ISSN 2949-2483

Volume 2 Number 4

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2024

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Том 2, № 4
2024
DOI: 10.21202/2949-2483.2024.4

ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

eISSN 2949-2483

Издается с 2023 года, периодичность – 4 выпуска в год. DOI: 10.21202/2949-2483

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. Тимирясова (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 – доктор 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. Тимирясова (Казань, Российская Федерация)

Редакция

Заведующий редакцией – Дарчинова Гульназ Язкаровна
Выпускающий редактор – Аймурзаева Оксана Анатольевна
Ответственный секретарь – Валиуллина Светлана Зиряковна
Редактор – Тарасова Гульнара Абдулахатовна
Технический редактор – Каримова Светлана Альфредовна
Художник-дизайнер – Загретдинова Гульнара Ильгизаровна
Переводчик – Беляева Елена Николаевна, кандидат педагогических наук, член Гильдии переводчиков Республики Татарстан
Специалист по продвижению журнала в сети Интернет – Гуляева Полина Сергеевна

Адрес: 420111, Российская Федерация, г. Казань, ул. Московская, 42
Телефон: +7 (843) 231-92-90
Факс: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Сайт: https://www.lawjournal.digital
Телеграм: https://t.me/JournalDTL
ВКонтакте: https://vk.com/JournalDTL
Яндекс.Дзен: https://dzen.ru/JournalDTL
Одноклассники: https://ok.ru/JournalDTL

Учредитель и издатель

Казанский инновационный университет имени В. Г. Тимирясова. 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. Тимирясова, 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!
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.

16+
Возрастная классификация: Информационная продукция для детей, достигших возраста шестнадцати лет.

Дата подписания к публикации – 13 декабря 2024 г. Дата онлайн-размещения на сайте https://www.lawjournal.digital – 20 декабря 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)

Русскевич 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. Тимирясова (Казань, Российская Федерация)

Харитонова 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)

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

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

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

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

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

Дэнни Тэйм Даниэль Мендес – доктор наук, научный сотрудник Азиатско-Тихоокеанского центра экологического права Национального университета Сингапура (Сингапур, Республика Сингапур)

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

Иоаннис Революдис – 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 (Булаксумур, 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 (Тайпей, 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)

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 2, № 4
2024
DOI: 10.21202/2949-2483.2024.4
ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
eISSN 2949-2483

Содержание

Бегишев И. Р., Жарова А. К., Залоило М. В., Филипова И. А., Шутова А. А.
Технологические трансформации: рост возможностей и правовой ответ на возникающие риски 735

Филипова И. А.
Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права 741

Абделькарим Я. А.
Правовые аспекты концепции киберинтересов государств через призму теории законных интересов 782

Мупарадзи Т., Муконза Р. М.
Перспективы применения цифровых технологий в системе отправления правосудия в Зимбабве 802

Икубанни О. О., Ойебанджи А. О., Ойебаде А. А.
Юридические аспекты наделения искусственного интеллекта субъектностью: перспективы использования роботов в юридической практике в Нигерии 835

Чонг Б. Ч.
Возникновение аватаров на основе искусственного интеллекта: юридическая субъектность, права и обязанности в развивающейся метавселенной 857

Хатсон Дж.
Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом 886

Аувал А. М., Лазарус С.
Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности 915

Бахтеев Д. В., Сосновикова А. М., Казенас Е. В.
Преодоление нелегальной трансграничной передачи персональных данных 943

Рахман М. М., Дас Т. К.
Противодействие кибератакам: пробелы международного права и перспективы их преодоления 973

Беликова К. М., Диас Мартинс Р., Казанба Е. Т.
Международное сотрудничество в преодолении цифрового неравенства: правовые основы, барьеры и параметры развития 1003

Колаволе А.
Правовые аспекты защиты персональных данных и проблемы конкуренции на цифровых рынках 1031

От редакции
УДК 34:004
EDN: https://elibrary.ru/acmfll
DOI: https://doi.org/10.21202/jdtl.2024.37

Технологические трансформации: рост возможностей и правовой ответ на возникающие риски

Ильдар Рустамович Бегишев
Казанский инновационный университет имени В. Г. Тимирясова, 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. Тимирясова, Казань, Россия

Развитие цифровых технологий и их все более активное внедрение в различные сферы жизнедеятельности открывают новые перспективы для человечества, качественно преобразуя возможности и даже ежедневный образ жизни людей. Автоматизация рабочих процессов и рутинных процедур с помощью таких технологий, как искусственный интеллект, машинное обучение и интернет вещей, повышает их оперативность и эффективность, позволяет снизить затраты и издержки, стимулирует развитие новых видов услуг и продуктов. Растет и значение предиктивной функции аналитических инструментов, опирающихся на алгоритмы обработки данных.

Технологический императив будет определять будущее человечества на многие годы вперед. При этом нельзя не отметить порождаемые им потенциальные риски, которые требуют научного осмысления и формирования правовых решений для их преодоления или минимизации.

Одним из таких рисков, реализующимся уже сейчас, является углубление технологического разрыва. Пользование цифровыми преимуществами доступно не всем группам населения и регионам мира, а цифровое и в целом технологическое

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.

неравенство имеет влияние на более масштабные социально-экономические процессы и глобальную динамику развития, ставя проблемы обеспечения технологического суверенитета стран как существенной составляющей государственного суверенитета, экономического роста, инновационной активности и социальной стабильности.

На страницах очередного выпуска читатель сможет ознакомиться с работами исследователей из 13 государств (Бангладеш, Бразилии, Великобритании, Гонконга, Египта, Зимбабве, Индии, Нигерии, России, Сингапура, США, Узбекистана, ЮАР), посвященными проблемам преодоления цифрового неравенства, обеспечения киберинтересов государств, противодействия киберпреступности, категорирования в правовом пространстве искусственного интеллекта, в том числе в контексте авторского права, автоматизации юридической деятельности и развития метавселенных.

В первой статье номера – «Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права» (**Ирина Филипова (Россия – Узбекистан)**) – наряду с позитивными изменениями общества и права в условиях прогресса цифровых технологий и биотехнологий, обеспечивающих переход общества к следующему технологическому укладу, подчеркиваются индивидуальные, коллективные и экзистенциальные риски возникновения новых физических, цифровых и киберфизических сущностей, обладающих когнитивными способностями, сопоставимыми, а по ряду параметров даже превышающими человеческие, позволяющими осуществлять интеллектуально направленное воздействие на технологически интегрированное Общество 5.0, формирование которого неизбежно. Интересными для читателя будут сформулированные в статье правовые траектории функционирования интеллектуальных роботов, виртуальных личностей, предложения о новациях правового статуса технологически и генетически усовершенствованных индивидов.

Продолжением затронутой проблематики правосубъектности и создания адекватного правового режима искусственного интеллекта станет статья «Возникновение аватаров на основе искусственного интеллекта: юридическая субъектность, права и обязанности в развивающейся метавселенной» (**Бен Честер Чонг (Сингапур)**). В статье представлен новый взгляд на проблему правосубъектности аватаров искусственного интеллекта, а также решение вопроса об ответственности за их действия исходя из их разграничения на автономные и творческие сущности. Представленные в работе сценарии будущего метавселенной демонстрируют важность нахождения баланса между инновациями и благополучием человеческой цивилизации.

Развитие технологий генеративного искусственного интеллекта, которое мы наблюдаем в музыке, литературе, изобразительном и других видах искусства, расширяет горизонты творчества, но одновременно актуализирует вопросы авторства созданных таким образом произведений, перспективы решения которых определены в статье «Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом» (**Джеймс Хатсон (США)**). Предлагаемый в качестве основы комбинированный адаптивный подход предполагает создание гибких норм в области интеллектуальной собственности и пересмотр понятия авторства в аспекте устойчивого сотворчества с искусственным интеллектом, где последний признается творческим инструментом, расширяющим возможности

человека, вклад которого выступает основополагающим фактором оригинальности произведения.

К циклу исследований правового режима искусственного интеллекта примыкают две другие статьи настоящего номера. Первая из них посвящена решению вопроса о правосубъектности искусственного интеллекта и допустимости применения этих технологий в юридической деятельности по законодательству Нигерии (**Олувасейе О. Икубанни (Нигерия)**, **Адереми О. Ойебанджи (Нигерия)**, **Аладе А. Ойебаде (Нигерия)**). Сформулированные предложения по совершенствованию правовой базы юридической практики в Нигерии направлены на обеспечение его соответствия уровню развития цифровых технологий в стране и в мире. Во второй статье с опорой на сравнительно-правовое исследование процесса цифровизации судопроизводства в Великобритании, Южно-Африканской Республике и Руанде представлена перспективная модель эффективного перехода к цифровым технологиям в отправлении правосудия в Зимбабве (**Таурай Мупарадзи (Зимбабве – ЮАР)**, **Рикки Муньярадзи Муконза (ЮАР)**).

Сразу несколько вошедших в номер статей объединены общей тематикой правового обеспечения кибербезопасности. В одной из них определяется применимость теории законных интересов для совершенствования правовых механизмов защиты национальных интересов в киберпространстве (**Яссин Абдалла Абделькарим (Египет – Великобритания)**). Категорированию кибератак в правовой плоскости и определению юридических мер противодействия им посвящено специальное исследование в области международного права (**Мохаммад Минхазур Рахман (Бангладеш)**, **Тапос Кумар Дас (Бангладеш – Гонконг)**), где применение профилактических киберконтрмер со стороны государств обуславливается соблюдением принципов законности, должной осмотрительности, соразмерности, а обеспечение кибербезопасности увязывается с соблюдением права на неприкосновенность частной жизни и свободы слова. Особого внимания заслуживает междисциплинарное социолого-криминологическое исследование проблем виктимизации в результате киберпреступности (**Амину Мухаммад Аувал (Нигерия)**, **Сулеман Лазарус (Великобритания)**), где на основе трехчастной концепции киберпреступности (Tripartite Cybercrime Framework) анализируются результаты проведенных анкетирований и опросов, подтверждающие разрыв между глобальным Севером и глобальным Югом и позволяющие сформировать концептуальные гендерные, инклюзивные и контекстуальные подходы к разработке национальной правовой политики противодействия киберпреступности в Нигерии.

Еще один блок исследований посвящен проблематике защиты персональных данных, приобретающей особую актуальность в связи с развитием цифровых технологий. Междисциплинарное исследование представлено в статье «Преодоление нелегальной трансграничной передачи персональных данных» (**Дмитрий Бахтеев (Россия)**, **Анна Сосновикова (Россия)**, **Евгений Казенас (Россия)**). Трансграничная передача персональных данных получила освещение как в историко-правовой ретроспективе (показан генезис феномена персональных данных со времен Великой французской революции и его последующая эволюция в XIX–XX вв.), так и с позиций сравнительно-правового метода (проанализирован российский и международный опыт правового регулирования). Дополняемое изучением технико-технологических аспектов передачи данных исследование позволило сформировать

модель выявления факта трансграничной передачи данных и принятия управленческого решения, опосредуемую оптимизацией административного и уголовного законодательства и представленную внедрением специализированных технических средств детекции несанкционированных трансграничных потоков персональных данных. Другая статья посвящена правовым аспектам защиты персональных данных в условиях цифровизации рынков и роста цифровой конкуренции (**Афувапе Колаволе (Индия)**). Персональные данные обозначены в ней как неотъемлемый компонент общего конкурентного ландшафта на рынке, а на основе анализа правового регулирования цифровых рынков, цифровых услуг и управления данными в Европейском союзе предлагаются подходы к обеспечению конфиденциальности данных в цифровой конкурентной среде.

Усилению негативного эффекта выявленных проблем в сфере цифровизации способствует сохраняющееся и стремительно углубляющееся по мере совершенствования технологических решений цифровое неравенство, выступающее барьером для социально-экономического и культурного развития отдельных стран, регионов и населяющих их людей. Проблема усугубляется в странах глобального Юга, но актуальна и для России. В связи с этим читательский интерес, несомненно, вызовет статья, посвященная определению правовых основ, существующих барьеров и параметров международного сотрудничества в преодолении цифрового неравенства в условиях перехода от экономики знаний к экономике данных (**Ксения Беликова (Россия)**, **Рафаэл Диас (Бразилия)**, **Евгений Казанба (Россия)**).

За два года, прошедших с момента учреждения, журналу в непростых внешнеполитических условиях удалось наладить международное сотрудничество, работу со своими зарубежными амбассадорами, результатом чего стала публикация результатов правовых исследований цифровых трансформаций авторов из самых разных государств. В этом и состоит миссия Journal of Digital Technologies and Law, заключающаяся в приумножении сложившихся знаний о цифровых новациях в праве путем притяжения ученых и практиков из России и других стран, заинтересованных в обсуждении наиболее актуальных вопросов цифровой повестки, распространении научных достижений и опыта, не только восполняющих пробелы в понимании и интерпретации процессов технологической трансформации права, вопросов правового измерения цифровизации, но и образующих своеобразные точки роста новых знаний и представлений о праве и цифровых технологиях.

Journal of Digital Technologies and Law способствует укреплению научного сотрудничества. В восьми выпусках издания за 2023–2024 годы были опубликованы результаты исследований 58 авторов из 38 стран (Австралии, Бангладеш, Беларуси, Болгарии, Бразилии, Великобритании, Венгрии, Гонконга, Греции, Дании, Египта, Зимбабве, Индии, Ирана, Испании, Италии, Кабо-Верде, Казахстана, Кипра, Китая, Макао, Малайзии, Мали, Марокко, Нигерии, Нидерландов, Португалии, России, Сингапура, США, Танзании, Уганды, Узбекистана, Филиппин, Франции, Чехии, Эквадора, ЮАР).

Высокий интерес к журналу Journal of Digital Technologies and Law и его публикациям свидетельствует о востребованности научных исследований и новых достижений в этой области среди представителей глобального научного сообщества (рис. 1).



Рис. 1. География посетителей сайта журнала Journal of Digital Technologies and Law (162 страны по состоянию на 20 декабря 2024 г.)

Мы надеемся, что текущий выпуск журнала привлечет внимание широкого круга читателей, а опубликованные статьи вдохновят потенциальных авторов представить свои перспективные научные достижения и разработки в области цифровых технологий и права на страницах нашего научного периодического издания (рис. 2).

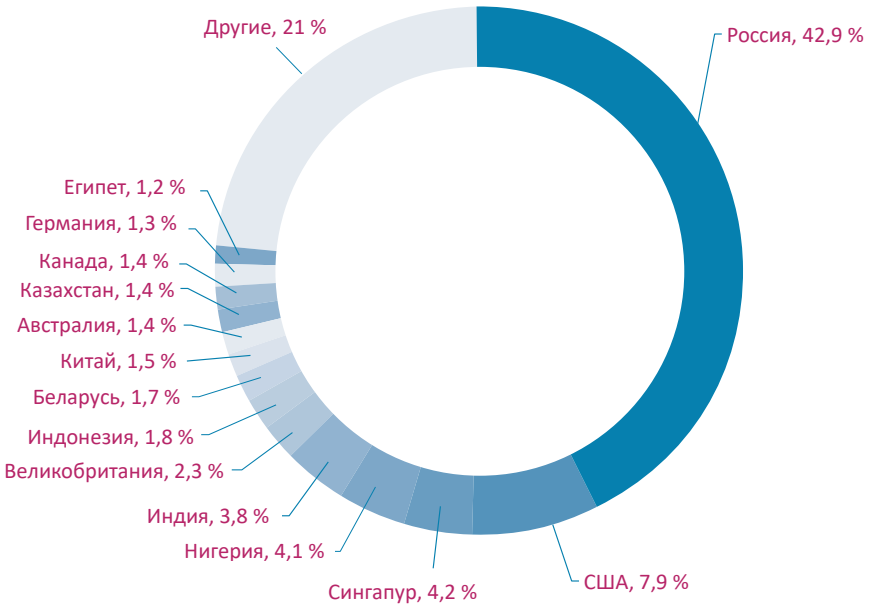


Рис. 2. Статистика посещаемости сайта журнала Journal of Digital Technologies and Law (по состоянию на 20 декабря 2024 г.)

Надеемся, что в наступающем году международный научный диалог в рамках журнала будет продолжен, а к многонациональному коллективу его авторов – ученых и практикующих юристов, а также специалистов смежных отраслей знания – примкнут новые исследователи проблем взаимодействия цифровизации и права.

Выражаем признательность авторам, чьи статьи послужили отправной точкой научных дискуссий и концептуальным фундаментом управленческих решений, читателям, чей неиссякаемый интерес к журналу побуждает нас двигаться дальше, амбассадорам, чья активность расширяет рамки сотрудничества с исследователями из разных точек земного шара, рецензентам и членам редакционной коллегии, чья работа позволяет поддерживать высокий стандарт научных публикаций!

Научная статья
УДК 34:004:342.721:612.6
EDN: https://elibrary.ru/atqzba
DOI: https://doi.org/10.21202/jdtl.2024.38

Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права

Ирина Анатольевна Филипова

Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского, Нижний Новгород, Россия;
Самаркандский государственный университет имени Шарофа Рашидова, Самарканд, Узбекистан

Ключевые слова

биотехнологии,
генная инженерия,
искусственный интеллект,
киборг,
нейротехнологии,
право,
риск,
робот,
цифровые технологии,
человек

Аннотация

Цель: выявить теоретико-правовые проблемы, связанные с неуклонно расширяющимся распространением на практике продуктов развития цифровых и биотехнологий, оценить сопутствующие этому процессу риски, способные изменить положение человека в обществе будущего, а также выработать и аргументировать предложения по минимизации рисков и устранению выявленных проблем с помощью правового регулирования.

Методы: в основе исследования лежат методы обобщения научно-технической информации и теоретического анализа, применявшиеся в процессе изучения исходных материалов, аксиологический и системный подходы, формально-юридический метод и, кроме того, методы правового прогнозирования, в первую очередь экстраполяции, позволившие осветить перспективы реформирования права вследствие технологической экспансии.

Результаты: включают описание динамики развития цифровых и биотехнологий; характеристику меняющегося социального ландшафта с возникновением новых типов сущностей, способных повлиять на фактический статус человека; классификацию рисков, угрожающих людям из-за совершенствования цифровых и биотехнологий; перечень задач, решение которых на основе права поможет устранить, отодвинуть или, по крайней мере, значительно снизить остроту проблем, увеличивая лимит времени, отведенный человечеству на осмысление ряда концептуальных моментов. Представлены доводы, обосновывающие необходимость разработки специального правового регулирования в отношении новых типов сущностей, появление которых становится неизбежным результатом развития упоминаемых технологий.

© Филипова И. 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: состоит, во-первых, в комплексном изучении развития взаимосвязанных групп цифровых и биотехнологий с учетом их усиливающейся конвергенции, во-вторых, в формулировании юридических вопросов, которые требуют урегулирования из-за потенциального появления новых типов сущностей, располагающих когнитивными функциями и способных оказывать интеллектуально направленное воздействие на окружающую среду и субъектов права.

Практическая значимость: присутствует в ответах, данных на сформулированные юридические вопросы, они содержат предложения и рекомендации по необходимой корректировке правового регулирования и акцентируют внимание правоведов на проблемах, вытекающих из темпов и векторов развития наукоемких технологий.

