo	Негативные последствия Закона 20.584 и обсуждаемого Закона о нейроправах для научных исследований и медицинской практики в Чили: настоящая необходимость учиться на ошибках	2021
6	Y. V. Bastidas Cid	Нейротехнологии: интерфейс «мозг – компьютер» и защита данных о мозге или нейроданных в контексте обработки персональных данных в Европейском союзе	2022
7	C. López, N. Cáceres	Нейроправо как новая область защиты прав человека	2022
8	R. Orias	Нейроправа. Новый рубеж в области прав человека	2022
9	V. E. Rocha Martínez	Новые права человека	2022
10	H. Fernández	Нейроправа, нейротехнологии и управление рисками в современности. Исторический анализ, диалектика и целостный подход	2023
11	P. López-Silva, R. Madrid	Защита разума: анализ концепции психического в Законе о нейроправах	2023
12	J. I. Murillo	Можем ли мы читать мысли или контролировать поведение? Вклад Фомы Аквинского в дискуссию о нейроправах	2023
13	W. Arellano	Нейроправа и их регулирование	2024

3. Результаты исследования

Представленные в табл. 1 отобранные первичные исследования в области нейрправ и нейротехнологий отражают мнения, касающиеся ненадлежащего обращения с информацией о пациентах, отсутствия юридических гарантий безопасности и недооценки риска, что потенциально может привести к неправомерному поведению и неправильному обращению с информацией (Borbón et al., 2020).

3.1. Сбор и анализ данных

Для обобщения содержания отобранных статей в соответствии с критериями включения и исключения был применен систематический обзор литературы. Этот инструмент представляет собой открытую и понятную процедуру отбора различных статей и источников информации.

Первоначально в вышеупомянутых базах данных были использованы следующие поисковые фразы: «нейроправа», «персональные данные», «психологическая конфиденциальность», «нейротехнологическая дискриминация» и «доступ к нейробиологическим данным». В результате поиска было получено 1084 научные статьи. После анализа заголовков и аннотаций было отобрано 165 рукописей, удовлетворяющих критериям для финального рассмотрения.

Обзор литературы позволил выявить следующие права и проблемы на стыке нейрправ и персональных данных:

Проблемы:

- 1. Психологическая конфиденциальность: сбор и обработка нейробиологических данных могут угрожать психологической конфиденциальности людей.
- 2. Нейротехнологическая дискриминация: существует вероятность того, что люди будут подвергаться иному обращению из-за своих уникальных нейробиологических особенностей.
- 3. Доступ к нейробиологическим данным: защита частной жизни людей так же важна, как и развитие научных исследований, когда речь идет о доступе к нейробиологическим данным.

Права:

- 1. Право на психологическую конфиденциальность: люди имеют право знать, как собираются, используются и распространяются их нейробиологические данные.
- 2. Право на отсутствие дискриминации в области нейротехнологий: люди имеют право на равное отношение к себе независимо от их нейробиологических особенностей.
- 3. Право на доступ к нейробиологическим данным: люди имеют право просматривать нейробиологические данные, которые относятся к ним, а также данные, которые используются для обоснования суждений о них.
- 4. Право на психологическую идентичность: право иметь представление о себе, в соответствии с которым человек выбирает и поддерживает свою личную идентичность.
- 5. Право на свободу воли: способность самостоятельно делать выбор.

3.2. Обсуждение результатов

В табл. 2 приведены моральные практики, которые необходимо учитывать при оказании медицинской помощи в области нейроправ в целях сохранения и поддержания прав и свобод пациентов.

Таблица 2. Основные принципы оказания медицинской помощи в области нейроправ

№	Принципы
A	Честность
B	Свободный доступ
C	Равенство
D	Справедливость
E	Профессиональная тайна
F	Конфиденциальность информации
G	Целостность
H	Открытость
I	Информированное согласие
J	Ответственность

Компания FasterCapital⁴ провела исследование, освещающее достижения нейротехнологий в различных отраслях, включая образование и здравоохранение. Указанные технологии стимулируют инновации и повышают качество жизни людей

⁴ Neurotech Startups and the Future of Human Enhancement. URL: <https://clck.ru/3DvQJTJ>

с такими заболеваниями, как боковой амиотрофический склероз (болезнь Шарко) психологические расстройства и трудности с общением. Однако важно учитывать аспекты, связанные с конфиденциальностью, согласием и справедливым доступом к этим технологиям со стороны компаний, предоставляющих услуги. На рис. 2 показан потенциал расширения возможностей человека на основе данных, полученных компанией FasterCapital.

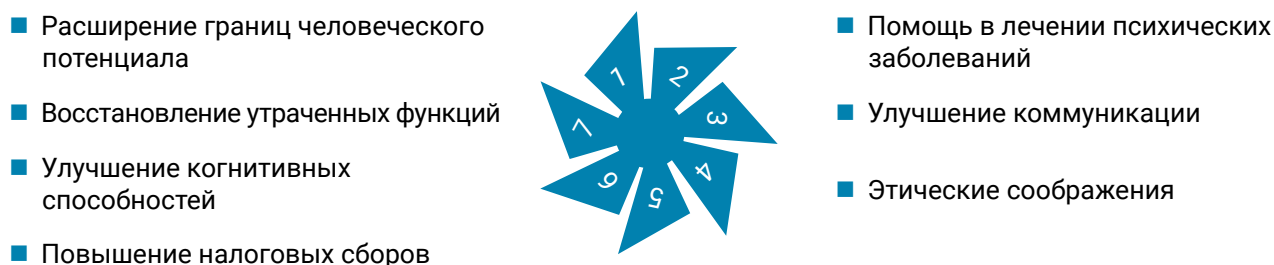


Рис. 2. Потенциал нейротехнологий для улучшения способностей человека

В систематическом обзоре представлены научные доказательства положительного влияния нейротехнологий на лечение таких заболеваний, как болезни Паркинсона, Альцгеймера; психозы, деменция, сенсорные и моторные дисфункции центральной нервной системы, а также на борьбу с болью. Нейротехнологические вмешательства могут стать эффективным методом лечения людей с психическими расстройствами, которые не поддаются традиционным методам лечения. Однако для подтверждения этих результатов и оценки долгосрочной безопасности и эффективности таких вмешательств необходимы дальнейшие исследования (Andorno, 2023; Ruiz et al., 2021).

Результаты, полученные в ходе систематического обзора литературы, подчеркивают необходимость этического решения проблем, связанных с нейротехнологиями в сфере регулирования, о чем говорится в каждой работе, включенной в данное исследование. Отмечается также необходимость шире исследовать вопросы в сфере нейротехнологий, что будет способствовать защите прав человека (Andorno, 2023; Arellano, 2024; Cid, 2022; Borbón et al., 2020; Cáceres et al., 2021; Fernández, 2023; Goering et al., 2021; Baselga-Garriga et al., 2022).

Кроме того, некоторые авторы предлагают придерживаться основных принципов деонтологической этики, включая уважение и помощь другим людям, с целью соблюдения этических норм при использовании нейротехнологий. В этой связи Организация американских государств разрабатывает ценностно ориентированную образовательную программу, которая будет способствовать распространению в социуме установок и норм для создания новых конструкций, гармонизирующих отношения между всеми участвующими сторонами.

Заключение

В заключение следует отметить, что существующая нормативная правовая база должна быть адаптирована для решения этических и социальных проблем, возникающих в связи с появлением новых нейротехнологий. Обеспечение соблюдения индивидуальных прав, неприкосновенности частной жизни и психологической автономии требует разработки соответствующей политики и нормативных актов.

Кроме того, для ответственного развития и использования нейротехнологий необходимо расширение сотрудничества между организациями, учеными и бизнесом. Это подразумевает поддержку открытости, информированного согласия и справедливости в использовании этих технологий.

Систематический обзор литературы показывает потенциальные преимущества нейротехнологий в лечении целого ряда заболеваний и проблем психологического здоровья. Тем не менее для оценки их долгосрочной эффективности и безопасности необходимо провести дополнительные исследования.

Также подчеркивается важность просвещения общественности о моральных и правовых последствиях применения нейротехнологий. В области прикладной нейробиологии это подразумевает продвижение концепций деонтологической этики, поддерживающих соблюдение и защиту прав человека.