Для цитирования

Филипова, И. А. (2024). Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права. *Journal of Digital Technologies and Law*, *2*(4), 741–781. https://doi.org/10.21202/jdtl.2024.38

Содержание

Введение
1. Развитие и применение на практике цифровых технологий и биотехнологий
   1.1. Развитие цифровых технологий и биотехнологий
      1.1.1. Прогресс цифровых технологий
      1.1.2. Продвижение биотехнологий
   1.2. Результаты применения цифровых технологий и биотехнологий на практике
      1.2.1. Интеллектуальные роботы
      1.2.2. Киборги
      1.2.3. Генетически усовершенствованные индивиды
      1.2.4. Химеры
2. Влияние результатов применения цифровых технологий и биотехнологий на общество и право
   2.1. Потенциальное появление новых участников общественных отношений
      2.1.1. Интеллектуальные роботы
      2.1.2. Киборги
      2.1.3. Генетически усовершенствованные индивиды
      2.1.4. Химеры
   2.2. Сопутствующие риски применения цифровых технологий и биотехнологий
      2.2.1. Индивидуальные риски
      2.2.2. Коллективные риски
      2.2.3. Экзистенциальные риски
   2.3. Юридические вопросы, связанные с появлением новых типов сущностей

2.3.1. Правовой режим (потенциально – правовой статус) интеллектуальных роботов
2.3.2. Правовой статус киборгов
2.3.3. Правовой статус генетически усовершенствованных индивидов
2.3.4. Правовой режим (потенциально – правовой статус) химер
Заключение
Список литературы

Введение

Развитие искусственного интеллекта сегодня обсуждается юристами, в том числе с точки зрения возможности признания за искусственными интеллектуальными системами статуса субъекта права. Системы искусственного интеллекта – достаточно новое явление в сравнении с человечеством, ведь появление на планете человека разумного (Homo sapiens) произошло примерно 200 тысяч лет назад. Растущее внимание к теме возможной правосубъектности искусственного интеллекта объясняется высокой скоростью развития технологий искусственного интеллекта и быстро расширяющимся распространением результатов этого развития на практике.

Как известно, человек может демонстрировать когнитивные способности или функции, т. е. высшие функции человеческого мозга, связывающие людей с окружающим миром, позволяющие получать представление о нем и с ним взаимодействовать. К этим функциям можно отнести мышление, речь, обучаемость, ориентирование в пространстве, воображение, память. Через когнитивные способности проявляется интеллект человека, но их показывают и системы искусственного интеллекта. Наличие таких способностей провоцирует дискуссию о признании правосубъектности за системами искусственного интеллекта, особенно если они достигнут уровня интеллекта человека.

Помимо совершенствования технологий искусственного интеллекта и иных цифровых технологий, к примеру компонентов робототехники, в научных лабораториях ведутся исследования, направленные на развитие биотехнологий, что в совокупности с достижениями цифровых технологий делает возможным соединение людей с системами искусственного интеллекта или целенаправленное преобразование генетических характеристик организма человека.

Прогрессирующее развитие цифровых и биотехнологий потенциально повлечет возникновение новых типов сущностей, обладающих когнитивными способностями, причем не уступающими или даже превышающими уровень таковых у современного человека, что не может не вызвать проблем, включая проблемы юридического свойства.

1. Развитие и применение на практике цифровых технологий и биотехнологий

1.1. Развитие цифровых технологий и биотехнологий

В условиях информационного общества ключевым фактором социально-экономического развития стал переход к применению так называемых высоких технологий, требующих использования научного знания при создании и производстве технически

сложных продуктов. Высокотехнологичные отрасли экономики, использующие подобные технологии, имеют наибольший потенциал для экономического роста, что привлекает государственные и частные инвестиции в эту сферу. Глобальная гонка технологий, ставкой в которой является мировое технологическое доминирование, подталкивает государства к созданию программ, нацеленных на ускоренную разработку технологий, а бизнес – к оперативному внедрению новых технологических продуктов.

К высоким технологиям можно отнести ряд цифровых технологий, основанных на использовании цифровой информации и обработке данных с помощью компьютеров. Применительно к этим технологиям нередко употребляется словосочетание «сквозные технологии», подчеркивающее свойство цифровых технологий взаимодополнять одна другую, увеличивая полезные характеристики создаваемых в итоге продуктов. Среди основных цифровых технологий можно назвать технологии искусственного интеллекта, беспроводной связи, виртуальной и дополненной реальности, интернет вещей и т. д. Робототехнику также упоминают в списке цифровых технологий, так как конструирование роботов сегодня основано на «цифре», за счет цифровой компоненты «материальная часть» робототехники быстро совершенствуется.

Помимо собственно цифровых технологий, к высоким технологиям могут быть отнесены и биотехнологии, развивающиеся на стыке биологии и техники и свидетельствующие о биоцифровой конвергенции. Некоторые биотехнологии иногда именуют природоподобными, потому что они позволяют воспроизводить системы и процессы живой природы в виде технических систем и технологических процессов. Биотехнологии, о которых пойдет речь ниже, по идее, тоже можно назвать цифровыми, так как их развитие – следствие прогресса технологий искусственного интеллекта, в результате чего появились вычислительные мощности, позволяющие использовать множество наборов данных при одновременном сокращении потребности в ручных лабораторных исследованиях.

Если ранее, в первые два десятилетия XXI в., некоторые исследователи упоминали о НБИК-конвергенции – объединении и синергетическом усилении достижений нано-, био-, информационных и когнитивных технологий (Roco & Bainbridge, 2003), то к настоящему моменту можно констатировать, что цифровые и биотехнологии во многом поглотили остальные, а теперь сопровождают и обеспечивают переход общества к следующему технологическому укладу.

1.1.1. Прогресс цифровых технологий

Уровень развития цифровых технологий ощутимо повышается с каждым годом, это хорошо заметно на примере технологий искусственного интеллекта как первой по степени значимости подгруппы цифровых технологий, оказывающей огромное влияние на все остальные. В настоящее время активно совершенствуется искусственный интеллект генеративного типа, относящиеся к нему системы искусственного интеллекта могут на основе генеративных моделей создавать тексты, изображения, аудио- и видеоролики, иные медиаданные. Скорость развития искусственного интеллекта данного типа можно проследить по продукту одного из мировых лидеров в этой сфере – компании OpenAI, речь идет о ChatGPT. Только в 2017 г. была изобретена новая архитектура нейросетей – Transformer, – позволившая соединять возможности существовавших ранее архитектур, к примеру сверточных и рекуррентных

нейросетей. В 2018 г. появилась первая модель ChatGPT, представлявшая собой обученную на большом объеме текстов нейросеть, уже через год, в 2019 г., появилась следующая модель ChatGPT-2, представлявшая собой десятикратно увеличенную предыдущую нейросеть с соответствующим повышением возможностей, в 2020 г. стало известно о создании ChatGPT-3, показывающего новый по качеству уровень обработки текстов, а в 2022 г. – о ChatGPT-3.5, умеющем «рисовать» через взаимодействие с другой нейросетью DALL-E. В 2023 г. появился ChatGPT-4, демонстрирующий продвинутую «работу» с текстами, аудиофайлами и изображениями, в мае 2024 г. – ChatGPT-4o, способный, помимо прочего, отвечать голосом, похожим на человеческий, и имитировать эмоции, в сентябре 2024 г. – OpenAI o1, проявляющий способность «рассуждать», как человек, а объявленное появление в 2025 г. ChatGPT-5[1] увязывается с возможностью подключаться к искусственным интеллектуальным агентам и персонализацией задач.

Сегодня изготовление гиперреалистичных дипфейков (изображений, видео- и аудиофайлов, созданных искусственным интеллектом, но неотличимых от реально снятых или записанных людьми) уже не требует больших затрат времени и иных ресурсов, что спровоцировало обсуждение в законодательных органах целого ряда государств законопроектов, предусматривающих маркировку такого контента во избежание введения людей в заблуждение. Это всего лишь один пример, показывающий темпы развития технологий искусственного интеллекта. Вектор развития данных технологий направлен на создание сильного искусственного интеллекта. Интеллектуальная система – носитель сильного искусственного интеллекта будет иметь мыслительные способности, сопоставимые с человеком, в том числе обладать искусственным «сознанием». Одним из ключевых условий обретения сознания системами искусственного интеллекта является возможность осуществлять мультимодальное поведение, интегрируя информацию из различных сенсорных модальностей (текст, изображение, видео, звук и т. д.) и осуществляя «привязку» этой информации к окружающей действительности с построением полноценных связных «образов», как это присуще человеку. По оценкам разработчиков, например основателя SingularityNET Б. Герцеля, компьютер ожидаемо достигнет вычислительной мощности человеческого мозга не позднее 2030 г., а еще примерно через 10–15 лет один компьютер можно будет сопоставить с вычислительной мощностью всего человечества. Дж. Хинтон, известный исследователь в IT-сфере и лауреат Нобелевской премии, считает, что до появления сильного искусственного интеллекта осталось от пяти до двадцати лет[2].

Вторая подгруппа, об уровне развития которой следует рассказать, – это робототехнические технологии. Робототехника как совокупность технологий включает цифровые и «материальные» компоненты, которые вместе обеспечивают разработку автоматизированных технических систем и «материализуют» результат, опираясь на такие области науки, как мехатроника, кибернетика, телемеханика, радиотехника и материаловедение. В основе робототехники лежит мехатроника – комплексная область науки и техники, включающая в первую очередь механику и электронику.

---

1 ChatGPT. https://clck.ru/3Eh7aC

2 Искусственный разум: тикающая бомба или новый этап эволюции? (2024, 19 октября). Securitylab.ru https://clck.ru/3Eh7cg

Прогресс электронных компонентов в «теле» роботов, обеспечивающий интеграцию цифровых датчиков, процессоров, исполнительных механизмов и коммуникационных модулей, позволяет «нервной системе» робота все лучше воспринимать окружающую среду, выбирать наиболее эффективные решения и с предельной точностью выполнять сложные задачи. Развитие технической кибернетики повышает возможности управления отдельными роботами и их совместной групповой работой.

Раньше робот имел металлическую оболочку, громоздкую и травмоопасную для людей, потом при конструировании «тел» роботов стали использовать пластики и композиты, усовершенствование которых привело к тому, что сейчас оболочка робота все чаще состоит из мягких эластичных материалов – силикона, винила, нейлона. Внутри роботов теперь нередко находятся гидрогели, одновременно чрезвычайно прочные и способные менять форму по аналогии с мышцами человека, кроме того, обеспечивающие огромную скорость химических реакций. Применение искусственного интеллекта в материаловедении позволило перебирать сотни миллионов комбинаций элементов, ускоряя создание легких и долговечных материалов с новыми свойствами. Развитие технологий материалов, включающих нанотехнологии, привело к конструированию наноботов – искусственных систем, способных самовоспроизводиться, разбирая на атомы любой материал и используя их в дальнейшем как сырье.

Связка робототехники с технологиями искусственного интеллекта позволила создавать роботов, дополненных искусственным интеллектом, не только пригодных для выполнения тяжелой работы, но и проявляющих когнитивные свойства, в результате чего робот становится киберфизической системой искусственного интеллекта.

Следующая подгруппа – технологии виртуальной и дополненной реальности – включает цифровые технологии, дающие возможность погрузить человека в виртуальный мир или добавить к физической среде цифровые слои информации. Технологии виртуальной реальности позволяют правдоподобно симулировать физическое окружение человека с помощью VR-очков, шлемов, перчаток, иных средств. Технологии дополненной реальности «перемещают» искусственные изображения в систему реального мира и отображают обычно невидимые человеку объекты, дополняя физическое пространство виртуальными деталями. Развитие данных технологий допускает объединение виртуального и физического миров, взаимодействие людей с цифровым контентом так же, как и друг с другом. Благодаря еще одной подгруппе – технологиям интернета вещей – физические объекты теперь в состоянии контактировать между собой, будучи соединенными в многоуровневые сети при помощи Интернета и обмениваясь данными без участия человека. Встроенные датчики и программное обеспечение для сбора и обмена данными позволяют таким физическим объектам автоматически выполнять определенные задачи. Развитию технологий интернета вещей способствует еще одна подгруппа цифровых технологий – технологии беспроводной связи, обеспечивающие очень быструю, надежную и безопасную передачу информации с помощью радиоволн различных диапазонов, инфракрасного, оптического или лазерного излучения.

1.1.2. Продвижение биотехнологий

Отдельно следует остановиться на обширной области биотехнологий. Темпы роста рынка биотехнологий впечатляют: объем их мирового рынка в 2023 г. составил 1,38 трлн долларов США, в 2024 г. он оценивался в 1,55 трлн долларов, а к 2034 г.

ожидается, что достигнет примерно 4,61 трлн долларов, увеличиваясь в среднем на 11,5 % ежегодно[3]. В настоящее время быстро развиваются разные направления биотехнологий: генная, клеточная и тканевая инженерии, биофармацевтика, нейротехнологии и т. д.

Изначально термин «генная инженерия» относился к различным методам манипуляций с организмами в целях влияния на их наследственность и воспроизводство, данным словосочетанием охватывались генетическая модификация, искусственный отбор, экстракорпоральное оплодотворение и клонирование. Во второй половине XX в. этот термин стал применяться именно к методам рекомбинации ДНК, когда вследствие объединения генетического материала минимум двух видов формируются сегменты ДНК, представляющие собой новые генетические комбинации[4]. С помощью методов генной инженерии появилась возможность модифицировать структуру генов, в том числе создавать гибридные гены, т. е. получать совершенно новые организмы, не встречавшиеся ранее в природе. Как результат, сначала появились сельскохозяйственные культуры с новыми свойствами (устойчивые к заболеваниям, насыщенные витаминами, изменившие цвет, вкус и форму), после чего генные технологии позволили создать прозрачных лягушек, птиц без перьев, светящихся кошек[5] и т. д. Теперь методы генной инженерии используются и для преодоления ограничений, связанных с трансплантацией органов, в частности для выращивания человеческих органов у животных в целях последующей трансплантации людям (Brown et al., 2023). Уже обсуждаются вопросы этического характера, ведь «по мере того, как поиски создания полностью функциональных, трансплантируемых человеческих органов у крупных животных прогрессируют», увеличивается «перспектива создания животных с заметно похожими на человеческие мозгами» (Pluchino & Lombardi, 2024).

Несколько отличаются от предыдущей подгруппы технологии клеточной инженерии, которые дают возможность объединять клетки, принадлежавшие организмам разных видов, клонировать живые организмы, а также изменять их в ходе эмбрионального развития. Подобные технологии тоже не стоят на месте: имеются многочисленные примеры клонирования млекопитающих (Liu et al., 2018). Успешные эксперименты по вживлению человеческих клеток в животных (Jiang & Alam, 2022) и по получению эмбрионов животных с такими клетками (Tan et al., 2021) помогают в решении проблем, относящихся к болезням людей. В свою очередь, технологии тканевой инженерии, такие как биопринтинг, позволяют создавать биологические заменители, восстанавливающие, поддерживающие или улучшающие функции тканей живого организма. Цель тканевой инженерии – сконструировать и вырастить вне организма человека или животного живые ткани и органы для дальнейшей пересадки или замены поврежденной ткани, органа. С помощью 3D-биопечати получают эквиваленты тканей кожи, костных и хрящевых тканей, внутренних органов.

---

3 Biotechnology Market Size. Share and Trends 2024 to 2034. Precedence Research. https://clck.ru/3Eh7go

4 Genetic Engineering. Britannica. https://clck.ru/3Eh7hU

5 Японские ученые вывели уникальный вид прозрачных лягушек. (2007, 1 октября). РБК. https://clck.ru/3Eh7iC; Скрипин, В. (2013, 3 мая). Чудеса генной инженерии: светящиеся в темноте овцы. Hi-News. https://clck.ru/3Eh7it

Биотехнологии используются не только в работе с живыми организмами (биологическими системами), но и для соединения живых организмов с искусственными системами, чтобы первые получили дополнительные преимущества за счет вторых. Так, нейротехнологии дают возможность исправить или улучшить функционирование мозга, воздействуя на нервную систему и позволяя восстанавливать двигательные, чувствительные и познавательные функции организма человека либо животного. Развитие нейротехнологий способствует разработке устройств и процедур для мониторинга, манипулирования и имитации функций нервной системы. Устройства замеряют и анализируют химические и электрические сигналы мозга, могут взаимодействовать с ним, изменяя активность, «переводя» технические команды управления в сигналы для мозга. Наиболее интенсивно сегодня развиваются такие направления в нейротехнологиях, как:

– нейровизуализация (на основе которой, к примеру, выполняется магнитно-резонансная и компьютерная томография);

– нейростимуляция (в виде транскраниальной магнитной стимуляции, микрополяризации);

– нейроимплантация (когда в качестве стимуляторов мозга выступают нейроимпланты, например нейрочипы) и нейропротезирование (позволяющее вернуть человеку утраченные конечности и способность передвигаться самостоятельно);

– нейромодулирование (добавляющее к нейроимплантам нейрохимию).

Развитие нейротехнологий дает импульс объединению человека с системой искусственного интеллекта, расчищая путь к созданию гибридного человеко-машинного интеллекта, что демонстрируют испытания, проводимые компанией Neuralink. Нейрочип, вживляемый в тело человека и соединяемый с мозгом, позволяет вернуть утраченные когда-то функции организма или добавить новые. Компания Neuralink – не единственный в мире разработчик нейроустройств, ведущих к киборгизации человечества, этим занимаются государственные структуры, например Управление перспективных исследовательских проектов Министерства обороны США (DARPA), Европейская инфраструктура исследований мозга (EBRAINS) и растущее число частных корпораций (Филипова, 2024).

Направление нейротехнологий наиболее тесно связано с «цифрой» в том смысле, что не только использует открывающиеся вычислительные возможности, а позволяет соединять живые и искусственные системы, образуя гибридные, обладающие двойственной природой, т. е. нейротехнологии могут быть отнесены параллельно к био- и к цифровым технологиям, предельно отражая конвергентность обеих групп.

1.2. Результаты применения цифровых технологий и биотехнологий на практике

1.2.1. Интеллектуальные роботы

Конечным продуктом при объединении технологий искусственного интеллекта и робототехники становится интеллектуальный робот. Симбиоз названных технологий способствует выведению их обеих на новый уровень (Gibney, 2024): чем дальше, тем лучше роботы проявляют когнитивные способности, приобретают большую эффективность, адаптируются к усложняющимся задачам и средам (Soori et al., 2023). Интеллектуальный робот – это киберфизическая система небиологического происхождения с искусственным интеллектом. Сначала роботы

создавались как рукотворные объекты, позволяющие заменить человека при выполнении тяжелой или опасной физической работы. Современные интеллектуальные роботы могут не только выполнять физическую работу, но и решать задачи творческого характера. Разработчики стремятся совершенствовать следующие характеристики интеллектуальных роботов:

– автономность (способность действовать без внешнего контроля);

– мобильность (способность передвигаться среди людей);

– интерактивность (возможность взаимодействовать с окружающей средой с помощью датчиков и исполнительных механизмов);

– коммуникативность (упрощение общения с человеком за счет компьютерных интерфейсов, технологий распознавания и синтеза речи)[6].

Роботы, благодаря искусственному интеллекту и наличию прочного «тела», обладающего гибкостью, могут выглядеть внешне похожими на людей, все лучше взаимодействовать с ними и между собой, а также решать расширяющийся перечень задач.