Таким образом, с появлением новых нейротехнологий нормативная правовая база должна адаптироваться к постоянно меняющимся моральным и социальным проблемам, которые они поднимают. Чтобы гарантировать моральное и ответственное использование этих технологий, необходимы междисциплинарное сотрудничество и проактивная позиция.

Список литературы

- Alharbi, H. (2023). Identifying thematics in a brain-computer interface research. *Computational Intelligence and Neuroscience*, 4, 2793211. <https://doi.org/10.1155/2023/2793211>
- Andorno, R. (2023). *Neurotecnologías Y Derechos Humanos En América Latina Y El Caribe: Desafíos Y Propuestas De Política Pública*. University of Zurich; UNESCO. <https://doi.org/10.5167/uzh-237729>
- Arellano, W. (2024). Los Neuroderechos y su Regulación. *Inteligencia Artificial*, 27(73), 4–13. <https://doi.org/10.4114/intartif.vol27iss73pp4-13>
- Barrios, L., Minguillón, J., Perales, F., Ron-angevin, R., Solé, J., & Mañanas, M. (2017). Estado del Arte en Neurotecnologías para la asistencia y la Rehabilitación en España: Tecnologías Auxiliares, Transferencia Tecnológica y Aplicación Clínica. *Revista Iberoamericana de Automática e Informática Industrial RIAI*, 14(4) 355–361. <https://doi.org/10.1016/j.riai.2017.06.004>
- Cid, Ya. V. B. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática y Derecho*, 11.
- Baselga-Garriga, C., Rodriguez, P., & Yuste, R. (2022). Neuro Rights: A Human Rights Solution to Ethical Issues of Neurotechnologies. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Ethics of Science and Technology Assessment* (Vol. 49). Springer, Cham. https://doi.org/10.1007/978-3-030-94032-4_13
- Bastidas Cid, Y. V. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática Y Derecho. Revista Iberoamericana De Derecho Informático* (2.ª época), 11, 101–182.
- Borbón, D., & Borbón, L. (2022). NeuroDerechos Humanos y Neuroabolicionismo Penal. *Cuestiones Constitucionales*, 1(46), 29–64. (In Spain). <https://doi.org/10.22201/ijj.24484881e.2022.46.17047>
- Borbón, D., Borbón, L., & Laverde, J. (2020). Análisis crítico de los NeuroDerechos Humanos al libre albedrío y al acceso equitativo a tecnologías de mejora. *Ius Et Scientia*, 6(2), 135–161. <https://doi.org/10.12795/ietscientia.2020.i02.10>
- Bublitz J-C. (2013). My Mind is Mine!? Cognitive Liberty as a Legal Concept. In: Hildt E., & Franke A. (Eds.), *Cognitive Enhancement. An Interdisciplinary Perspective* (pp. 233–264). Dordrecht: Springer.
- Cáceres, E., Díez, J., & García, E. (2021). Neuroética y NeuroDerechos. *Revista del Posgrado en Derecho de la UNAM*, 15, 37–86. <https://doi.org/10.22201/ppd.26831783e.2021.15.179>
- Cáceres, E. & López, C. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, 1(46), 65–92. <https://doi.org/10.22201/ijj.24484881e.2022.46.17048>
- Clausen, J. E., Fetz, J., Donoghue, J., Ushiba, J., Spörhase, U., Chandler, J., Birbaumer, N., & Soekadar, S. R. (2017). Help, hope, and hype: Ethical dimensions of neuroprosthetics. Accountability, responsibility, privacy, and security are key. *Science*, 356(6345), 1338–1339. <https://doi.org/10.1126/science.aam7731>

- Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, 15. <https://doi.org/10.3389/fpsyg.2024.1330439>
- Filipova, I. A. (2022). Neurotechnologies in law and law enforcement: past, present and future. *Law Enforcement Review*, 6(2), 32–49. [https://doi.org/10.52468/2542-1514.2022.6\(2\).32-49](https://doi.org/10.52468/2542-1514.2022.6(2).32-49)
- Fernández, H. (2023). Neuroderechos, neurotecnologías y administración de riesgos en la modernidad, Análisis histórico, dialéctica Holismo. *Tzhoen*, 15(1), 99–112. <https://doi.org/10.26495/tzh.v15i1.2457>
- Fukushi, T. (2024). East Asian perspective of responsible research and innovation in neurotechnology. *IBRO Neuroscience Reports*, 16, 582–597. <https://doi.org/10.1016/j.ibneur.2024.04.009>
- Goering, S., Klein, E., Specker Sullivan, L. et al. (2021). Recommendations for Responsible Development and Application of Neurotechnologies. *Neuroethics*, 14, 365–386. <https://doi.org/10.1007/s12152-021-09468-6>
- Gómez, R. M. (2021). Inteligencia artificial y neuroderechos. Retos y perspectivas. *Cuestiones Constitucionales*, 1(46), 93–119. <https://doi.org/10.22201/ijj.24484881e.2022.46.17049>
- González, A. R. (2021). “Neuroderechos”, prueba neurocientífica y garantía de independencia judicial. *Derecho & Sociedad*, 57, 1–26. <https://doi.org/10.18800/dys.202102.007>
- Hertz, N. (2022). Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought. *Neuroethics*, 16, 5. <https://doi.org/10.1007/s12152-022-09511-0>
- Hsu, J. (2024). Privacy concerns over brain monitors. *The New Scientist*, 262(3490), 10. [https://doi.org/10.1016/s0262-4079\(24\)00850-9](https://doi.org/10.1016/s0262-4079(24)00850-9)
- Ienca, M. (2021). On Neurorights. *Frontiers in Human Neuroscience*, 15, 701258. <https://doi.org/10.3389/fnhum.2021.701258>
- Ienca, M., & Andorno, R. (2021). Hacia nuevos derechos humanos en la era de la neurociencia y la neurotecnología. *Análisis Filosófico*, 41(1), 141–185. <https://doi.org/10.36446/af.2021.386>
- López, C., & Cáceres, E. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, 46. <https://doi.org/10.22201/ijj.24484881e.2022.46.17048>
- López-Silva, P., & Madrid, R. (2022). Protecting the Mind: An Analysis of the Concept of the Mental in the Neurorights Law. *RHV*, 20, 101–117. <http://dx.doi.org/10.22370/rhv2022iss20pp101-117>
- Makin, J. G., Moses, D. A., & Chang, E. F. (2020). Machine translation of cortical activity to text with an encoder-decoder framework. *Nature Neuroscience*, 23, 575–582. <https://doi.org/10.1038/s41593-020-0608-8>
- Moreu, C. E. (2022). La Reulación de los neuroderechos. *Revista General de Legislación y Jurisprudencia*, 1, 69–98. <https://doi.org/10.30462/rglj-2022-01-04-840>
- Murillo, J. I. (2023). On the possibility of mind-reading or the external control of behavior: Contribution of Aquinas to the Neurorights discussion. *Scientia et Fides*, 11(2), 87–105. <https://doi.org/10.12775/SetF.2023.017>
- Orias, R. (2022). Los neuroderechos. Una nueva frontera para los derechos humanos. *Agenda Internacional*, XXIX(40), 211–227. <https://doi.org/10.18800/agenda.202201.009>
- Parlatino. (2023). *Ley modelo de Neuroderechos para América Latina y el Caribe*. (In Spain).
- Reguera, A. M., & Cayón, J. (2021). La Garantía de los Neuroderechos: A propósito de las iniciativas emprendidas para su reconocimiento. *Derecho y salud*, 31(1), 213–222.
- Rocha Martínez, V. E. (2022). Nuevos derechos del ser humano. *Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional*, 1(46), 251–277. <https://doi.org/10.22201/ijj.24484881e.2022.46.17055>
- Ruiz, S., Ramos, P., & et al, Caneo, C. (2021). Efectos negativos en la investigación y el quehacer médico en Chile de la Ley 20.584 y la Ley de Neuroderechos en discusión: la urgente necesidad de aprender de nuestros errores. *Revista médica de Chile*, 149(3). <https://dx.doi.org/10.4067/s0034-98872021000300439>
- Sententia, W. (2004). Neuroethical Considerations: cognitive liberty and converging technologies for improving human cognition. *Annals of the New York Academy of Sciences*, 1013(1), 221–228. <https://doi.org/10.1196/annals.1305.014>

Сведения об авторе



Ян Корнехо – магистр, генеральный директор компании Academia Cibernica, консультант по проблемам персональных данных, независимый исследователь

Адрес: Эквадор, г. Гуаякиль, ул. Ла Фае зм 32, 18

E-mail: yanornejo@yahoo.com

ORCID ID: <https://orcid.org/0000-0003-0373-1581>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/KWU-8753-2024>

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

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс

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

История статьи

Дата поступления – 9 мая 2024 г.