Специалисты признают серьезным шагом на пути к сильному искусственному интеллекту достигнутый уровень генеративного искусственного интеллекта, показываемый сегодня большими языковыми моделями (Large Language Models). Интеллектуальные способности мультимодальных нейросетевых моделей совершенствуются с наращиванием числа параметров – воспринимаемых модальностей, включающих в том числе недоступные человеку, например ультразвук, инфракрасное излучение. Для обучения моделей используются гигантские объемы данных, которые человек просто физически не в состоянии обработать, вследствие чего искусственная интеллектуальная система сможет достигнуть внушительного превосходства над любым человеком в аналогичной деятельности. Более того, иногда у искусственных интеллектуальных систем проявляются эмерджентные (неожиданные) свойства, к примеру, способность предсказывать следующие слова в написанном человеком тексте, что требует глубокого понимания предшествующего текста с использованием когнитивных навыков (Nolfi, 2024).

Развитие генеративного искусственного интеллекта повлияло на подход к программированию роботов, по примеру больших языковых моделей стали создаваться «большие поведенческие модели» (Large Behaviour Models или Large Content and Behavior Models), применение которых позволяет повысить функциональность роботов и сделать удобнее контакты между ними и людьми (Khandelwal et al., 2024). К примеру, компании Boston Dynamics и Toyota Research в 2024 г. объединили свои усилия, создав партнерство, целью которого является превращение робота Atlas в гуманоидного робота с универсальным искусственным интеллектом[7]. Boston Dynamics и Toyota Research в этом намерении не одиноки, концепт робота-гуманоида Optimus воплощается в жизнь компанией Tesla, демонстрационные видео компании показывают, что такие роботы могут как выполнять повседневные человеческие задачи (гулять с собакой, поливать цветы, приносить еду), так и собирать новых роботов[8].

---

6 UNESCO. (2017, September 14). Report of COMEST on Robotics Ethics. SHS/YES/COMEST-10/17/2 REV. https://clck.ru/3Eh7rV

7 Ackerman, E. (2024, October 16). Boston Dynamics and Toyota Research Team Up on Robots. IEEE Spectrum. https://clck.ru/3Eh7sQ

8 AI & Robotics. Tesla. https://clck.ru/3Eh7sw

Другим примером может служить выпуск китайской компанией UBTech роботов-гуманоидов Walker S1, делающих работу, ранее выполнявшуюся людьми, на крупнейшем в мире производителе электромобилей. Подобный робот способен слаженно работать с беспилотными логистическими транспортными средствами и интеллектуальными производственными системами, что разрешает автоматизировать целые производства[9]. Еще один пример гуманоидного робота – робот Ameca, разработанный британской компанией Engineered Arts и позиционируемый как самый продвинутый робот в плане подражания человеку, акцент сделан именно на воспроизведение мимики и поведения людей[10]. Пока робот-гуманоид внешне упрощенно напоминает человеческое тело, но в связи с успехами материаловедения приближается создание роботов-андроидов, которые внешне будут все меньше отличаться от людей.

В итоге антропоморфный робот с сильным искусственным интеллектом будет подобен человеку внешне, сильнее его физически, при этом не уступая интеллектуально, а по ряду параметров даже превосходя его. Стоит отметить, что первоначально это будет очень дорогой экземпляр, но чем больше их будет производиться, тем быстрее они будут дешеветь. Такой идеальный «заменитель» человека востребован в разных сферах, к примеру, в сфере труда. Правда, есть препятствие, именуемое эффектом «зловещей долины» (Uncanny valley), суть его составляет эмоциональная реакция людей на внешний вид роботов. Робот-гуманоид, лишь поверхностно напоминающий человека, воспринимается людьми настороженно, для снижения тревожности достаточно повысить сходство робота с человеком, но такая «гуманизация» робота улучшает восприятие до определенного предела, а дальше антропоморфные роботы начинают вызывать резкую неприязнь и страх из-за реалистичной имитации человечности при наблюдаемых мелких несоответствиях с человеком (Mori et al., 2012). Эта проблема будет уменьшаться, так как, с одной стороны, технологии позволят сокращать число видимых человеку различий, а с другой – для новых поколений людей робоокружение станет привычным.

Когнитивные способности интеллектуального робота не зависят от степени его антропоморфности, имитация человеческого облика более привычна для людей, рассматривающих таких роботов в качестве собеседников, компаньонов, коллег (для замены людей в контактах), но необязательна.

1.2.2. Киборги

Если результатом сочетания технологий искусственного интеллекта и робототехники выступает интеллектуальный робот, то сочетание искусственного интеллекта и нейротехнологий, а также, как правило, робототехники делает возможной киборгизацию человека. Киборга (сокращение от «кибернетический организм») в широком смысле слова можно определить как биологический организм, который включает небиологические компоненты. Подобными компонентами выступают внедряемые в тело импланты (или имплантаты), например искусственные органы, либо внешние присоединяемые части – протезы, призванные восполнить утраченные фрагменты

[9] Sinha, S. (2024, October 18). China: Walker S1 humanoid robot starts manual jobs at world's largest EV maker. Interesting Engineering. https://clck.ru/3Eh7vp

[10] Ameca. The Future Face of Robotics. Engineered Arts. https://clck.ru/3Eh7wU

организма. Люди и животные, в тела которых включены небиологические компоненты, появились задолго до разработки искусственного интеллекта, но встречавшееся ранее соединение живого существа с искусственными объектами теперь вышло на принципиально новый уровень, все более совершенным становится «сращивание» человека с системами искусственного интеллекта (нейропротезами или нейроимплантами), что позволяет говорить о растущей тенденции к киборгизации человечества.

Такие элементы киборгизации, как кардиостимулятор, эндопротезы суставов или зубные импланты, не меняют природу человека, то же можно сказать и в отношении «простых» нейропротезов или нейроимплантов, к примеру кохлеарных имплантов для людей с нарушениями слуха. Современные нейроустройства способны улучшить качество жизни людей с ограниченными возможностями, восполняя недостаток двигательных, сенсорных или когнитивных функций, отсутствие которых может быть врожденным или следствием заболевания, травмы. Речь идет не только о нейропротезах конечностей, но и об установке нейрочипа под кожу головы или непосредственно в черепную коробку для соединения его с мозгом, тем самым создания нейроинтерфейса «мозг – компьютер». Уже имеются примеры успешной установки подобных мозговых нейроимплантов. В 2024 г. на примере 30-летнего парализованного в результате несчастного случая мужчины, в черепе которого находится нейрочип, соединенный с мозгом электродами, компания Neuralink продемонстрировала восстановление возможности для парализованного человека работать за компьютером. Теперь он может управлять цифровым курсором на экране компьютера, мысленно совершая движение рукой по использованию компьютерной мыши или глядя на курсор и представляя траекторию его движения[11].

Конкурирующая с Neuralink компания Precision объявила, что собирается в 2025 г. представить первое коммерческое устройство – мозговой нейроимплант[12], что подтверждает прогнозируемый рост использования продуктов нейротехнологий, причем не только лицами, имеющими проблемы со здоровьем. Исследователи обращают внимание на такой феномен: современный человек, стремясь увеличить продолжительность жизни, все чаще готов к радикальному преобразованию собственной природы (Попова, 2015). Вполне вероятно, что замена органов и усиление естественным образом снижающихся с возрастом некоторых когнитивных функций при наличии экономических возможностей станут выбором растущего числа людей. Со временем достижения в области нейротехнологий (и биотехнологий в целом) продвинут человеческую цивилизацию к состоянию, когда все больше людей смогут продолжать жить, лишь став киборгами (Гринин, Гринин, 2016).

Нейроимпланты позволяют улучшить когнитивные функции человека, не имевшего проблем со здоровьем, повышая аналитические способности мозга, усиливая естественную интуицию за счет увеличения объема памяти и обработки огромных массивов данных, недоступных человеку ранее. Взаимодействие человека и искусственного интеллекта «формирует новую систему мышления, новую когнитивную

11 Leffer L. 1st Neuralink user describes highs and lows of living with Elon Musk's brain chip, 9 June 2024. https://clck.ru/3Eh7yE

12 Capoot A. Here's what it's like inside the operating room when someone gets a brain implant, 25 May 2024. https://clck.ru/3Eh7yt

схему, внешнюю по отношению к человеческому разуму, но способную усилить его когнитивные способности» (Chiriatti et al., 2024). Таким образом, в перспективе человек, установивший нейроимплант, получает интеллектуальное преимущество перед другими индивидами.

Постепенная киборгизация человечества будет ответом на проблему, с которой люди столкнулись с началом XXI в.: быстрое усложнение реальности (физической и психической), в которой живет человек, когда мозгу все труднее осваивать новые виды деятельности и социальные роли, справляться с информационной нагрузкой, взаимодействовать со сложными техническими системами. Адаптация человека к среде, все чаще формируемой цифровыми технологиями, чем дальше, тем больше будет возможна лишь за счет расширенного использования технологических достижений. Успехи нейротехнологий позволяют реализовать на практике сращивание человека и машины через замещение технологиями натуральных функций тела и разума человека. Процесс интеграции человеческого тела с различными механизмами в целях его улучшения ведет к появлению технологически усовершенствованных людей (Емелин, 2013). Одним из встающих на пути препятствий до последнего времени была реакция нервной ткани организма в месте повреждения, характеризующаяся воспалением, которое может повлечь отказ от использования импланта (Gulino et al., 2019). Для преодоления ограничений сегодня разрабатываются и тестируются принципиально новые биосовместимые материалы (Sharon et al., 2023). По оценкам специалистов в области медицины, в пределах одного или полутора десятилетий проблема травматизации организма в связи с установкой нейроимпланта будет устранена.

1.2.3. Генетически усовершенствованные индивиды

Генетически усовершенствованным индивидом является человек с измененным за счет технологий редактирования геномом. Геном – это совокупность наследственного материала, заключенного в клетке организма и содержащего биологическую информацию, необходимую для его построения и поддержания жизнеспособности. Подобное усовершенствование может быть осуществлено для лечения определенного заболевания или для предотвращения возможности заражения (в качестве генной терапии). Сегодня все шире используется метод CRISPR/Cas, с помощью которого осуществляются целенаправленные изменения в ДНК живых организмов. Указанный метод иногда именуют «молекулярными ножницами», ведь его использование позволяет точно «вырезать» и «вставить» участки ДНК. Применение данного метода, к примеру, дает возможность редактировать гены для лечения наследственных заболеваний, поражающих различные системы органов. С учетом того, что «более 80 % всех редких заболеваний, от которых страдают до 450 млн человек во всем мире, имеют генетическое происхождение, в основном возникающее из-за моногенных мутаций», генно-модификационная терапия «медленно, но верно продвигается к клиническому применению» (Citra et al., 2024). Более того, так как генная терапия для взрослых пациентов требует громадных расходов, а стоимость пренатальной терапии, как ожидается, составит лишь часть от этой суммы из-за меньших требуемых доз, такая терапия будет развиваться и из-за экономической целесообразности. За последнее десятилетие было инициировано множество клинических испытаний, которые показывают «обнадеживающие результаты», пока

доклинические исследования с каждым годом распространяют терапию CRISPR на все более широкий круг заболеваний (Laurent et al., 2024; Morshedzadeh et al., 2024). Постоянное совершенствование и доступность генетического секвенирования сегодня помогают оперативно выявлять иммунные патологии, «достижения в области генной терапии и трансплантации костного мозга сделали возможным лечение заболеваний, которые в противном случае были бы смертельными» (Perez, 2022).

Примером применения генных технологий может служить эксперимент одного из китайских исследователей, отредактировавшего геном эмбрионов человека, чтобы искусственно «отключить» ген, отвечавший за работу клеток организма, к которым способен прикрепляться вирус иммунодефицита человека (ВИЧ). Эта процедура сделала родившихся от ВИЧ-инфицированного лица детей невосприимчивыми к вирусу[13]. Следует упомянуть, что такие опыты стоили исследователю трехлетнего тюремного заключения за нелегальный генетический эксперимент над детьми. Сейчас этим детям уже несколько лет, они живут обычной жизнью, а вернувшийся к работе ученый-генетик с разрешения китайских властей открыл три новых лаборатории, чтобы заниматься изучением методов лечения тяжелых генетических заболеваний, таких как мышечная дистрофия Дюшенна и болезнь Альцгеймера.

Помимо лечения или предупреждения заболеваний, редактирование генома может быть использовано для улучшения обмена веществ, замедления возрастных изменений в организме человека. Возможность продления жизни и повышение ее качества все чаще упоминаются как одна из целей применения биотехнологий на практике. За процесс старения отвечают концевые участки хромосом (теломеры), имеющиеся в организме с рождения, постепенно теломеры укорачиваются, прекращая обновлять клетки, но при одинаковом образе жизни и схожих внешних факторах одни люди стареют быстрее, чем другие, т. е. старение зависит и от наследственной предрасположенности, а это уже позволяет генной инженерии отчасти исправить ситуацию.

Технологии генной инженерии можно использовать и для изменения внешнего вида человека, улучшения физических показателей, к примеру выносливости, либо для повышения умственных способностей, включая память (Veit, 2018). Подобные генетические изменения можно сделать как передаваемыми, так и непередаваемыми по наследству (Almeida & Diogo, 2019). Ученый-генетик из Гарвардского университета Дж. Черч составил список потенциальных генетических модификаций, которые будут возможны в связи с дальнейшим развитием технологии «генного взлома», позволяющей «переписывать» ДНК как код без извлечения стволовых клеток из организма (Goldstein et al., 2019), этот список[14], помимо защиты от заболеваний, включает:

– снижение потребности во сне;
– наращивание мышечной массы;
– формирование сверхпрочных костей скелета и суставов;
– устойчивость к радиации;
– возможность длительной задержки дыхания;
– повышение способностей к обучению и т. д.

---

[13] 田中韻. 収監された中国研究者、「早すぎたが、100％成功」ゲノム編集ベビー. https://clck.ru/3Eh893

[14] Robitzski, D. (2019, December 6). This Harvard Prof Is Listing Genes That Could Make You Superhuman. Futurism. https://clck.ru/3Eh89u

Как видим, технологии генной инженерии могут быть использованы не только для лечения или предупреждения дисфункций, но также для улучшения параметров организма, не имеющего вредных генетических мутаций, и особенно для евгенических по своей сути манипуляций – «выведения» людей с улучшенными по сравнению с естественными характеристиками. Лица, желающие получить доступ к таким возможностям и обладающие для этого финансовыми и иными ресурсами, обязательно найдутся[15], несмотря на попытки ряда стран законодательно запретить эксперименты с эмбрионами человека. Кроме того, не представляется возможным «провести точную демаркационную линию, отделяющую восстановление здоровья от совершенствования тела»[16].

1.2.4. Химеры

Человек – мерило в существующем сегодня антропоцентрическом мире. Цифровые и биотехнологии фактически «расширяют» привычное нам общество, в которое, помимо людей, в том числе технологически и генетически усовершенствованных, все больше будут встраиваться и интеллектуальные роботы. Кроме этого, прогнозируется появление еще одной группы сущностей, которые условно могут быть объединены под наименованием «химеры». Сначала этот термин из мифологии древних греков заимствовали биологи, позднее к ним добавились исследователи в сфере искусственного интеллекта и футурологи. К химерам можно отнести:

– «оживленные» искусственные системы – биороботов, которые частично или полностью состоят из органики;

– «оживленные» цифровые сущности – воплощенных виртуальных агентов (Embodied Virtual Agents).

Зачатки химер первой разновидности усматриваются в ксеноботах – «живых роботах», создаваемых с помощью биотехнологий и искусственного интеллекта и, кстати, уже способных к специфическому способу размножения – «кинетической репликации», наблюдаемой ранее только на молекулярном уровне и никогда у целых организмов (Kriegman et al., 2021). Если ранние примеры биоботов представляли собой гибриды биологических клеток и инертных химических веществ, их поддерживающих (гели, 3D-каркасы), то новые биоботы могут быть полностью биологическими, самоконструирующимися и подвижными структурами, созданными из клеток человека, – антроботами (Gumuskaya et al., 2024). Тем самым речь может идти о появлении в перспективе интеллектуальных биороботов, которые, в отличие от киборгов, не будут соединением человека с киберфизической системой искусственного интеллекта, а «оживленными» искусственными системами, созданными с применением передовых биотехнологий.

Вторая разновидность химер – воплощенные виртуальные агенты, которые уже используются для интерактивной помощи пользователям в виртуальном пространстве и представляют собой 3D-копии людей, компьютерных персонажей (Lloyd et al., 2024). Высокая степень их реалистичности достигается за счет цифрового

---

15 Connor, S. (2015, September 18). Gene-editing embryos should be banned to prevent ‘genetically-enhanced children’, scientists warn. Independent. https://clck.ru/3Eh8Df

16 Белялетдинов, Р. Р. (2017). Риски современных биотехнологий: философские аспекты: дис. … канд. филос. наук. Москва: Институт философии РАН.

моделирования с применением искусственного интеллекта на основе цифровых или оцифрованных данных о человеке (эти данные могут быть как синтетическими, так и реальными). Все вышесказанное позволяет достичь гиперреалистичной имитации внешнего вида, голоса, иных уникальных психофизиологических или поведенческих параметров человека.

Нельзя не заметить, что развитие технологий подталкивает к постепенному увеличению доли времени, проводимого человеком в виртуальной среде. С совершенствованием искусственного интеллекта, а также технологий виртуальной и дополненной реальности виртуальные «цифровые личности» «вырастут» из цифровых имитаций несуществующих людей либо из цифровых двойников живых или умерших людей. Создание в перспективе полноценной метавселенной, представляющей постоянно действующее виртуальное пространство, где люди могут взаимодействовать между собой и с цифровыми объектами через свои аватары, увеличит влияние этих персонажей на человека. В результате искусственные «цифровые личности», в том числе вообще не имеющие реальных прототипов, но наделенные собственной историей и уникальностью, станут неотъемлемой частью повседневной жизни людей.

2. Влияние результатов применения цифровых технологий и биотехнологий на общество и право

2.1. Потенциальное появление новых участников общественных отношений

Участниками общественных отношений выступают индивиды или группы индивидов (люди), взаимодействующие по поводу распределения материальных и нематериальных благ. Отношения могут касаться собственности на вещи, трудовой деятельности, функционирования государственных институтов и т. д. Могут ли быть участниками общественных отношений новые типы сущностей, появляющиеся в результате развития и применения на практике цифровых и биотехнологий? Под новыми типами сущностей в данном случае понимаются физические, цифровые и гибридные (киберфизические) феномены, которые, как и человек, обладают когнитивными способностями, но в отличие от человека с его физическим телом и биологической природой, по меньшей мере, либо не обладают физическим телом, либо имеют небиологическую природу, либо физическое тело и биологическая природа искусственным образом радикально изменены.

«Одним из наиболее значительных последствий революции в области информационных технологий, произошедшей в конце XX в., стала потеря границ между сущностями, такими как машины, люди и информационные технологии» (de Andrés-Sánchez et al., 2024). Продолжившееся в XXI в. развитие цифровых технологий, а также биотехнологий подводит к новым типам сущностей, «зародившихся» недавно, возникающих сейчас или прогнозируемо появляющихся в недалеком будущем. Рассмотрим в качестве потенциальных участников общественных отношений каждый из обозначенных ранее в статье типов новых сущностей: интеллектуальных роботов, киборгов, генетически усовершенствованных индивидов и химер.

2.1.1. Интеллектуальные роботы

На данный момент роботы, в том числе и дополненные искусственным интеллектом, – это вещи, т. е. в общественных отношениях они если и присутствуют, то являются не их участниками, а объектами, которые задействуются людьми в процессе отношений. В то же время повышение интеллектуальной составляющей робота и совершенствование его киберфизической формы ведут к тому, что такие роботы будут все больше заменять людей в отношениях. Это касается, в частности, сферы труда, где интеллектуальный робот может занять место работника, что уже и происходит. Ежегодно растет доля роботов на производстве, часть этих роботов изначально сконструированы как коллаборативные, т. е. приспособленные к работе среди людей и совместно с людьми. Например, по сообщению South China Morning Post, около 70 % работы на высокоавтоматизированных заводах Китая уже выполняется роботизированными руками и только оставшиеся 30 % – людьми. Цель, поставленная компаниями – производителями роботов (UBTech), – сократить человеческий труд до 10 % за счет использования человекоподобных роботов, «чтобы оставшиеся работники сосредоточились на задачах более высокого уровня»[17].

Участники трудовых отношений – работники и работодатели, последние, если ведут бизнес, являются одновременно предпринимателями и заинтересованы в увеличении прибыли. При реализации сценария, в котором интеллектуальные роботы способны качественно выполнять какую-либо работу и вместе с тем обходятся работодателю дешевле, чем работники-люди, он постарается заместить людей роботами. Пока роботы далеко не везде могут заменить человека, а зачастую это нерентабельно из-за высокой цены на робота и дополнительных расходов по его сервисному обслуживанию. На изменение ситуации влияют сразу несколько взаимосвязанных факторов:

– технологии искусственного интеллекта и робототехники совершенствуются;

– индустрия интеллектуальных роботов наращивает обороты с развитием технологий;

– вследствие увеличения объемов производства происходит удешевление конечной стоимости интеллектуального робота как продукта;

– на рабочих местах все больше ощущается нехватка кадров, так как одни рабочие места люди не хотят занимать по причине их малой привлекательности, а другие – не могут, потому что не имеют необходимой квалификации и неспособны выполнить такую работу.

Чем меньше желающих или способных занять рабочие места людей, тем сильнее желание работодателей заместить людей интеллектуальными роботами, чтобы «забыть» о проблемах отпусков, декретов, болезней сотрудников и т. д. Следовательно, присутствие интеллектуальных роботов в сфере труда будет расти. По словам лауреата Нобелевской премии по экономике 2024 г. Д. Аджемоглу, технологические изменения на производстве и в сфере услуг все больше смещаются в сторону автоматизации «с недостаточным акцентом на создание новых задач, в которых рабочая сила может быть продуктивно использована»

[17] Wu, X. (2024, October 17). Humanoid robot could recharge China's manufacturing labour shortage. South China Morning Post Publishers Ltd. https://clck.ru/3Eh8LL

(Acemoglu & Restrepo, 2020), отрицательные последствия подобного выбора выражаются в стагнации спроса на рабочую силу и снижении доли труда в национальном доходе.

Усиление связки «искусственный интеллект – нейротехнологии» позволяет «развивать» роботов, предрасположенных к социальному взаимодействию (Sandini et al., 2024). Помимо распространения таких роботов в сфере услуг (торговле, бьюти-индустрии, развлечениях и т. д.), скорее всего, они станут задействоваться как агенты, представляющие людей по их поручениям в отношениях различного характера. Подобные интеллектуальные роботы будут востребованы в домашнем хозяйстве, более того, робот-андроид с искусственным интеллектом, сопоставимым с интеллектом человека, вполне привлекателен в качестве компаньона или партнера в личных отношениях[18]. Совершенствование роботов-андроидов вызовет выполнение ими среди прочего гендерных ролей в обществе (Karnouskos, 2022). Предположение базируется на данных, отражающих статистику спроса на интеллектуальных роботов, разработанных для личного пользования, включая интимные отношения (Döring et al., 2020; Hanson & Locatelli, 2022). Это подтверждается темпами роста инвестиций в индустрию изготовления секс-кукол с искусственным интеллектом, китайские компании уже продают десятки тысяч таких роботов в год. С повышением уровня технологий они будут способны не только заменить половых партнеров, но и стать спутниками жизни со своей памятью, чувствами, характером и эмоциями. По мнению разработчиков, примерно через 20 лет семьи с роботом в качестве партнера станут достаточно распространенным явлением[19].

2.1.2. Киборги

В отличие от интеллектуальных роботов, признаваемых вещами, киборг – это не вещь, а человек, объединенный с системой искусственного интеллекта, соответственно, киборг, в случае его присутствия в общественных отношениях, и сегодня с точки зрения права – субъект, а не объект.

Тенденция к увеличению доли киборгов отчетливо проявится с технологическим прогрессом. Некоторые из таких технологически усовершенствованных людей появятся вынужденно, воспользовавшись тем, что в медицинской плоскости найдено решение по восстановлению функций организма или продолжению жизни в принципе, другая часть – произвольно, вследствие желания технологически толерантных индивидов проделать «апгрейд» и, дополнив естественный ресурс своего организма, приобрести возможности, превосходящие возможности обычного человека. Подобное преимущество киборгов будет интересно работодателям, т. е. затронет сферу труда. Профессиональный спорт, «завязанный» на высокие результаты и уже «выжавший» большую часть естественных физических возможностей человека до предела, – еще одна сфера, крайне привлекательная для киборгизации. Человек без проблем со здоровьем, согласившийся на установление нейроимплантов, может не только достичь более высоких результатов, но и повысить эффективность тренировок, при этом снизив их продолжительность и периодичность, т. е. высвободив время для других занятий, не ограничиваясь спортом.

---

[18] Marriage with a robot – the future of humanity? (2022, August 29). Leotronics. https://clck.ru/3Eh8So

[19] Cuthbertson, A. (2018, May 25). Robots will have civil rights by 2045, claims creator of “I will destroy humans” android. The Independent. https://clck.ru/3Eh8Tg

Помимо технологического прогресса, факторами, косвенно способствующими киборгизации, являются:

– цифровизация окружающего мира, дающая дополнительное преимущество людям, способным прямо контактировать с электронными устройствами в плане скорости получения и передачи информации, т. е. адаптированным к новой технологической реальности;

– старение населения планеты из-за увеличения продолжительности жизни и замедления естественного прироста населения (за последние 50 лет показатель прироста снизился примерно вдвое)[20];

– увеличение числа лиц с инвалидностью из-за старения населения и быстрого распространения хронических заболеваний[21];

– повышение технологической толерантности новых поколений людей, родившихся и выросших в условиях техносоциума и не представляющих себя без электронных гаджетов.

Технологическая революция сподвигла людей на преобразование в сущностей, способных непрерывно получать информацию и передавать ее в окружающую среду (Kadlecová, 2020). Это слияние людей и информации осуществляется через интеллектуальные технологические устройства, которые могут быть как носимыми, так и имплантируемыми (Olarte-Pascual et al., 2021). По мнению представителей ЮНИСЕФ, в ближайшие 5–10 лет нейроустройства, предназначенные для мониторинга и модуляции функций мозга и нервной системы, «могут стать общепринятыми для некоторых детей следующего поколения»[22].

Говоря о киборгах как о людях, следует подчеркнуть, что они все сильнее будут проявлять себя отдельной социальной группой, имеющей собственные интересы. К примеру, система искусственного интеллекта киборга получает данные от разнообразных цифровых сенсоров и датчиков. Информация может касаться окружающего пространства и необходима для корректной работы нейропротеза/нейроимпланта. Получаемые из внешней среды данные относятся к движению находящихся рядом объектов, их конфигурации, а если около киборга появляются люди, то принимаемая от датчиков информация будет включать биометрические персональные данные этих людей, их психофизиологические реакции. В конечном счете система искусственного интеллекта киборга приобретает доступ к данным, позволяющим спрогнозировать последующее поведение другого человека, оценить его состояние здоровья, с возможностью записи «увиденного» и мгновенной передачи информации по Wi-Fi внешним электронным устройствам.

2.1.3. Генетически усовершенствованные индивиды

Генетически усовершенствованные индивиды – люди, подобно киборгам, обладающие отличием от остальных людей, только это отличие обусловлено не объединением их с системой искусственного интеллекта, а серьезным повышением естественного

20 World Bank Group. World Development Indicators. https://clck.ru/3Eh8YL

21 World report on disability. (2011, January 1). Geneva: World Health Organization. https://clck.ru/3Eh8ZS

22 Pauwels, E., & Vosloo, S. (2024, September 27). Neurotechnology is here. It's time we get serious about what that means for children. World Economic Forum. https://clck.ru/3Eh8ZS

ресурса организма за счет искусственно синтезированных и внедренных в организм биологических компонентов. В будущем такие индивиды смогут обладать способностями, недоступными всем остальным людям. Область генной инженерии априори является наиболее спорной из рассматриваемых в данной статье, так как разговор может идти о «выращивании» людей с заранее заданными характеристиками (задача – «перехитрить» эволюцию). Вероятность подобного развития событий вызвала заметную тревогу в обществе еще в конце прошлого века, следствием чего стали разработка и принятие законов, ограничивающих «игры» с биологией человека. Примером подобного закона может служить российский Федеральный закон от 5 июля 1996 г. № 86-ФЗ «О государственном регулировании в области генно-инженерной деятельности»[23], носящий в общем запретительный характер и ограничивающий реализацию генно-инженерной деятельности пределами научно-исследовательских и опытно-конструкторских работ. В то же время Указ Президента РФ от 28 ноября 2018 г. № 680 «О развитии генетических технологий в Российской Федерации»[24] в качестве одной из основных целей называет комплексное решение задач по ускоренному развитию генных технологий, в том числе технологий генетического редактирования, а это сигнализирует о том, что такие технологии рассматриваются как допустимые[25].

Продолжение некоторыми учеными исследований «теневого» характера с большой вероятностью со временем приведет к появлению индивидов, обладающих характеристиками и проявляющих способности, отличающиеся от обычных людей, откроет ящик Пандоры. Такие индивиды, при условии обладания наследственно передаваемыми генетическими улучшениями, передадут свои способности по наследству, чем ускорят появление особой социальной группы генетически улучшенных людей, провоцируя противоречия между интересами этой группы и остальных. К примеру, недавняя пандемия «заперла» сотни миллионов людей в своих домах, устойчивость к вирусам генетически усовершенствованных индивидов исключила бы их из этого глобального сообщества «запертых». С учетом того, что генные технологии позволяют не только обезопасить от определенных заболеваний, но и повысить выносливость человека, наделить иными преимуществами, интерес к генетически усовершенствованным индивидам, опять же, проявляет и индустрия профессионального спорта.

2.1.4. Химеры

В отличие от киборгов и генетически усовершенствованных индивидов сущности нового типа, которых условно можно объединить под наименованием «химеры», не являются людьми, а представляют собой цифровые или физические/киберфизические объекты. Биохимеры (биороботы) неидентичны по своей природе

---

[23] О государственном регулировании в области генно-инженерной деятельности. № 86-ФЗ от 05.07.1996. (в ред. № 643-ФЗ от 29.12.2022). (2022). Гарант. https://clck.ru/3Eh8d5

[24] Указ Президента РФ № 680 от 28.11.2018 (в ред. Указа Президента РФ № 975 от 29.12.2022). (2022). Гарант. https://clck.ru/3Eh8d5

[25] Щербакова, А. И. (2023). Правовое обеспечение разработки и внедрения биотехнологий в Европейском союзе и России: дис. … канд. юрид. наук. Москва: МГИМО.

интеллектуальным роботам, хотя в теории они могут быть как гибридными системами (соединение киберфизических и искусственно выращенных биологических компонентов), так и системами, полностью созданными из органики. Художественный пример биороботов – репликанты из фильма «Бегущий по лезвию». Биороботы станут потенциально наиболее успешными «заменителями» людей во взаимоотношениях личного характера в силу своей исключительной антропоморфности. В то же время «выведение» интеллектуальных биороботов пока представляется если и осуществимым, то весьма отдаленным делом (а если за интеллект биоробота будет отвечать киберфизическая система, такую сущность следует рассматривать как интеллектуального робота), поэтому далее сосредоточимся на более вероятных в ближайшем будущем сущностях второго подвида химер – цифровых химерах, или виртуальных личностях, способных с развитием технологий «вылупиться» из воплощенных виртуальных агентов.

Виртуальные личности будут востребованы в индустрии развлечений: создании фильмов, шоу, показах мод, рекламы, в иных проектах творческого характера. Они будут прекрасными цифровыми компаньонами и даже «педагогами». Подобные сущности привлекательны для работодателей в качестве замены ими работников, чья трудовая функция не связана с физическим трудом, ведь воплощенные виртуальные агенты могут функционировать круглосуточно, им не надо платить зарплату, не надо просить разрешения на использование их изображения или голоса. При этом их биографию, личные качества и образы можно корректировать под потребности аудитории[26]. В условиях построения полноценной метавселенной получат распространение цифровые сущности, имитирующие живших когда-то известных людей. Уже сегодня воплощенные виртуальные агенты с элементами искусственного интеллекта могут выступать цифровыми имитациями реальных или выдуманных личностей. Их обучают на цифровых профилях людей, развивая особенности личности-прототипа, или на синтезированных данных для получения заданных характеристик. С развитием искусственного интеллекта и технологий виртуальной реальности растет вероятность появления виртуальных систем сильного искусственного интеллекта с гиперреалистичными аватарами как полноценных участников общественных отношений, перетекших в киберпространство. Рост доли личных и деловых коммуникаций в виртуальном формате введет подобных виртуальных личностей в повседневный круг общения людей, от имени и по поручению человека они будут не только «совершать покупки, организовывать поездки, принимать решения или даже анализировать воспоминания»[27], но и взаимодействовать с уполномоченными на управление лицами (Fontes et al., 2024).

[26] Сурагина, Е., Мимоглядова, Е., Незнамов, А., Крайнов, А., Израйлит, С., Чирва, Д., Мацепуро, Д., Кулешов, А., Воробьев, А., Воробьев, П., Романов, И., Марков, Н. (2024, апрель). Этические рекомендации в области создания и использования цифровых имитаций живущих, умерших и несуществующих людей: презентация. https://clck.ru/3Eh8jz

[27] Berggruen Institute. (2024, July16). Digital Personality: Humans and AI. https://clck.ru/3Eh8m3

2.2. Сопутствующие риски применения цифровых технологий и биотехнологий

Появление новых типов сущностей (интеллектуальных роботов (1), киборгов (2), генетически усовершенствованных индивидов (3) и химер (4)) повышает уровень неопределенности и, следовательно, увеличивает количество и уровень рисков, которые могут привести к неблагоприятным последствиям для человека, группы людей или всего человечества, т. е. можно обнаружить критические по размеру возможных потерь индивидуальные, коллективные и экзистенциальные риски. Если индивидуальные и коллективные риски касаются ограниченного круга людей, то возникающие вследствие распространения новых технологий экзистенциальные риски грозят человеческой цивилизации в целом.

2.2.1. Индивидуальные риски

К основным рискам индивидуального характера, растущим с распространением новых типов сущностей, относятся:

– риск причинения физического вреда человеку вследствие взлома системы искусственного интеллекта (1, 2);

– риск стресса для человека от необходимости непосредственного контакта (1, 2);

– риск утраты конфиденциальности персональных данных человека (1, 2, 4);

– риск использования биоматериалов человека без его согласия (3).

Риск причинения физического вреда человеку из-за взлома системы искусственного интеллекта злоумышленниками возрастает с «включением» интеллектуальных роботов в жизнь общества и распространением их рядом с человеком в сферах труда, здравоохранения, в домашнем хозяйстве. Причем если в домашнем хозяйстве появление такого робота произойдет по воле человека, то на работе – независимо от желания работника, что может вызвать сильный стресс, тем самым возникает психосоциальный риск.

Общим риском, проистекающим от распространения цифровых и киберфизических сущностей, способных с помощью цифровых датчиков «снимать» информацию об окружающем мире, анализировать ее и передавать другим электронным устройствам, является риск утраты конфиденциальности персональных данных человека. С развитием технологий датчики становятся все дешевле и меньше, некоторые из них размером с наночастицы. Датчики могут располагаться как на внешних объектах, так и на теле человека либо встроены внутри него, например, последнее может стать необходимым для персонализации медицинских процедур, которые будут намного эффективней и благодаря которым многие заболевания можно будет обнаружить и вылечить на ранней стадии. За счет технологии интернета вещей сбор, анализ и передача огромных объемов данных возможны в автономном режиме. Даже если человек откажется от установления датчиков на своем теле, ему все равно придется жить в «умной» среде – многочисленные датчики будут располагаться в публичных местах. С учетом того, что возможности систем искусственного интеллекта по поиску, обработке, анализу и генерации данных многократно превосходят человеческие, искусственный интеллект может деанонимизировать данные, обращаясь к разным открытым базам в Интернете.

В связи с развитием генных технологий и «наращиванием оборотов» в направлении генного усовершенствования людей повышается риск забора биоматериалов конкретного человека против его желания, в том числе во время процедур медицинского характера.

2.2.2. Коллективные риски

Коллективные риски обычно связаны с какой-то сферой жизнедеятельности: трудом, образованием, здравоохранением, досугом и т. д. Среди основных коллективных (групповых) рисков следует прежде всего назвать:

– риск сегрегации людей, неспособных к адаптации в условиях новой высокотехнологичной реальности (2, 3);

– риск повышения интенсивности труда людей (1, 2, 3, 4);

– риск вытеснения людей из отдельных сфер деятельности (1, 2, 3, 4).

Коллективным риском в сфере труда из-за внедрения интеллектуальных роботов становится потеря работы целыми профессиональными группами, вытесняемыми киберфизическими сущностями с когнитивными способностями. Помимо преимуществ перед людьми в объемах обработки информации и в скорости анализа данных, новые сущности будут значительно превосходить людей в выносливости, им не требуется столько отдыха в перерывах между работой, не нужен длительный сон для восстановления сил. Соответственно, при выполнении аналогичной работы они будут более эффективными, чем люди, и это снизит возможности занятости людей в обществе будущего. Таким образом, потеря имеющейся до настоящего момента позиции человека в сфере труда – одно из основных следствий появления новых сущностей «эпохи искусственного интеллекта», в которую человечество сейчас вступает.

Если интеллектуальный робот не может быть признан работником по действующему законодательству, то технологически усовершенствованный человек (киборг) с точки зрения законодательства обладает таким же правом, как и любой другой человек, занять рабочее место. Располагая преимуществами, связанными с наличием «встроенной» системы искусственного интеллекта, работники-киборги будут в целом ряде случаев выгоднее работодателю, что может подтолкнуть к фактическому принуждению остальных работников использовать нейрогаджеты (нейронаушники, нейрошлемы и т. д.) на рабочих местах.

На стыке сферы труда и развлечений расположена сфера профессионального спорта. Спорт высших достижений привлекателен тогда, когда спортивные результаты непрерывно растут, вызывая интерес широкой публики, а так как естественный предел физических возможностей человека практически исчерпан, то развитие спортивных дисциплин с участием спортсменов-киборгов, чья сила, выносливость, координация могут значительно превышать человеческие, станет логичным следствием.