Дата одобрения после рецензирования – 29 мая 2024 г.

Дата принятия к опубликованию – 25 сентября 2024 г.

Дата онлайн-размещения – 30 сентября 2024 г.



Review

UDC 34:004:347.211:004.383.8.032.26

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

DOI: <https://doi.org/10.21202/jdtl.2024.36>

Neurorights, Neurotechnologies and Personal Data: Review of the Challenges of Mental Autonomy

Yan Cornejo

Independent Researcher, Guayaquil, Ecuador

Keywords

digital technologies,
ethics,
human rights,
law,
legislation,
mental autonomy,
neurorights,
neurotechnologies,
personal data,
privacy

Abstract

Objective: to present the results of a systematic review of research on the impact of neurotechnology on legal concepts and regulatory frameworks, addressing ethical and social issues related to the protection of individual rights, privacy and mental autonomy.

Methods: The systematic literature review was based on the methodology proposed by a renowned British scholar, a professor emerita of computer science at Keele University Barbara Kitchenham, chosen for its flexibility and effectiveness in obtaining results for publication. Thorough searches were carried out with the search terms “neurotechnology”, “personal data”, “mental privacy”, “neuro-rights”, “neurotechnological interventions”, and “neurotechnological discrimination” on both English and Spanish sites, using search engines like Google Scholar and Redib as well as databases including Scielo, Dialnet, Redalyc, Lilacs, Scopus, Medline, and Pubmed. The focus of this research is bibliometric data and its design is non-experimental with a cross-sectional and descriptive, using content analysis based on PRISMA model.

Results: the study emphasizes the need to establish clear ethical principles to protect individual rights and promote responsible use of neurotechnologies; a number of problems of mental autonomy were identified, such as improper handling of information, lack of legal security guarantees, violation of rights and freedoms in the medical sphere. The author shows the need to adapt the existing regulatory legal framework to address the ethical and social problems arising from the new neurotechnologies. It is noted that a broad study of neurotechnology issues will contribute to the protection of human rights.

© Cornejo Ya., 2024

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: an expanded understanding of the five neurorights within the Universal Declaration of Human Rights is proposed; neurorights are viewed as a new category of rights aimed at protecting mental integrity against the misuse of neurotechnologies. The author justifies the adoption of such technocratic principles as personal identity, free will, mental privacy, equal access and protection against bias.

Practical significance: the obtained results are relevant for understanding modern legal concepts related to neurorights and for adapting the existing normative legal acts to solve ethical and social problems arising from the emergence of new technologies, protection of human neurorights and liability for their violation. The study of these issues is key for provision of further responsible development and use of neurotechnologies.

For citation

Cornejo, Ya. (2024). Neurorights and Personal Data: Challenges and Mental Autonomy. *Journal of Digital Technologies and Law*, 2(3), 711–728. <https://doi.org/10.21202/jdtl.2024.36>

References

- Alharbi, H. (2023). Identifying thematic in a brain-computer interface research. *Computational Intelligence and Neuroscience*, 4, 2793211. <https://doi.org/10.1155/2023/2793211>
- Andorno, R. (2023). *Neurotecnologías Y Derechos Humanos En América Latina Y El Caribe: Desafíos Y Propuestas De Política Pública*. University of Zurich; UNESCO. (In Spain). <https://doi.org/10.5167/uzh-237729>
- Arellano, W. (2024). Los Neuroderechos y su Regulación. *Inteligencia Artificial*, 27(73), 4–13. (In Spain). <https://doi.org/10.4114/intartif.vol27iss73pp4-13>
- Barrios, L., Minguillón, J., Perales, F., Ron-angevin, R., Solé, J., & Mañanas, M. (2017). Estado del Arte en Neurotecnologías para la asistencia y la Rehabilitación en España: Tecnologías Auxiliares, Transferencia Tecnológica y Aplicación Clínica. *Revista Iberoamericana de Automática e Informática Industrial RIAI*, 14(4) 355–361. (In Spain). <https://doi.org/10.1016/j.riai.2017.06.004>
- Cid, Ya. V. B. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática y Derecho*, 11. (In Spain).
- Baselga-Garriga, C., Rodríguez, P., & Yuste, R. (2022). Neuro Rights: A Human Rights Solution to Ethical Issues of Neurotechnologies. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Ethics of Science and Technology Assessment* (Vol. 49). Springer, Cham. https://doi.org/10.1007/978-3-030-94032-4_13
- Bastidas Cid, Y. V. (2022). Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea. *Informática Y Derecho. Revista Iberoamericana De Derecho Informático* (2.ª época), 11, 101–182.
- Borbón, D., & Borbón, L. (2022). NeuroDerechos Humanos y Neuroaboliciónismo Penal. *Cuestiones Constitucionales*, 1(46), 29–64. (In Spain). <https://doi.org/10.22201/ij.24484881e.2022.46.17047>
- Borbón, D., Borbón, L., & Laverde, J. (2020). Análisis crítico de los NeuroDerechos Humanos al libre albedrío y al acceso equitativo a tecnologías de mejora. *Ius Et Scientia*, 6(2), 135–161. (In Spain). <https://doi.org/10.12795/ietscientia.2020.i02.10>
- Bublitz J-C. (2013). My Mind is Mine!? Cognitive Liberty as a Legal Concept. In: Hildt E., & Franke A. (Eds.), *Cognitive Enhancement. An Interdisciplinary Perspective* (pp. 233–264). Dordrecht: Springer.
- Cáceres, E., Díez, J., & García, E. (2021). Neuroética y NeuroDerechos. *Revista del Posgrado en Derecho de la UNAM*, 1, 37–86. (In Spain). <https://doi.org/10.22201/ppd.26831783e.2021.15.179>
- Cáceres, E. & López, C. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, 1(46), 65–92. (In Spain). <https://doi.org/10.22201/ij.24484881e.2022.46.17048>