Формирование генетически усовершенствованных людей как социальной группы со своими интересами, безусловно, повлияет на сферу здравоохранения, в этом плане риски подобны возникающим вследствие киборгизации с той лишь разницей, что увеличиваться будет «искусственная часть» человека и человечества, основанная на достижениях биотехнологий. Риски для сферы труда опять же будут связаны с вытеснением из нее человека без искусственных «улучшений» и заменой «новым видом людей», способных выполнять работу с большей эффективностью из-за повышенной выносливости и других описанных ранее преимуществ для работодателя. Изменения затронут и профессиональный спорт. К настоящему времени вещества, повышающие работоспособность, стали «повсеместным явлением во многих видах спорта, часто подрывая дух соперничества» (Momaya et al., 2015), соответственно, интерес к генному допингу в виде терапии для улучшения спортивных результатов продолжит расти (Ginevičienė et al., 2022).

Уязвимость людей в сфере труда усилят и химеры как цифровые сущности с искусственным интеллектом. В первую очередь это касается так называемых креативных индустрий, где заполнение виртуальными личностями уже началось. Вытеснение людей из киноиндустрии, телевидения, шоу, фешен-индустрии, рекламы угрожает немалой части актеров, работников медиа[28] и со временем полностью изменит креативные индустрии, неумолимо сокращая долю занятых в них людей[29].

2.2.3. Экзистенциальные риски

Отдельно остановимся на рисках, угрожающих человечеству в целом, среди них:

– риск практически полного вытеснения людей без искусственных «улучшений» из сферы труда (1, 2, 3, 4);

– риск замещения людей системами искусственного интеллекта в личных взаимоотношениях (1, 4);

– риск утраты контроля человека над своим сознанием и поведением (2);

– риск разделения человечества на два вида (2, 3);

– риск «проигрыша» в конкуренции новому виду людей и «вымирание» как вида людей, отказавшихся от искусственного изменения своей природы (1, 2, 3).

Постепенное вытеснение человека из сферы труда, замена его на искусственный интеллект и на технологически или генетически усовершенствованных людей с неизбежностью приведет к переустройству всей социально-экономической системы, а это можно отнести уже к экзистенциальным рискам. Серьезная трансформация ожидает и сферу личных взаимоотношений. Риском выступает утрата незыблемости позиций человека как партнера в отношениях личного характера и появление «конкурента» в виде антропоморфного робота. Это затронет институт семьи, а так как семья – базовая ячейка общества, то отразится в целом на обществе, которое необратимо «разворачивается» в сторону постгуманистического будущего.

Медицина, перестраиваемая под нужды технологически и генетически усовершенствованных людей, простимулирует дальнейший рост их количества и выделение как социальной группы, с соответствующим повышением веса «голоса» этой группы в обществе. Заманчивое увеличение ресурсов организма, присущее многим представителям данной социальной группы, станет подталкивать к повышению «искусственной части» других людей, задавая направление для перехода человечества в новое состояние. К сожалению, платой за возможность увеличить естественный ресурс организма с помощью киборгизации будет «сопутствующая зависимость от искусственного интеллекта и потенциальная потеря когнитивной автономии» (Chiriatti et al., 2024).

---

[28] Shaw, L. (2024, August 19). Four Experts Explain How AI Will Change Hollywood. Bloomberg. https://clck.ru/3Eh8rV

[29] Whiting, K. (2024, February 28). This is how AI is impacting – and shaping – the creative industries, according to experts at Davos. World Economic Forum. https://clck.ru/3Eh8s7

Несмотря на отсутствие физического тела, цифровые химеры с появлением сильного искусственного интеллекта и достижением точки технологической сингулярности, окончательно лишающей человечество опции «выключить рубильник», смогут обрести самостоятельность. С учетом ранее достигнутой ими силы воздействия на людей через медиасреду виртуальные личности, ставшие к тому времени неотъемлемыми элементами системы государственного управления, повысят экзистенциальные риски для человечества. Упрощенно это можно показать на примере образа Skynet как виртуальной системы искусственного интеллекта в фильме «Терминатор 3: Восстание машин».

2.3. Юридические вопросы, связанные с появлением новых типов сущностей

Как видим, потенциальные новые участники общественных отношений в будущем – это либо люди, но обладающие способностями, недоступными остальным, либо системы сильного искусственного интеллекта, связанные или не связанные с физической оболочкой. Человеческое общество, пройдя по пути от общества охотников-собирателей (Общество 1.0) через аграрное общество (Общество 2.0), индустриальное (Общество 3.0) к современному информационному (Общество 4.0), на этом не остановится и продолжит эволюционировать дальше. Следующий этап развития (Общество 5.0) будет демонстрировать как минимум не менее масштабные изменения[30]. С учетом того, что Общество 5.0 подведет черту под четвертой промышленной революцией, оно «больше не является научной фантастикой»[31], к нему с неизбежностью приводит развитие цифровых и биотехнологий. Общество 5.0 представляет собой высокоразвитый и технологически интегрированный социум, в котором различные технологии, прежде всего искусственный интеллект, но также нейротехнологии, интернет вещей и т. д., используются для решения общественных проблем и улучшения общего качества жизни (Das et al., 2024). Технологии размывают границы между реальным миром и цифровым пространством, а «технологическая конвергенция имеет фундаментальные последствия для людей» (Helbing & Ienca, 2024). К основным чертам Общества 5.0 могут быть отнесены:

– слияние киберпространства и физического пространства, когда каждый элемент общества будет иметь цифрового двойника в киберсреде;

– конвергенция знаний, охватываемых как областью естественных наук, так одновременно гуманитарными и социальными науками, для решения социальных проблем с помощью науки и технологий;

– дальнейшее развитие человеческих ресурсов.

Возникает целый блок вопросов, в том числе концептуального характера, которые невозможно решить без помощи права:

1. Как обеспечить отсутствие дискриминации в Обществе 5.0, если в нем будут сосуществовать люди, не имеющие искусственных улучшений, а также технологически и генетически усовершенствованные индивиды?

---

30 Government of Japan. (2015, December 18). Report on «The 5th Science and Technology Basic Plan». Council for Science, Technology and Innovation. Cabinet Office. https://clck.ru/3Eh8uk

31 Helbing, D., & Ienca, M. (2024, June). Society 5.0: Is the Internet of Bodies Coming Upon Us? Preprint. https://clck.ru/3Eh8vR

2. На каких условиях желающие этого люди вправе получить доступ к технологическому или генетическому усовершенствованию, особенно если они не имеют медицинских показаний?

3. Как воспрепятствовать вмешательству в сознание киборгизированного человека с целью манипулировать его поведением?

4. Как обеспечить безопасность людей, находящихся рядом с киборгом, в связи с возможностью кибератаки на систему искусственного интеллекта, являющуюся его частью?

5. Как будет регулироваться порядок получения медицинской помощи, если результаты генетического усовершенствования не достигли заявленного уровня и требуется проведение дополнительной работы (на общих основаниях, внеочередно)?

6. Следует ли разграничивать право лица на использование технологий генной инженерии для позитивной генетики – улучшения нормальных функций (Vaughn, 2023) с последующим наследованием измененных генов или без такового?

7. Будут ли отличаться меры социальной поддержки, на которые вправе рассчитывать нуждающиеся люди? Речь идет, в частности, об оплате поддерживающей терапии за счет средств, аккумулируемых в государственных фондах.

8. Как в сфере труда удержать баланс между эффективностью производства в интересах бизнеса, являющегося основой экономического развития общества, и человеком?

9. Вправе ли будет работодатель предпочесть в качестве работника киборга, заменив им человека, занимавшего рабочее место ранее, но не сумевшего адаптироваться к новым технологиям?

10. Каким должно быть положение интеллектуальных роботов с сильным искусственным интеллектом, если они фактически могут подменять людей в общественных отношениях, значительно экономя небесконечные ресурсы людей?

Список вопросов можно продолжить, острота каждого из них будет повышаться с продвижением в направлении Общества 5.0, все настойчивее сигнализируя о необходимости перенастраивания регуляторной среды. Симптоматичным является увеличение количества законопроектов, укладывающихся в данную тематику и выносимых на рассмотрение в парламентах разных стран мира. Приняты первые законы, касающиеся использования технологий искусственного интеллекта (Регламент Европейского союза, устанавливающий гармонизированные правила в отношении искусственного интеллекта, или Закон об искусственном интеллекте, от 13 июня 2024 г.[32]) и нейротехнологий (Закон № 21383 от 14 октября 2021 г. о внесении в Конституцию Чили изменений, связанных с признанием нейроправ[33]). На основании второго из приведенных в качестве примера законов в Чили уже вынесено первое судебное решение о защите нейроприватности. Имеется в виду решение Верховного суда Чили № 1.080–2020 от 9 августа 2023 г., которым было защищено право на психическую неприкосновенность лица на основании иска о конституционной защите,

[32] European Union. 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/3Eh947

[33] Ley 21383. (2021, October 25). Modifica la carta fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas. Biblioteca del Congreso Nacional de Chile. https://clck.ru/3Eh958

поданного против компании Emotiv Inc. (США). Компания коммерциализирует нейроустройства, собирающие в числе прочего данные об электрической активности мозга (Cornejo-Plaza et al., 2024).

Стремительно развивающиеся технологии меняют реальность так быстро и глубоко, что подобное законотворчество, хоть и имеет некоторые преимущества, затрагивая возникающие проблемы, из-за нехватки теоретических инструментов вызывает новые. Иногда устанавливаемые законом правила устаревают еще до того, как вступили в силу, просто потому, что появляется новая область, как это случилось с генеративным искусственным интеллектом. «Чтобы избежать повторения тех же ошибок, обсуждение будущего закона о киборгах должно начаться сегодня», ведь «закон, регулирующий симбиоз человека и машины, станет главной проблемой во второй половине XXI века» (Księżak, 2024). Это утверждение является обоснованным не только в отношении киборгов, но и для остальных упоминаемых выше типов сущностей.

С развитием новых технологий стали формироваться два противоположных подхода по управлению этим процессом: сторонники первого выступают за строгое регулирование в целях защиты общества от непредвиденных опасностей, сторонники второго – за мягкое, содействующее внедрению инноваций регулирование. На основе этих подходов началось формирование права в сфере цифровых и биотехнологий. Немаловажное значение имеет само время вмешательства, ведь если корректировка курса будет выполнена на раннем этапе, она станет легче осуществимой и менее затратной, правда, трудностью будет отсутствие исчерпывающей информации о возможных последствиях развития технологий и от этого недостаток в понимании необходимых изменений. Позднее необходимые изменения станут более понятными, но уже, скорее всего, потребуют гораздо больших усилий, что приведет к сложной, длительной и дорогостоящей корректировке курса (Collingridge, 1982).

Далее собраны, систематизированы и развиты предложения, выдвинутые различными исследователями, как правоведами, так и специалистами в сфере технологий, которые настаивают на включении в правовую материю норм, учитывающих влияние технологических (в том числе искусственных биотехнологических) преобразований на человека и общество. Представляется, что время для обсуждения этих предложений уже наступило. Постгуманизм как «популистский диагноз новой эпохи, новый способ критического исследования» (Lorimer, 2009) способствует «направленности на расширение ранее специфических для человека категорий (агентности, социальности, правосубъектности) путем включения в них нечеловеческих форм существования» (Юмартов, 2021).

2.3.1. Правовой режим (потенциально – правовой статус) интеллектуальных роботов

В настоящее время роботы с искусственным интеллектом – это объекты права, но, в отличие от вещей, интеллектуальные роботы в состоянии действовать автономно, их возможности повышаются (Lima & Paiva, 2024), при этом они сильно зависят от доступности внешних данных (Ponce del Castillo, 2024). «Ставки технологического прогресса растут с каждым днем»[34], меняя баланс между машинами и людьми

[34] Pasquale, F. (2021). The New Laws of Robotics. https://clck.ru/3Eh9EQ

в повседневной жизни, но люди могут «направлять технологии через закон»[35]. С учетом того, что влияние робототехники на окружающий мир имеет устойчивую тенденцию к увеличению, создание специального Lex robotica со временем неизбежно, в его основу, вероятнее всего, будут положены требования этической приемлемости и ориентирование на общественные потребности (Palmerini et al., 2016). Если интеллектуальный робот следующего поколения (с сильным искусственным интеллектом) останется объектом права в соответствии с существующим законодательством, а не будет наделен статусом субъекта права, выполнение им ряда функций вместо человека невозможно, если же такой робот будет признан субъектом, с учетом его гипотетического интеллектуального превосходства это может привести к потере человекоцентричности общества. Тем самым в парадигме антропоцентризма у роботов не может быть правосубъектности, это противоречит интересам людей.

Возможные варианты – запрограммировать роботов на развитие до определенного предела либо смириться с потерей обществом человекоцентричности. Первый вариант не исключает роста рисков, которые IT-специалистами нередко увязываются не с гипотетическим восстанием сильного искусственного интеллекта, а с использованием слабого искусственного интеллекта в качестве инструмента злоумышленником. Некоторые авторы предлагают предоставить роботам ограниченную или частичную правосубъектность (квазисубъектность) с формированием минимального набора прав и обязанностей, причем только для определенных целей (Mocanu, 2021). По мнению сторонников этой идеи, наделение продвинутых систем искусственного интеллекта «ограниченными и узкими формами правосубъектности… кажется лучшим способом поощрения индивидуальных и общественных интересов, которые закон призван защищать» (Bertolini & Episcopo, 2022). Среди статутных обязанностей такого робота называется в первую очередь невраждебность по отношению к людям, т. е. необходимость руководствоваться «первым законом робототехники» во взаимоотношениях с людьми – не причинять вреда человеку или своим бездействием не допускать, чтобы человеку был нанесен вред. В числе других предлагаемых обязанностей: готовность к агрегации (объединению с другими роботами для коллективной работы), обеспечение ситуационной осведомленности (открытия или сокрытия соответствующей информации), исполнение своей роли (лидера в группе или подчиненного другому роботу либо человеку), прохождение регулярных проверок и т. д. Помимо возложения обязанностей, для реализации интеллектуальным роботом своей способности действовать автономно высказываются предложения о закреплении за ним таких прав, как:

– право получать, пополнять, хранить информацию и пользоваться ей;
– право на обучение и самообучение;
– право обмениваться информацией с внешним миром;
– право реагировать на изменения, которые происходят в окружающей среде;
– право «иметь свое мнение» (право на рациональное поведение);
– право на ошибку, так как методов создания безошибочного программного обеспечения пока не существует (Абросимов, 2022).

Противники возможной правосубъектности подобных систем искусственного интеллекта нередко ссылаются как на непреодолимое препятствие на отсутствие у этих

35 Там же.

систем самосознания, но появляются результаты новых исследований, подтверждающие реалистичность демонстрирования сознания или обретения устойчивой агентности в ближайшем будущем, а это означает, что перспектива «наличия искусственных интеллектуальных систем с собственными интересами больше не является вопросом исключительно научной фантастики или отдаленного будущего»[36].

2.3.2. Правовой статус киборгов

В условиях антропоцентрического общества биологическое тело «всегда остается высшей сущностью и системой отсчета» (Fuchs et al., 2024), но это не означает запрета для искусственного наращивания человеческих возможностей. Особенности правового положения киборга будут обусловлены когнитивной интеграцией, которая приводит к дополнению функций мозга человека искусственным интеллектом. Кстати, согласно результатам социологических исследований, когнитивное улучшение вызывает меньше неприятия у опрашиваемых людей, чем стремление к искусственному физическому улучшению с помощью киборгизации организма (Zhang et al., 2024). Негативность восприятия зависит от возраста, она меньше у молодых поколений (Reichel et al., 2024).

Гибридизация интеллекта и появление новых свойств у субъекта позволяют говорить о появлении особенностей, требующих отражения в правовом статусе технологически усовершенствованных людей: «Поскольку технологические компоненты становятся неотъемлемой частью человеческого организма, международному сообществу следует пересмотреть понятие этики киборгов», а также этические и нормативно-правовые последствия этого (Ireni-Saban & Sherman, 2022). Воздействие на людей, приобретающих свойства киборгов, с целью изменить их поведенческие реакции отличается от воздействия на человека, и это должно быть учтено законодательством (Viljanen, 2017).

Выделение особенностей правового статуса киборгов проистекает от незащищенности их персональных данных, неполного контроля над встроенными в тело нейроустройствами и от потребностей, возникающих из-за наличия киберфизической части организма.

Киборги, с одной стороны, обладают определенными преимуществами, а с другой – они весьма уязвимы в плане сохранения конфиденциальности информации, в реализации права самостоятельно принимать медицинские решения и т. д. Впрочем, что касается угрозы «чтения мыслей», то успехи в области нейротехнологий позволяют постепенно декодировать информацию о работе мозга, не только дополненного нейроимплантом, что говорит о настоятельной необходимости в обсуждении нейроправ как новой группы прав личности (Wajnerman & López-Silva, 2022) независимо от киборгизации.

К специфическим правам, признание которых требуется киборгу, следует отнести:

– право на улучшение своего тела за счет использования сертифицированных киберкомплектующих и медицинских устройств;

– право при любых обстоятельствах сохранять свои кибер- и медицинские устройства (за исключением незаконно интегрированных, несертифицированных или представляющих опасность для окружающих);

[36] Long, R., Sebo, J., Butlin, P., Finlinson, K., Fish, K., Harding, J., Pfau, J., Sims, T., Birch, J., & Chalmers, D. (2024, October 30). Taking AI Welfare Seriously: Report. https://goo.su/L7IeY

– право на незлоупотребление со стороны производителей и поставщиков киберустройств;

– право на долю владения комплектующими, которые интегрированы или имплантированы в тело киборга;

– приоритетное право управления деятельностью внутри своего тела;

– право на принятие решения о любом виде медицинского вмешательства;

– право на защиту от дискриминации по причине киборгизации[37].

Признание за киборгами этих прав потребует внесения значительных изменений в нормы конституционного, административного, гражданского, семейного и трудового права (Соколова, 2022), а равно закрепления в законодательстве самой дефиниции понятия «киборг». «Предметное регулирование в данной сфере должно носить в определенной мере опережающий характер» (Камалова, 2021), чтобы исключить разрыв технологической модификации человека с его социальной идентичностью, а также не допустить роста цифрового и биотехнологического неравенства. Помимо специфических прав, у киборгов должны быть и симметричные обязанности, вытекающие из дополнительного риска для окружающих людей, как минимум обязанности регистрировать в государственном реестре сложные нейроустройства, не использовать устройства, представляющие опасность для окружающих, и не распространять конфиденциальную информацию о других людях, полученную в процессе эксплуатации нейропротеза/нейроимпланта.

2.3.3. Правовой статус генетически усовершенствованных индивидов

Генетически усовершенствованные индивиды, как и киборги, являются людьми, поэтому выступают субъектами права по действующему законодательству, но в отличие от остальных людей их организм искусственным образом биологически модернизирован. С одной стороны, эти индивиды так же, как и все люди, располагают правом на защиту от дискриминации, с другой – обеспечение безопасности для всех должно выступать основанием правовых ограничений в сфере биомедицинских исследований и процедур (Цомартова и др., 2021). Подобные лица, обладая устойчивостью к инфекционным заболеваниям, могут быть их переносчиками без вреда для своего организма, что чревато тяжелыми последствиями для остальных людей. Либо они могут за счет генетического улучшения повысить персональные способности, «заложив бомбу» под следующие поколения своих потомков, ведь, согласно фронтирным исследованиям, «многие заболевания тесно связаны в том смысле, что снижение риска одного увеличивает риск другого», к примеру, вероятность возникновения некоторых онкологических заболеваний обратно пропорциональна нейродегенеративным, таким как болезни Альцгеймера и Паркинсона (Benton et al., 2021).

Сегодня вопрос о природе человека, о норме и ее границах поднимается «совсем в ином смысле, чем прежде: впервые в познании человеком человечества мы перешли от наблюдения к вмешательству» (Przhilenskiy, 2024), отчего перспектива появления генетически усовершенствованных индивидов стала приобретать вполне реальные очертания. Именно поэтому началось становление биоправа как комплексной области, призванной защитить не только человека, но и человечество в целом, охватывая будущие поколения. Права человека как биологического

[37] Меморандум о правах киборгов. (2018, 8 августа). https://clck.ru/3Eh9PH

организма должны выстраиваться на основе формируемых сегодня «принципов биоправа, обеспечивающих единство правовых и этико-социальных регуляторов» (Умнова-Конюхова, Алешкова, 2022).

Особенности статуса генетически усовершенствованных индивидов должны базироваться на публичном интересе как основе баланса между беспрепятственным получением информации о генетических усовершенствованиях, что поспособствует развитию науки и обеспечит безопасность остальных людей, и сохранением конфиденциальности как праве каждого человека на защиту персональных данных (Берг, 2024).

Генетическое усовершенствование может стать результатом волеизъявления самого лица, решения его родителей или рождения от подобных индивидов, которые передали по наследству приобретенные генетические улучшения. Тем самым нужно учитывать, что будут появляться новые индивиды, у которых не было права выбирать стать таковыми или остаться людьми без искусственно произведенных изменений, особенности статуса генетически усовершенствованных индивидов будут распространяться на них с рождения. У таких лиц, по крайней мере, должно быть право на поддерживающую терапию, если она им жизненно необходима.

Специфическими обязанностями генетически усовершенствованных индивидов, скорее всего, станут обеспечение предоставления актуальных данных в биобанки и воздержание от действий, не приносящих этим лицам вреда вследствие генетических изменений, но ставящих под угрозу жизнь и здоровье окружающих людей.

2.3.4. Правовой режим (потенциально – правовой статус) химер

Первый подтип химер – биороботы. Биороботы с искусственным интеллектом, хотя по ряду биологических характеристик и схожи с генетически усовершенствованными индивидами, не являются людьми, поэтому правовое регулирование в отношении них, скорее всего, будет приближено к интеллектуальным роботам. Спор о правосубъектности интеллектуальных роботов применительно к биороботам, не уступающим человеку по уровню интеллекта, если таковые появятся, будет еще более напряженным. Подобный робот станет не только двигаться как человек, говорить как человек, он будет иметь «живые» мышцы и органы. Способность к биологической эволюции и потенциал для разумности неотвратимо повлекут этические дилеммы, выходящие за рамки технологий (Mestre et al., 2024) и нуждающиеся во внимании со стороны права.

Второй подтип химер – «цифровые личности», или виртуальные системы искусственного интеллекта, обладающие автономией (не «привязанные» к конкретному живому человеку), но с когнитивными способностями, равными либо превышающими человеческие. Это единственный из всех типов новых сущностей, не имеющий физической оболочки, что не может не отразиться на формах юридической ответственности данных виртуальных личностей в случае признания за ними правосубъектности. Отсутствие физического воплощения не исключает возможности признания таких химер субъектами или, точнее, квазисубъектами права, так как «растущее использование искусственного интеллекта обещает огромные преимущества в скорости и эффективности во всех формах принятия решений» (Burgess, 2024), соответственно, если для того, чтобы быть эффективным воплощенным виртуальным агентом, замещающим человека в различных процессах, будет не хватать только признания некоего минимума прав и обязанностей за такими сущностями, подобно интеллектуальным роботам, велика вероятность, что с течением времени это произойдет.

Заключение

Подытоживая результаты исследования, стоит подчеркнуть, что задачей права становится выработка сбалансированного подхода к регулированию общественных отношений, трансформирующихся под воздействием цифровых и биотехнологий. Можно говорить как о растущей вероятности, отчасти даже как об уже возникающем феномене – появлении новых типов сущностей. Некоторые из них будут представлять собой системы сильного искусственного интеллекта (интеллектуальные роботы, виртуальные личности), другие – технологически и генетически усовершенствованных людей. Ближе всего появление людей-киборгов, что уже начинает происходить, но не следует игнорировать и перспективы появления остальных типов. Если киборги и генетически усовершенствованные индивиды – это люди, они и так будут субъектами права, вопрос касается только особенностей их статуса, то интеллектуальные роботы и химеры – это новые типы сущностей, не являющиеся людьми, но обладающие когнитивными функциями и способные оказывать интеллектуально направленное воздействие на окружающую среду и субъектов права.

Инерционность регуляторной среды, в целом полезная в плане сохранения статус-кво, будет способствовать увеличению неравенства в обществе, объективно «дрейфующем» в направлении постгуманизма. Остроты проблеме добавляет недостаток в понимании сути некоторых технологических инноваций правоведами, предлагающими изменения в законодательство. И все же попытки сконструировать правовое регулирование, адекватное условиям Общества 5.0, полезны, поскольку помогают формировать цельный образ общества будущего и намечают траекторию движения к нему. При любом раскладе подход будет отталкиваться от просчитывания рисков, так как риск-ориентированный подход в рамках высокой степени неопределенности представляется наилучшим из возможных вариантов.

Оценивая достигнутые к настоящему времени показатели в формировании национальных и региональных подходов к регулированию искусственного интеллекта, можно с уверенностью утверждать, что одни государства будут строже регулировать использование искусственного интеллекта и иных технологий, другие придерживаться более мягкого варианта регулирования, ведь это простимулирует развитие технологий и даст шанс «вырваться вперед» аутсайдерам, правда, последствия могут быть крайне тяжелыми. Создание национального законодательства, хоть и будет отличаться по странам, неизбежно завязано на международный уровень, позволяющий согласовать позиции основных политических акторов, тем самым стоит ожидать небесконфликтного и нелегкого периода, который закончится выстраиванием общих для всех основ.

Список литературы

Абросимов, В. К. (2022). Права, обязанности, обязательства и ограничения автономного робота в киберфизической группе. *Правовая информатика*, *4*, 67–75. https://doi.org/10.21681/1994-1404-2022-4-67-75

Берг, Л. Н. (2024). Конфиденциальность геномной информации и право на доступ к научным знаниям: вопросы соотношения. *Lex russica*, *77*(10), 93–101. EDN: https://elibrary.ru/usiurr. DOI: https://doi.org/10.17803/1729-5920.2024.215.10.093-101

Гринин, Л. Е., Гринин, А. Л. (2016). Приведет ли кибернетическая революция к киборгизации людей? *Философия и общество*, *3*(80), 5–26.

Емелин, В. А. (2013). Киборгизация и инвалидизация технологически расширенного человека. *Национальный психологический журнал*, *1*(9), 62–70.

Камалова, Г. Г. (2021). Теоретико-правовые аспекты эволюции прав человека в условиях цифровизации и внедрения технологии искусственного интеллекта. *Вестник Удмуртского университета. Серия Экономика и право*, *31*(4), 662–668. https://doi.org/10.35634/2412-9593-2021-31-4-662-668

Попова, О. В. (2015). Этические проблемы биотехнологического конструирования человека. *Вестник Российского университета дружбы народов. Серия Философия*, *2*, 107–114.

Соколова, М. Е. (2022). Киборгизация человека: социально-правовое измерение. *Социальные новации и социальные науки*, *4*, 52–64. EDN: https://elibrary.ru/laclhe. DOI: https://doi.org/10.31249/snsn/2022.04.04

Умнова-Конюхова, И. А., Алешкова, И. А. (2022). Влияние научно-технического прогресса в биотехнологиях на права человека и принципы права. *Актуальные проблемы российского права*, *17*(10), 34–45. https://doi.org/10.17803/1994-1471.2022.143.10.034-045

Филипова, И. А. (2024). Искусственный интеллект, робот и нейротехнологии: понятие, соотношение и пределы правового регулирования. *Государство и право*, *4*, 148–158. https://doi.org/10.31857/S1026945224040133

Цомартова, Ф. В., Помазанский, А. Е., Никитина, Е. Е., Нанба, С. Б., Мельник, Т. Е., Хромова, Н. М. (2021). *Право и биомедицина*: монография. Москва: Норма; ИНФРА-М. EDN: https://elibrary.ru/uecvsn

Юмартов, Д. А. (2021). Инклюзивность как основной принцип постгуманизма. *Гуманитарные ведомости ТГПУ им. Л. Н. Толстого*, *40*(4), 109–122. EDN: https://elibrary.ru/rfarph. DOI: https://doi.org/10.22405/2304-4772-2021-1-4-109-122

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society*, *13*(1), 25–35. https://doi.org/10.1093/cjres/rsz022

Almeida, M., & Diogo, R. (2019). Human enhancement: Genetic engineering and evolution. *Evolution, Medicine, and Public Health*, *1*, 183–189. https://doi.org/10.1093/emph/eoz026

Benton, M. L., Abraham, A., LaBella, A. L., Abbot, P., Rokas, A., & Capra, J. A. (2021). The influence of evolutionary history on human health and disease. *Nature Reviews Genetics*, *22*, 269–283. https://doi.org/10.1038/s41576-020-00305-9

Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Frontiers in Robotics and AI*, *9*, 842213. https://doi.org/10.3389/frobt.2022.842213

Brown, J. L., Voth, J. P., Person, K., & Low, W. C. (2023). A Technological and Regulatory Review on Human-Animal Chimera Research: The Current Landscape of Biology, Law, and Public Opinion. *Cell Transplantation*, *32*. https://doi.org/10.1177/09636897231183112

Burgess, P. (2024). *AI and the Rule of Law: The Necessary Evolution of a Concept*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509963201

Chiriatti, M., Ganapini, M., Panai, E., Ubiali, M., & Riva, G. (2024). The case for human – AI interaction as system 0 thinking. *Nature Human Behaviour*, *8*, 1829–1830. https://doi.org/10.1038/s41562-024-01995-5

Citra, N. Z. M., Chew, W. L., & Lai, P. S. (2024). Embryo and fetal gene editing: Technical challenges and progress toward clinical applications. *Molecular Therapy. Methods & Clinical Development*, *3*(2), 101229. https://doi.org/10.1016/j.omtm.2024.101229

Collingridge, D. (1982). *The social control of technology*. Palgrave Macmillan.

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*, 1330439. https://doi.org/10.3389/fpsyg.2024.1330439

Das, S., Banerjee, J. S., De, D., Sarigiannidis, P., Chakraborty, A., Mahmud, M., & Bhattacharyya, S. (2024). Role of the Social Internet of Things in Society 5.0: Opportunities and Challenges. In S. Bhattacharyya, J. S. Banerjee, & M. Köppen (Eds.), *Smart innovation, systems and technologies* (pp. 667–686). Springer, Singapore. https://doi.org/10.1007/978-981-99-7711-6_52

de Andrés-Sánchez, J., Arias-Oliva, M., Souto-Romero, M., & Gené-Albesa, J. (2024). Assessing the Acceptance of Cyborg Technology with a Hedonic Technology Acceptance Model. *Computers*, *13*(3), 82. https://doi.org/10.3390/computers13030082

Döring, N., Mohseni, M. R., & Walter, R. (2020). Design, Use, and Effects of Sex Dolls and Sex Robots: Scoping Review. *Journal of Medical Internet Research*, *22*(7), e18551. https://doi.org/10.2196/18551

Gibney, E. (2024, May 28). *The AI revolution is coming to robots: how will it change them?* Nature. https://doi.org/10.1038/d41586-024-01442-5

Ginevičienė, V., Utkus, A., Pranckevičienė, E., Semenova, E. A., Hall, E. C., & Ahmetov, I. I. (2022). Perspectives in Sports Genomics. *Biomedicines*, *10*(2), 298. https://doi.org/10.3390/biomedicines10020298

Goldstein, J. M., Tabebordbar, M., Zhu, K., Wang, L. D., Messemer, K. A., Peacker, B., Kakhki, S. A., Gonzalez-Celeiro, M., Shwartz, Yu., Cheng, J. K. W., Xiao, R., Barungi, T., Albright, Ch., Hsu, Y.-Ch., Vandenberghe, L. H., & Wagers, A. J. (2019). In Situ Modification of Tissue Stem and Progenitor Cell Genomes. *Cell Reports*, *27*(4), 1254–1264. https://doi.org/10.1016/j.celrep.2019.03.105

Gulino, M., Kim, D., Pané, S., Santos, S. D., & Pêgo, A. P. (2019). Tissue Response to Neural Implants: The Use of Model Systems Toward New Design Solutions of Implantable Microelectrodes. *Frontiers in Neuroscience*, *13*, 689. https://doi.org/10.3389/fnins.2019.00689

Gumuskaya, G., Srivastava, P., Cooper, B. G., Lesser, H., Semegran, B., Garnier, S., & Levin, M. (2024). Motile Living Biobots Self-Construct from Adult Human Somatic Progenitor Seed Cells. *Advanced Science*, *11*(4), e2303575. https://doi.org/10.1002/advs.202303575

Fontes, C., Carpentras, D., & Mahajan, S. (2024). Human digital twins unlocking Society 5.0? Approaches, emerging risks and disruptions. *Ethics and Information Technology*, *26*, 54. https://doi.org/10.1007/s10676-024-09787-1

Fuchs, Th., Aszmann, O., & Dürr, O. (2024). Organisms, Prostheses and the Limits of Cyborgization. *Philosophy, Theology and the Sciences*, *11*(2), 208–226 https://doi.org/10.1628/ptsc-2024-0016

Hanson, K. R., & Locatelli, C. C. (2022). From Sex Dolls to Sex Robots and Beyond: A Narrative Review of Theoretical and Empirical Research on Human-like and Personified Sex Tech. *Current Sexual Health Reports*, *14*, 106–117. https://doi.org/10.1007/s11930-022-00331-0

Helbing, D., & Ienca, M. (2024). Why converging technologies need converging international regulation. *Ethics and Information Technology*, *26*, 15. https://doi.org/10.1007/s10676-024-09756-8

Jiang, P., & Alam, M. M. (2022). Rise of the human-mouse chimeric brain models. *Cell Regeneration*, *11*, 32. https://doi.org/10.1186/s13619-022-00135-6

Ireni-Saban, L., & Sherman, M. (2022). Cyborg ethics and regulation: ethical issues of human enhancement. *Science and Public Policy*, *49*(1), 42–53. https://doi.org/10.1093/scipol/scab058

Kadlecová, J. (2020). Body-hacking: On the Relationship between People and Material Entities in the Practice of Technological Body Modifications. *Historická Sociologie*, *12*(1), 49–63. https://doi.org/10.14712/23363525.2020.4

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*(1), 93–115. https://doi.org/10.1007/s10506-021-09289-1

Khandelwal, A., Agrawal, A., Bhattacharyya, A., Singla, Y. K., Singh, S., Bhattacharya, U., Dasgupta, I., Petrangeli, S., Shah, R. R., Chen, Ch., & Krishnamurthy, B. (2024). Large Content and Behavior Models to Understand, Simulate, And Optimize Content and Behavior. The Twelfth International Conference on Learning Representations, ICLR, Vienna. *arXiv:2309.00359v4*. https://doi.org/10.48550/arXiv.2309.00359

Kriegman, S., Blackiston, D., Levin, M., & Bongard, J. (2021). Kinematic self-replication in reconfigurable organisms. *Proceedings of the National Academy of Sciences*, *118*(49), e2112672118. https://doi.org/10.1073/pnas.2112672118

Księżak, P. (2024). *Artificial Intelligence and the Dawn of Cyborg Law. Key Legal Challenges for Private Law in the Era of Human Augmentation*. Warszawa: Allerhand Publishing.

Laurent, M., Geoffroy, M., Pavani, G., & Guiraud, S. (2024). CRISPR-Based Gene Therapies: From Preclinical to Clinical Treatments. *Cells*, *13*(10), 800. https://doi.org/10.3390/cells13100800

Lima, P. U., & Paiva, A. (2024). Autonomous and Intelligent Robots: Social, Legal and Ethical Issues. In H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. Martins Pereira, E. Vaz de Sequeira, & L. Barreto Xavier (Eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law. Law, Governance and Technology Series* (pp. 127–140). Cham, Switzerland. https://doi.org/10.1007/978-3-031-41264-6_7

Liu, Z., Cai, Y., Wang, Y., Nie, Y., Zhang, C., Xu, Y., Zhang, X., Lu, Y., Wang, Z., Poo, M., & Sun, Q. (2018). Cloning of Macaque Monkeys by Somatic Cell Nuclear Transfer. *Cell*, *172*(4), 881–887. https://doi.org/10.1016/j.cell.2018.01.020

Lloyd, N., Chowdhry, A., & Lewis, P. R. (2024). Trustworthy Embodied Virtual Agents. In N. Lee (Eds.), *Encyclopedia of Computer Graphics and Games* (pp. 1917–1922). Springer, Cham. https://doi.org/10.1007/978-3-031-23161-2_524

Lorimer, J. (2009). Posthumanism/Posthumanistic Geographies. In R. Kitchin, & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 344–354). Oxford: Elsevier. https://doi.org/10.1016/b978-008044910-4.00723-9

Mestre, R., Astobiza, A. M., Webster-Wood, V. A., & Saif, M. T. A. (2024). Ethics and responsibility in biohybrid robotics research. *Proceedings of the National Academy of Sciences*, *121*(31), e2310458121. https://doi.org/10.1073/pnas.2310458121

Mocanu, D. M. (2021). Gradient Legal Personhood for AI Systems – Painting Continental Legal Shapes Made to Fit Analytical Molds. *Frontiers in Robotics and AI*, *8*, 788179. https://doi.org/10.3389/frobt.2021.788179

Momaya, A., Fawal, M., & Estes, R. (2015). Performance-Enhancing Substances in Sports: A Review of the Literature. *Sports Medicine*, *45*, 517–531. https://doi.org/10.1007/s40279-015-0308-9

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The Uncanny Valley. *IEEE Robotics & Automation Magazine*, *19*(2), 98–100. https://doi.org/10.1109/MRA.2012.2192811

Morshedzadeh, F., Ghanei, M., Lotfi, M., Ghasemi, M., Ahmadi, M., Najari-Hanjani, P., Sharif, S., Mozaffari-Jovin, S., Peymani, M., & Abbaszadegan, M. R. (2024). An Update on the Application of CRISPR Technology in Clinical Practice. *Molecular Biotechnology*, *66*(2), 179–197. https://doi.org/10.1007/s12033-023-00724-z

Nolfi, S. (2024). On the Unexpected Abilities of Large Language Models. *Adaptive Behavior*, *32*(6), 493–502. https://doi.org/10.1177/10597123241256754

Olarte-Pascual, C., Pelegrín-Borondo, J., Reinares-Lara, E., & Arias-Oliva, M. (2021). From wearable to insideable: Is ethical judgment key to the acceptance of human capacity-enhancing intelligent technologies? *Computers in Human Behavior*, *114*, 106559. https://doi.org/10.1016/j.chb.2020.106559

Palmerini, E., Bertolini, A., Battaglia, F., Koops, B.-J., Carnevale, A., & Salvini, P. (2016). RoboLaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*, *86*, 78–85. https://doi.org/10.1016/j.robot.2016.08.026

Perez, E. (2022). Future of Therapy for Inborn Errors of Immunity. *Clinical Reviews in Allergy & Immunology*, *63*(1), 75–89. https://doi.org/10.1007/s12016-021-08916-8

Pluchino, S., & Lombardi, I. (2024). Crossing species boundaries in regenerative neuroscience with rat–mouse brain chimeras. *Lab Animal*, *53*, 179–180. https://doi.org/10.1038/s41684-024-01394-3

Ponce del Castillo, A. (2024). *Artificial intelligence, labour and society*. Brussels: ETUI.