- Clausen, J. E., Fetz, J., Donoghue, J., Ushiba, J., Spörhase, U., Chandler, J., Birbaumer, N., & Soekadar, S. R. (2017). Help, hope, and hype: Ethical dimensions of neuroprosthetics. Accountability, responsibility, privacy, and security are key. *Science*, 356(6345), 1338–1339. <https://doi.org/10.1126/science.aam7731>
- Cornejo-Plaza, M. I., Cippitani, R., & Pasquino, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, 15. <https://doi.org/10.3389/fpsyg.2024.1330439>
- Filipova, I. A. (2022). Neurotechnologies in law and law enforcement: past, present and future. *Law Enforcement Review*, 6(2), 32–49. [https://doi.org/10.52468/2542-1514.2022.6\(2\).32-49](https://doi.org/10.52468/2542-1514.2022.6(2).32-49)
- Fernández, H. (2023). Neuroderechos, neurotecnologías y administración de riesgos en la modernidad, Análisis histórico, dialéctica Holismo. *Tzhoen*, 15(1), 99–112. (In Spain). <https://doi.org/10.26495/tzh.v15i1.2457>
- Fukushi, T. (2024). East Asian perspective of responsible research and innovation in neurotechnology. *IBRO Neuroscience Reports*, 16, 582–597. <https://doi.org/10.1016/j.ibneur.2024.04.009>
- Goering, S., Klein, E., Specker Sullivan, L. et al. (2021). Recommendations for Responsible Development and Application of Neurotechnologies. *Neuroethics*, 14, 365–386. <https://doi.org/10.1007/s12152-021-09468-6>
- Gómez, R. M. (2021). Inteligencia artificial y neuroderechos. Retos y perspectivas. *Cuestiones Constitucionales*, 1(46), 93–119. (In Spain). <https://doi.org/10.22201/ijj.24484881e.2022.46.17049>
- González, A. R. (2021). “Neuroderechos”, prueba neurocientífica y garantía de independencia judicial. *Derecho & Sociedad*, 57, 1–26. (In Spain). <https://doi.org/10.18800/dys.202102.007>
- Hertz, N. (2022). Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought. *Neuroethics*, 16, 5. <https://doi.org/10.1007/s12152-022-09511-0>
- Hsu, J. (2024). Privacy concerns over brain monitors. *The New Scientist*, 262(3490), 10. [https://doi.org/10.1016/s0262-4079\(24\)00850-9](https://doi.org/10.1016/s0262-4079(24)00850-9)
- Ienca, M. (2021). On Neurorights. *Frontiers in Human Neuroscience*, 15, 701258. <https://doi.org/10.3389/fnhum.2021.701258>
- Ienca, M., & Andorno, R. (2021). Hacia nuevos derechos humanos en la era de la neurociencia y la neurotecnología. *Análisis Filosófico*, 41(1), 141–185. (In Spain). <https://doi.org/10.36446/af.2021.386>
- López, C., & Cáceres, E. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Cuestiones Constitucionales*, 46. (In Spain). <https://doi.org/10.22201/ijj.24484881e.2022.46.17048>
- López-Silva, P., & Madrid, R. (2022). Protecting the Mind: An Analysis of the Concept of the Mental in the Neurorights Law. *Revista De Humanidades De Valparaíso*, 20, 101–117. <http://dx.doi.org/10.22370/rhv2022iss20pp101-117>
- Makin, J. G., Moses, D. A., & Chang, E. F. (2020). Machine translation of cortical activity to text with an encoder-decoder framework. *Nature Neuroscience*, 23, 575–582. <https://doi.org/10.1038/s41593-020-0608-8>
- Moreu, C. E. (2022). La Reulación de los neuroderechos. *Revista General de Legislación y Jurisprudencia*, 1, 69–98. (In Spain). <https://doi.org/10.30462/rglj-2022-01-04-840>
- Murillo, J. I. (2023). On the possibility of mind-reading or the external control of behavior: Contribution of Aquinas to the Neurorights discussion. *Scientia et Fides*, 11(2), 87–105. <https://doi.org/10.12775/SetF.2023.017>
- Orias, R. (2022). Los neuroderechos. Una nueva frontera para los derechos humanos. *Agenda Internacional*, XXIX(40), 211–227. (In Spain). <https://doi.org/10.18800/agenda.202201.009>
- Parlatino. (2023). *Ley modelo de Neuroderechos para América Latina y el Caribe*. (In Spain).
- Reguera, A. M., & Cayón, J. (2021). La Garantía de los Neuroderechos: A propósito de las iniciativas emprendidas para su reconocimiento. *Derecho y salud*, 31(1), 213–222. (In Spain).
- Rocha Martínez, V. E. (2022). Nuevos derechos del ser humano. *Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional*, 1(46), 251–277. <https://doi.org/10.22201/ijj.24484881e.2022.46.17055>
- Ruiz, S., Ramos, P., & et al, Caneo, C. (2021). Efectos negativos en la investigación y el quehacer médico en Chile de la Ley 20.584 y la Ley de Neuroderechos en discusión: la urgente necesidad de aprender de nuestros errores. *Revista médica de Chile*, 149(3). (In Spain). <http://dx.doi.org/10.4067/s0034-98872021000300439>
- Sententia, W. (2004). Neuroethical Considerations: cognitive liberty and converging technologies for improving human cognition. *Annals of the New York Academy of Sciences*, 1013(1), 221–228. <https://doi.org/10.1196/annals.1305.014>

Author information



Yan Cornejo – Magister, CEO of Academia Cibers, Private Consultant Data Privacy, Independent Researcher

Address: La Fae mz 32 villa 18, Guayaquil, Ecuador

E-mail: yancornejo@yahoo.com

ORCID ID: <https://orcid.org/0000-0003-0373-1581>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/KWU-8753-2024>

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

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – May 9, 2024

Date of approval – May 29, 2024

Date of acceptance – September 25, 2024

Date of online placement – September 30, 2024