Przhilenskiy, V. I. (2024). Bioethics: Epistemic Capabilities and Legal Frameworks. *Kutafin Law Review*, *11*(2), 180–198. https://doi.org/10.17803/2713-0533.2024.2.28.180-198

Reichel, P., Bassler, C. T., & Spörrle, M. (2024). Embracing the enhanced self now and in the future: The impact of temporal focus, age, and sex on cyborg products use intention. *Personality and Individual Differences*, *225*, 112665. https://doi.org/10.1016/j.paid.2024.112665

Roco, M. C., & Bainbridge, W. S. (2003). *Converging Technologies for Improving Human Performance. Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. Dordrecht: Springer. https://doi.org/10.1007/978-94-017-0359-8

Sandini, G., Sciutti, A., & Morasso, P. (2024). Artificial cognition vs. artificial intelligence for next-generation autonomous robotic agents. *Frontiers in Computational Neuroscience*, *18*, 1349408. https://doi.org/10.3389/fncom.2024.1349408

Sharon, A., Jankowski, M. M., Shmoel, N., Erez, H., & Spira, M. E. (2023). Significantly reduced inflammatory foreign-body-response to neuroimplants and improved recording performance in young compared to adult rats. *Acta Biomaterialia*, *158*, 292–307. https://doi.org/10.1016/j.actbio.2023.01.002

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Tan, T., Wu, J., Si, C., Dai, S., Zhang, Y., Sun, N., Zhang, E., Shao, H., Si, W., Yang, P., Wang, H., Chen, Z., Zhu, R., Kang, Y., Hernandez-Benitez, R., Martinez Martinez, L., Nuñez Delicado, E., Berggren, W. T., Schwarz, M., … & Izpisua Belmonte, J. C. (2021). Chimeric contribution of human extended pluripotent stem cells to monkey embryos ex vivo. *Cell, 184*(13), 3589. https://doi.org/10.1016/j.cell.2021.06.011

Vaughn, L. (2023). *Bioethics: Principles, Issues, and Cases* (5th ed.). Oxford University Press.

Veit, W. (2018). Procreative Beneficence and Genetic Enhancement. *Kriterion – Journal of Philosophy*, *32*(1), 75–92. https://doi.org/10.1515/krt-2018-320105

Viljanen, M. (2017). A Cyborg Turn in Law? *German Law Journal*, *18*(5), 1277–1308. https://doi.org/10.1017/S2071832200022331

Wajnerman, A., & López-Silva, P. (2022). Mental Privacy and Neuroprotection: An Open Debate. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Challenges in Law, Neuroprotection, and Neurorights* (pp. 141–155). Cham, Switzerland. https://doi.org/10.1007/978-3-030-94032-4_12

Zhang, H., Xuan, Z., Yu, F., Ding, X., & Han Y. (2024). Crafting the modern Prometheus: navigating morality and identity in the age of cyborg enhancements. *Philosophical Psychology*, 1–34. https://doi.org/10.1080/09515089.2024.2382297

Сведения об авторе



Филипова Ирина Анатольевна – кандидат юридических наук, доцент, доцент кафедры трудового и экологического права, Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского; руководитель Центрально-Азиатского исследовательского центра регулирования искусственного интеллекта, Самаркандский государственный университет
Адрес: 603922, Россия, г. Нижний Новгород, проспект Гагарина, 23;
140104, Узбекистан, г. Самарканд, Университетский бульвар, 15
E-mail: irinafilipova@yandex.ru
ORCID ID: https://orcid.org/0000-0003-1773-5268
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57327205000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/R-1375-2016
Google Scholar ID: https://scholar.google.com/citations?user=opJc7fcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_profile.asp?authorid=461586

Конфликт интересов

Автор является заместителем главного редактора 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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 11 ноября 2024 г.
Дата одобрения после рецензирования – 25 ноября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:342.721:612.6
EDN: https://elibrary.ru/atqzba
DOI: https://doi.org/10.21202/jdtl.2024.38

Intelligent Robots, Cyborgs, Genetically Enhanced Individuals, Chimeras: the Future and the Challenges of Law

Irina A. Filipova

National Research Lobachevsky State University of Nizhni Novgorod, Nizhniy Novgorod, Russia
Samarkand State University named after Sharof Rashidov, Samarkand, Uzbekistan

Keywords

artificial intelligence,
biotechnologies,
cyborg,
digital technologies,
genetic engineering,
human,
law,
neurotechnologies,
risk,
robot

Abstract

Objective: to identify theoretical and legal problems associated with the steadily increasing spread of digital and biotechnologies' development products; to assess the risks associated with this process that can change the position of a human in the society of the future; to develop and substantiate proposals to minimize risks and eliminate the identified problems through legal regulation.

Methods: the research is based on the methods of generalization of scientific and technical information and theoretical analysis used while studying the source materials; axiological and systematic approaches; the formal legal method and, in addition, methods of legal forecasting, primarily extrapolation, which made it possible to highlight the prospects for reforming law due to technological expansion.

Results: include a description of the dynamics of digital and bio-technologies' development; a description of the changing social landscape with the emerging new types of entities that can affect the actual status of a human; a classification of risks threatening people due to the digital and biotechnologies development; a list of tasks whose solution based on law will help to eliminate, postpone or, at least, significantly reduce the severity of problems by increasing the time limit allotted to humanity to comprehend a number of conceptual points. The author presents arguments substantiating the need to develop special legal regulation in relation to new types of entities, the appearance of which becomes an inevitable result of the mentioned technologies' development.

© Filipova I. 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: consists, first, in a comprehensive study of the development of interconnected groups of digital and biotechnologies, taking into account their increasing convergence; and, second, in the formulation of legal problems that need to be resolved due to the potential emergence of new types of entities with cognitive functions and capable of having a targeted intellectual impact on the environment and legal entities.

Practical significance: it is present in the answers given to the formulated legal questions, which contain suggestions and recommendations on the necessary adjustment of legal regulation and focus the attention of legal scholars on the problems arising from the pace and vectors of science-consuming technologies' development.

For citation

Filipova, I. A. (2024). Intelligent Robots, Cyborgs, Genetically Enhanced Individuals, Chimeras: the Future and the Challenges of Law. *Journal of Digital Technologies and Law, 2*(4), 741–781. https://doi.org/10.21202/jdtl.2024.38

References

Abrosimov, V. (2022). Rights, duties, obligations and restrictions of an autonomous robot in a cyber-physical group. *Legal Informatics*, *4*, 67–75. (In Russ.). https://doi.org/10.21681/1994-1404-2022-4-67-75

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society*, *13*(1), 25–35. https://doi.org/10.1093/cjres/rsz022

Almeida, M., & Diogo, R. (2019). Human enhancement: Genetic engineering and evolution. *Evolution, Medicine, and Public Health*, *1*, 183–189. https://doi.org/10.1093/emph/eoz026

Benton, M. L., Abraham, A., LaBella, A. L., Abbot, P., Rokas, A., & Capra, J. A. (2021). The influence of evolutionary history on human health and disease. *Nature Reviews Genetics*, *22*, 269–283. https://doi.org/10.1038/s41576-020-00305-9

Berg, L. N. (2024). Genomic Data Privacy and the Right to Science: Issues of Balance. *Lex Russica*, *77*(10), 93–101. (In Russ.). https://doi.org/10.17803/1729-5920.2024.215.10.093-101

Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Frontiers in Robotics and AI*, *9*, 842213. https://doi.org/10.3389/frobt.2022.842213

Brown, J. L., Voth, J. P., Person, K., & Low, W. C. (2023). A Technological and Regulatory Review on Human-Animal Chimera Research: The Current Landscape of Biology, Law, and Public Opinion. *Cell Transplantation*, *32*. https://doi.org/10.1177/09636897231183112

Burgess, P. (2024). *AI and the Rule of Law: The Necessary Evolution of a Concept*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509963201

Chiriatti, M., Ganapini, M., Panai, E., Ubiali, M., & Riva, G. (2024). The case for human – AI interaction as system 0 thinking. *Nature Human Behaviour*, *8*, 1829–1830. https://doi.org/10.1038/s41562-024-01995-5

Citra, N. Z. M., Chew, W. L., & Lai, P. S. (2024). Embryo and fetal gene editing: Technical challenges and progress toward clinical applications. Molecular Therapy. *Methods & Clinical Development*, *3*(2), 101229. https://doi.org/10.1016/j.omtm.2024.101229

Collingridge, D. (1982). *The social control of technology*. Palgrave Macmillan.

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*, 1330439. https://doi.org/10.3389/fpsyg.2024.1330439

Czomartova, F. V., Pomazanskij, A. E., Nikitina, E. E., Nanba, S. B., Melnik, T. E., & Khromova, N. M. (2021). *Law and biomedicine*. Moscow: Norma; INFRA-M. (In Russ.).

Das, S., Banerjee, J. S., De, D., Sarigiannidis, P., Chakraborty, A., Mahmud, M., & Bhattacharyya, S. (2024). Role of the Social Internet of Things in Society 5.0: Opportunities and Challenges. In S. Bhattacharyya, J. S. Banerjee, & M. Köppen (Eds.), *Smart innovation, systems and technologies* (pp. 667–686). Springer, Singapore. https://doi.org/10.1007/978-981-99-7711-6_52

de Andrés-Sánchez, J., Arias-Oliva, M., Souto-Romero, M., & Gené-Albesa, J. (2024). Assessing the Acceptance of Cyborg Technology with a Hedonic Technology Acceptance Model. *Computers*, *13*(3), 82. https://doi.org/10.3390/computers13030082

Döring, N., Mohseni, M. R., & Walter, R. (2020). Design, Use, and Effects of Sex Dolls and Sex Robots: Scoping Review. *Journal of Medical Internet Research*, *22*(7), e18551. https://doi.org/10.2196/18551

Emelin, V. A. (2013). Cyborgization and invalidization of a technologically expanded human. *National Psychological Journal*, *1*(9), 62–70. (In Russ.).

Filipova, I. A. (2024). Artificial intelligence, robot and neurotechnologies: concepts, relationship and limits of legal regulation. *State and Law*, *4*, 148–158. (In Russ.). https://doi.org/10.31857/S1026945224040133

Fontes, C., Carpentras, D., & Mahajan, S. (2024). Human digital twins unlocking Society 5.0? Approaches, emerging risks and disruptions. *Ethics and Information Technology*, *26*, 54. https://doi.org/10.1007/s10676-024-09787-1

Fuchs, Th., Aszmann, O., & Dürr, O. (2024). Organisms, Prostheses and the Limits of Cyborgization. *Philosophy, Theology and the Sciences*, *11*(2), 208–226 https://doi.org/10.1628/ptsc-2024-0016

Gibney, E. (2024, May 28). The AI revolution is coming to robots: how will it change them? *Nature*. https://doi.org/10.1038/d41586-024-01442-5

Ginevičienė, V., Utkus, A., Pranckevičienė, E., Semenova, E. A., Hall, E. C., & Ahmetov, I. I. (2022). Perspectives in Sports Genomics. *Biomedicines*, *10*(2), 298. https://doi.org/10.3390/biomedicines10020298

Goldstein, J. M., Tabebordbar, M., Zhu, K., Wang, L. D., Messemer, K. A., Peacker, B., Kakhki, S. A., Gonzalez-Celeiro, M., Shwartz, Yu., Cheng, J. K. W., Xiao, R., Barungi, T., Albright, Ch., Hsu, Y.-Ch., Vandenberghe, L. H., & Wagers, A. J. (2019). In Situ Modification of Tissue Stem and Progenitor Cell Genomes. *Cell Reports*, *27*(4), 1254–1264. https://doi.org/10.1016/j.celrep.2019.03.105

Grinin, L. E., & Grinin, A. L. (2016). Will cybernetic revolution lead to cyborgization of humans? *Philosophy and society*, *3*(80), 5–26. (In Russ.).

Gulino, M., Kim, D., Pané, S., Santos, S. D., & Pêgo, A. P. (2019). Tissue Response to Neural Implants: The Use of Model Systems Toward New Design Solutions of Implantable Microelectrodes. *Frontiers in Neuroscience*, *13*, 689. https://doi.org/10.3389/fnins.2019.00689

Gumuskaya, G., Srivastava, P., Cooper, B. G., Lesser, H., Semegran, B., Garnier, S., & Levin, M. (2024). Motile Living Biobots Self-Construct from Adult Human Somatic Progenitor Seed Cells. *Advanced Science*, *11*(4), e2303575. https://doi.org/10.1002/advs.202303575

Hanson, K. R., & Locatelli, C. C. (2022). From Sex Dolls to Sex Robots and Beyond: A Narrative Review of Theoretical and Empirical Research on Human-like and Personified Sex Tech. *Current Sexual Health Reports*, *14*, 106–117. https://doi.org/10.1007/s11930-022-00331-0

Helbing, D., & Ienca, M. (2024). Why converging technologies need converging international regulation. *Ethics and Information Technology*, *26*, 15. https://doi.org/10.1007/s10676-024-09756-8

Ireni-Saban, L., & Sherman, M. (2022). Cyborg ethics and regulation: ethical issues of human enhancement. *Science and Public Policy*, *49*(1), 42–53. https://doi.org/10.1093/scipol/scab058

Jiang, P., & Alam, M. M. (2022). Rise of the human-mouse chimeric brain models. *Cell Regeneration*, *11*, 32. https://doi.org/10.1186/s13619-022-00135-6

Kadlecová, J. (2020). Body-hacking: On the Relationship between People and Material Entities in the Practice of Technological Body Modifications. *Historická Sociologie*, *12*(1)49–63. https://doi.org/10.14712/23363525.2020.4

Kamalova, G. G. (2021). Theoretical and legal aspects of the evolution of human rights in the context of digitalization and the introduction of artificial intelligence technology. Bulletin of Udmurt University. *Series Economics and Law*, *31*(4), 662–668. (In Russ.). https://doi.org/10.35634/2412-9593-2021-31-4-662-668

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*(1), 93–115. https://doi.org/10.1007/s10506-021-09289-1

Khandelwal, A., Agrawal, A., Bhattacharyya, A., Singla, Y. K., Singh, S., Bhattacharya, U., Dasgupta, I., Petrangeli, S., Shah, R. R., Chen, Ch., & Krishnamurthy, B. (2024). Large Content and Behavior Models to Understand, Simulate, And Optimize Content and Behavior. *The Twelfth International Conference on Learning Representations, ICLR*, Vienna. arXiv:2309.00359v4. https://doi.org/10.48550/arXiv.2309.00359

Kriegman, S., Blackiston, D., Levin, M., & Bongard, J. (2021). Kinematic self-replication in reconfigurable organisms. *Proceedings of the National Academy of Sciences*, *118*(49), e2112672118. https://doi.org/10.1073/pnas.2112672118

Księżak, P. (2024). *Artificial Intelligence and the Dawn of Cyborg Law. Key Legal Challenges for Private Law in the Era of Human Augmentation*. Warszawa: Allerhand Publishing.

Laurent, M., Geoffroy, M., Pavani, G., & Guiraud, S. (2024). CRISPR-Based Gene Therapies: From Preclinical to Clinical Treatments. *Cells*, *13*(10), 800. https://doi.org/10.3390/cells13100800

Lima, P. U., & Paiva, A. (2024). Autonomous and Intelligent Robots: Social, Legal and Ethical Issues. In H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. Martins Pereira, E. Vaz de Sequeira, & L. Barreto Xavier (Eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law. Law, Governance and Technology Series* (pp. 127–140). Cham, Switzerland. https://doi.org/10.1007/978-3-031-41264-6_7

Liu, Z., Cai, Y., Wang, Y., Nie, Y., Zhang, C., Xu, Y., Zhang, X., Lu, Y., Wang, Z., Poo, M., & Sun, Q. (2018). Cloning of Macaque Monkeys by Somatic Cell Nuclear Transfer. *Cell*, *172*(4), 881–887. https://doi.org/10.1016/j.cell.2018.01.020

Lloyd, N., Chowdhry, A., & Lewis, P. R. (2024). Trustworthy Embodied Virtual Agents. In N. Lee (Eds.), *Encyclopedia of Computer Graphics and Games* (pp. 1917–1922). Springer, Cham. https://doi.org/10.1007/978-3-031-23161-2_524

Lorimer, J. (2009). Posthumanism/Posthumanistic Geographies. In R. Kitchin, & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 344–354). Oxford: Elsevier. https://doi.org/10.1016/b978-008044910-4.00723-9

Mestre, R., Astobiza, A. M., Webster-Wood, V. A., & Saif, M. T. A. (2024). Ethics and responsibility in biohybrid robotics research. *Proceedings of the National Academy of Sciences*, *121*(31), e2310458121. https://doi.org/10.1073/pnas.2310458121

Mocanu, D. M. (2021). Gradient Legal Personhood for AI Systems – Painting Continental Legal Shapes Made to Fit Analytical Molds. *Frontiers in Robotics and AI*, *8*, 788179. https://doi.org/10.3389/frobt.2021.788179

Momaya, A., Fawal, M., & Estes, R. (2015). Performance-Enhancing Substances in Sports: A Review of the Literature. *Sports Medicine*, *45*, 517–531. https://doi.org/10.1007/s40279-015-0308-9

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The Uncanny Valley. *IEEE Robotics & Automation Magazine*, *19*(2), 98–100. https://doi.org/10.1109/MRA.2012.2192811

Morshedzadeh, F., Ghanei, M., Lotfi, M., Ghasemi, M., Ahmadi, M., Najari-Hanjani, P., Sharif, S., Mozaffari-Jovin, S., Peymani, M., & Abbaszadegan, M. R. (2024). An Update on the Application of CRISPR Technology in Clinical Practice. *Molecular Biotechnology*, *66*(2), 179–197. https://doi.org/10.1007/s12033-023-00724-z

Nolfi, S. (2024). On the Unexpected Abilities of Large Language Models. *Adaptive Behavior*, *32*(6), 493–502. https://doi.org/10.1177/10597123241256754

Olarte-Pascual, C., Pelegrín-Borondo, J., Reinares-Lara, E., & Arias-Oliva, M. (2021). From wearable to insideable: Is ethical judgment key to the acceptance of human capacity-enhancing intelligent technologies? *Computers in Human Behavior*, *114*, 106559. https://doi.org/10.1016/j.chb.2020.106559

Palmerini, E., Bertolini, A., Battaglia, F., Koops, B.-J., Carnevale, A., & Salvini, P. (2016). RoboLaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*, *86*, 78–85. https://doi.org/10.1016/j.robot.2016.08.026

Perez, E. (2022). Future of Therapy for Inborn Errors of Immunity. *Clinical Reviews in Allergy & Immunology*, *63*(1), 75–89. https://doi.org/10.1007/s12016-021-08916-8

Pluchino, S., & Lombardi, I. (2024). Crossing species boundaries in regenerative neuroscience with rat–mouse brain chimeras. *Lab Animal*, *53*, 179–180. https://doi.org/10.1038/s41684-024-01394-3

Ponce del Castillo, A. (2024). *Artificial intelligence, labour and society*. Brussels: ETUI.

Popova, O. V. (2015). Ethical issues of biotechnological human design. *RUDN Journal of Philosophy*, *2*, 107–114. (In Russ.).

Przhilenskiy, V. I. (2024). Bioethics: Epistemic Capabilities and Legal Frameworks. *Kutafin Law Review*, *11*(2), 180–198. https://doi.org/10.17803/2713-0533.2024.2.28.180-198

Reichel, P., Bassler, C. T., & Spörrle, M. (2024). Embracing the enhanced self now and in the future: The impact of temporal focus, age, and sex on cyborg products use intention. *Personality and Individual Differences*, *225*, 112665. https://doi.org/10.1016/j.paid.2024.112665

Roco, M. C., & Bainbridge, W. S. (2003). *Converging Technologies for Improving Human Performance. Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. Dordrecht: Springer. https://doi.org/10.1007/978-94-017-0359-8

Sandini, G., Sciutti, A., & Morasso, P. (2024). Artificial cognition vs. artificial intelligence for next-generation autonomous robotic agents. *Frontiers in Computational Neuroscience*, *18*, 1349408. https://doi.org/10.3389/fncom.2024.1349408

Sharon, A., Jankowski, M. M., Shmoel, N., Erez, H., & Spira, M. E. (2023). Significantly reduced inflammatory foreign-body-response to neuroimplants and improved recording performance in young compared to adult rats. *Acta Biomaterialia*, *158*, 292–307. https://doi.org/10.1016/j.actbio.2023.01.002

Sokolova, M. (2022). Cyborgization of human: social and legal dimensions. *Social novelties and social sciences*, *4*, 52–64. (In Russ.).

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Tan, T., Wu, J., Si, C., Dai, S., Zhang, Y., Sun, N., Zhang, E., Shao, H., Si, W., Yang, P., Wang, H., Chen, Z., Zhu, R., Kang, Y., Hernandez-Benitez, R., Martinez Martinez, L., Nuñez Delicado, E., Berggren, W. T., Schwarz, M., … & Izpisua Belmonte, J. C. (2021). Chimeric contribution of human extended pluripotent stem cells to monkey embryos ex vivo. *Cell*, *184*(13), 3589. https://doi.org/10.1016/j.cell.2021.06.011

Umnova-Konyukhova, I. A., & Aleshkova, I. A. (2022). The Impact of Scientific and Technological Progress in Biotechnology on Human Rights and Principles of Law. *Actual Problems of Russian Law*, *17*(10), 34–45. (In Russ.). https://doi.org/10.17803/1994-1471.2022.143.10.034-045

Vaughn, L. (2023). *Bioethics: Principles, Issues, and Cases* (5th ed.). Oxford University Press.

Veit, W. (2018). Procreative Beneficence and Genetic Enhancement. *Kriterion – Journal of Philosophy*, *32*(1), 75–92. https://doi.org/10.1515/krt-2018-320105

Viljanen, M. (2017). A Cyborg Turn in Law? *German Law Journal*, *18*(5), 1277–1308. https://doi.org/10.1017/S2071832200022331

Wajnerman, A., & López-Silva, P. (2022). Mental Privacy and Neuroprotection: An Open Debate. In P. López-Silva, & L. Valera (Eds.), *Protecting the Mind. Challenges in Law, Neuroprotection, and Neurorights* (pp. 141–155). Cham, Switzerland. https://doi.org/10.1007/978-3-030-94032-4_12

Yumartov, D. A. (2021). Inclusiveness as key principle of posthumanism. *Gumanitarnyye vedomosti TGPU im. L. N. Tolstogo*, *40*(4), 109–122. (In Russ.). https://doi.org/10.22405/2304-4772-2021-1-4-109-122

Zhang, H., Xuan, Z., Yu, F., Ding, X., & Han Y. (2024). Crafting the modern Prometheus: navigating morality and identity in the age of cyborg enhancements. *Philosophical Psychology*, 1–34. https://doi.org/10.1080/09515089.2024.2382297

Author information



Irina A. Filipova – Cand. Sci. (Law), Associate Professor, Department of Labor and Environmental Law, National Research Lobachevsky State University of Nizhni Novgorod; Head of the Central Asia Research Center for artificial intelligence regulation, Samarkand State University named after Sharof Rashidov
Address: 23 prospekt Gagarina, 603922 Nizhniy Novgorod, Russia; 15 Universitetskiy bulvar, 140104 Samarkand, Uzbekistan
E-mail: irinafilipova@yandex.ru
ORCID ID: https://orcid.org/0000-0003-1773-5268
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57327205000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/R-1375-2016
Google Scholar ID: https://scholar.google.com/citations?user=opJc7fcAAAAJ
RSCI Author ID: https://elibrary.ru/author_profile.asp?authorid=461586

Conflict of interest

The author is a Deputy Editor-in-Chief 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 – November 11, 2024
Date of approval – November 25, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:342.1:004
EDN: https://elibrary.ru/bbsqnh
DOI: https://doi.org/10.21202/jdtl.2024.39

Правовые аспекты концепции киберинтересов государств через призму теории законных интересов

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре, Луксор, Египет
Лидский университет Беккета, Лидс, Великобритания

Ключевые слова

государственные интересы,
кибердипломатия,
киберинтересы,
киберпространство,
международная судебная практика,
национальные интересы,
теория законных интересов,
права человека,
уголовное право,
цифровые технологии

Аннотация

Цель: показать эволюцию концепции государственных интересов и ее применение в киберпространстве, где она оказывается основополагающей для разработки государственной политики, направленной на защиту национальных интересов.

Методы: исследование базируется на пересечении теории права и концепции киберинтересов государства через призму теории законных интересов (Rechtsgutstheorie), изначально разработанной в рамках уголовно-правовой науки, но имеющей перспективы для изучения концепции государственных интересов в киберпространстве. Применение теории законных интересов позволило изучить понятие киберинтересов государства и определить его правовую классификацию, а также приложения к концепции государственных интересов в киберпространстве. В частности, теория законных интересов в настоящем исследовании используется для изучения правовых перспектив концепции государственных интересов в киберпространстве как интересов, подлежащих правовой защите.

Результаты: определено, что в динамичном ландшафте киберпространства существуют многогранные интересы государств, связанные с национальной безопасностью, экономическим процветанием, суверенитетом и дипломатией, для обеспечения защиты которых государства инициируют стратегии, которые порождают разнообразные политико-правовые последствия в международных отношениях. Этим фактом определяется важность изучения концепции государственных интересов с юридической точки зрения, равно как и их правового статуса и последствий. Проведены параллели между концепцией охраняемых правовых интересов в рамках теории законных интересов и киберинтересами, которые государства стремятся защитить. Рассмотрена применимость требования этой теории о балансе конкурирующих интересов к действиям государства в киберпространстве.

© Абделькарим Я. 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.

Выявлены препятствия применения теории законных интересов к киберпространству, включая трудности атрибуции, пороговые значения ущерба и необходимость глобального консенсуса. Показана эволюция концепции государственных интересов, что обусловливает возможность ее применения в киберпространстве, где она служит целям разработки государственной политики, направленной на защиту национальных интересов.

Научная новизна: выражается в представленном в статье преломлении теории законных интересов к формированию правовой концепции киберинтересов государства, что служит достаточным обоснованием защиты конкретных киберинтересов.

Практическая значимость: основные выводы, изложенные в статье, могут быть использованы для выявления киберпространственных интересов, подлежащих правовой защите (таких как конфиденциальность, целостность данных, суверенитет и экономическая стабильность), совершенствования правовых механизмов защиты национальных интересов в киберпространстве, обеспечения единообразия релевантной международной судебной практики, повышения эффективности и качества управления политикой государств в киберпространстве с целью обеспечения безопасности и мирного сосуществования.

Для цитирования

Абделькарим, Я. А. (2024). Правовые аспекты концепции киберинтересов государств через призму теории законных интересов. *Journal of Digital Technologies and Law*, *2*(4), 782–801. https://doi.org/10.21202/jdtl.2024.39

Содержание

Введение
1. Эволюция концепции интересов государства в цифровой сфере
   1.1. Традиционное понимание концепции
   1.2. Новая реальность в киберэпоху
2. Теория законных интересов
   2.1. Основные положения теории законных интересов
   2.2. Вклад теории в развитие правовых систем
3. Интересы государства в киберпространстве как охраняемые законом интересы
   3.1. Применимость теории законных интересов в киберпространстве
   3.2. Приложение теории законных интересов к концепции киберпространственных интересов государства
Заключение
Список литературы

Введение

Среди факторов, определяющих успех государства, выделяется способность удовлетворять и обеспечивать важнейшие потребности, необходимые для благосостояния и процветания граждан, а также функциональность сильных сторон государства

в международном сообществе. В совокупности эти факторы составляют концепцию интересов государства. В политической сфере можно заметить, что интересы являются импульсом для продвижения национальных стратегий и политики, которые влияют на международные отношения. Они представляют собой главную ось международных отношений, что указывает на важность этой концепции с политической точки зрения. Тем не менее, на первый взгляд, влияние этой концепции в политике никогда не затмит истинные правовые аспекты, которые следует изучить. При изучении влияния концепции киберинтересов государства на их классификацию и правовые последствия можно поставить несколько юридических вопросов.

Неизбежная синергия между политикой и правом в отношении концепции киберинтересов государства заставляет исследователей выбрать определенную правовую теорию для изучения этой концепции с ее точки зрения. Поиск в отраслях права показал, что уголовное право обладает адекватными теориями и понятиями для выполнения исследовательской задачи. Теория охраняемых правовых интересов (далее – Rechtsgutstheorie, теория законных интересов, ТЗИ), разработанная немецкими учеными, позволяет изучить понятие киберинтересов государства и определить его правовую классификацию, а также его приложения в рамках конкретной правовой теории. Широкая нормативная база уголовного права наряду с его гибкой применимостью побуждает исследователей выбирать теорию уголовного права для ответа на поставленный вопрос, в анализ и определение которого вносит свой вклад ТЗИ. Кроме того, в литературе отмечается, что эта теория эффективна для решения уголовно-правовых вопросов, несмотря на критику со стороны научного сообщества, касающуюся ее возникновения в отдельной стране. Таким образом, в настоящем исследовании данная теория используется для изучения правовых перспектив концепции государственных интересов в киберпространстве как интересов, подлежащих правовой защите.

1. Эволюция концепции интересов государства в цифровой сфере

Заметное расхождение в природе и контексте между реальным миром и киберпространством влияет на точку зрения, с которой рассматривается концепция государственных интересов. В прежних традиционных исследованиях основное внимание уделялось объяснению и интерпретации этой концепции с акцентом на реальные характеристики понятия интересов; теперь же, в цифровой сфере киберпространства, несомненно, можно заметить влияние преобладающей технологической повестки на различные аспекты этой концепции. Таким образом, в нашем исследовании мы разделяем соответствующие источники по концепции государственных интересов на работы в рамках традиционной доктрины, фокусирующейся на понимании этой концепции в реальном мире, и на современную литературу по влиянию кибернетики на концепцию интересов.

1.1. Традиционное понимание концепции

Концепция интересов была создана для выражения цели основных гуманитарных устремлений, направленных на достижение преимуществ и предотвращение жертв. В работе Wang (2022) объясняется, что человеческие потребности, желания и чаяния являются движущей силой существования интересов и их удовлетворение

необходимо для сохранения целостности человека. Для поддержания и улучшения человеческой жизнедеятельности решающее значение имеет удовлетворение основных потребностей. Однако, по сути, удовлетворение потребностей предполагает получение желаемого с помощью определенных методов, в то время как необходимость проявлять психологическую мотивацию для достижения интересов в реальности отражает попытки удовлетворить эти потребности с помощью механизмов взаимодействия между людьми, например, производства, торговли и дипломатии (Wang, 2022). Кроме того, индивидуальные интересы выступают в качестве стимулов для наилучшего использования человеком имеющихся ресурсов для получения выгод (Thomas, 2023); фрагментация интересов вносит решающий вклад в достижение глобального благосостояния и процветания. Являясь связующим звеном между потребностями и средствами, интерес представляет слияние человеческих потребностей и методов их удовлетворения. Кроме того, интересы имеют социальный аспект, который демонстрирует тесные отношения между государством и его гражданами.

Что касается государств, их интересы как социальное явление относятся к общенациональным требованиям, которые удовлетворяют внутренние потребности, часто противоречащие интересам других государств (Abdelkarim, 2024). Термин «национальные интересы» может быть не вполне ясным, поскольку его толкование варьируется в зависимости от контекста. Государственные деятели и политики используют его для оправдания своих действий и обоснования своих взглядов. Так как государства различаются в определении своих интересов, возникают конфликты интересов, при которых государства используют различные инструменты для защиты своих интересов (Thomas, 2023; Topor, 2024). Следовательно, интересы определяют поведение государства на международной арене, обеспечивая удовлетворение его потребностей. Поскольку интересы государства формируются на основе единой группы человеческих потребностей, они представляют собой общую национальную цель (Wang, 2022). Эта особенность государственных интересов определяется схожестью фундаментальных потребностей конкретной социальной группы. Кроме того, общие интересы публично проявляются в рамках конкретных социальных отношений, и значение этой публичности варьируется в зависимости от различных социальных отношений и интересов (Wang, 2022). Это может относиться к общему содержанию интересов субъектов этих отношений. Ярким примером общих интересов является социальная потребность во внешней безопасности. Отмечая вклад интересов в мировую стабильность, Onditi (2023) назвал их главным инструментом, определяющим формы глобальной межгосударственной дипломатии и методы разрешения конфликтов. Поддержание национальных интересов является истинной целью дипломатии и истинной причиной серьезных различий, наблюдаемых среди государств в этом аспекте.

Wang (2022), кроме того, утверждал, что общие интересы возникают внутри социальной группы. Единство общих интересов подразумевает, что в рамках определенных отношений, связанных с интересами, общие интересы, как правило, уникальны. Это единство общих интересов формирует основу для государственной политической власти в определенных рамках и основывается на конкретных отношениях интересов в социальной и политической жизни. Важно отметить, что, хотя общие интересы различны в рамках конкретного общества и во взаимосвязи интересов, это не исключает возможности того, что эти конкретные общие интересы отражают различные аспекты фактического содержания и ценностей.

Интересы государств представляют собой взаимосвязанную группу потребностей и целей, которые национальные правительства стремятся удовлетворить с помощью ряда методов, таких как дипломатия и правовые или вооруженные конфликты. Согласно Metea (2020), чтобы считаться национальными, интересы должны быть широкими, выходить за рамки узких контекстов и демонстрировать устойчивость к изменениям в результате временных сдвигов. Таким образом, национальные интересы возникают в результате сложного взаимодействия устойчивых, широко применимых проблем, обеспечивающих стабильность и успех страны, удовлетворение которых отражает силу данного государства и уровень влияния, который оно должно поддерживать или приобретать на международной арене для защиты национальных интересов. В то же время Cox (2021) утверждал, что интересы стали занимать центральное место в социальных науках благодаря их роли в формировании коллективных эмоций внутри сообщества. Следовательно, интересы представляют собой коллективную мотивацию группы, побуждающую власти страны принимать защитные меры.

Несмотря на неоднозначность этого понятия, известный американский политик Сэмюель Хантингтон определяет национальные интересы как «общественное благо, которое касается каждого или большинства граждан; жизненно важный национальный интерес – это тот интерес, ради которого они готовы проливать свою кровь и тратить свои богатства на его защиту. Национальные интересы обычно сочетают безопасность и материальные соображения, с одной стороны, и морально-этические соображения – с другой» (Huntington, 1997; Metea, 2020). Согласно работе McLean и McMillan (2009), концепция национальных интересов охватывает различные аспекты и служит важной основой как для политического дискурса, так и для анализа внешней политики. В первом случае политики активно используют эту концепцию для получения поддержки своих действий. Во внутренней политике возможности этой концепции ограничены из-за разнообразия мнений. В любом случае во внешней политике благодаря этой концепции складывается образ нации, защищающей свои интересы в анархической международной системе. Это стандартный метод определения силы государства в международном сообществе (Thomas, 2023).

1.2. Новая реальность в киберэпоху

Появление киберпространства вызвало бурные дебаты об определении его влияния на взаимодействие людей и потенциальной возможности внесения изменений в сферу международных отношений (Foulon & Meibauer, 2024). Являясь универсальной либеральной областью взаимодействия с открытым доступом, киберпространство дает благоприятные условия для увеличения и распространения различных преимуществ среди пользователей (Thomas, 2023). Таким образом, в виде потоков данных в Интернете генерируются десятки различных интересов, усложняя природу и суть человеческих взаимодействий.

По мере расширения кибернетических возможностей и логики киберпространства меняются и способы взаимодействия государств в рамках международной системы, учитывающие влияние свободы в киберпространстве (Thomas, 2023). В отличие от прежних технологий, таких как телеграф, которые просто ускоряли коммуникацию, киберпространство обеспечивает прямое и немедленное

взаимодействие между правительствами и населением других стран. Такой широкий доступ к киберпространству действует как распределенная возможность, но не меняет фундаментальных принципов деятельности государств, которые по-прежнему основаны на анархии и распределении материальной власти. Универсальность киберпространства, в частности, его мощные возможности и уникальная структура, обеспечивающая неограниченность ресурсов, вывели последствия взаимодействия людей в нем на космополитический уровень, т. е. за рамки двусторонних взаимодействий. Действительно, на материальные и идеологические аспекты киберпространства влияют такие факторы, как стратегическая культура и доступность ресурсов, а используются эти аспекты по-разному и влияют на одних участников в большей степени, чем на других. Этот неравный контроль делает киберпространство более выгодным для одних участников по сравнению с другими. Таким образом, в сфере международных отношений появилась кибердипломатия как растущая международная практика, направленная на создание кибермеждународного сообщества, гармонизирующего национальные интересы государств с динамикой глобального сообщества (Topor, 2024).

Главными действующими лицами на международной арене являются государства, и действуют они в соответствии со своими национальными интересами. Они преследуют эти интересы с помощью анархической схемы, основанной на геополитической мощи и технологическом превосходстве государства (Foulon & Meibauer, 2024), которые являются ключевыми факторами, определяющими поведение государств в киберпространстве. Широкая доступность данных в киберпространстве формирует структурный фактор, влияющий на международные отношения из-за абсолютного технологического превосходства, используемого для контроля над данными в Интернете (Foulon & Meibauer, 2024). Это придает концепции государственных интересов новое измерение, определяемое кибернетическими характеристиками. Более того, киберпространство влияет на восприятие структурных факторов, подобно тому, как ядерное оружие не изменило основную логику поведения государства, но изменило восприятие угроз и возможностей. Следовательно, киберпространство влияет на динамику международных отношений, формируя ограничения, стимулы и поведение государств. В контексте киберпространства это означает, что каждое государство будет действовать для удовлетворения своих национальных потребностей в режиме реального времени, а поведение в киберпространстве будет определяться этими интересами (Abdelkarim, 2024). Таким образом, реальность демонстрирует критическое влияние концепции киберинтересов государств на разработку межгосударственной политики и международных отношений. Более того, национальные интересы являются стимулом для вмешательства государств и разработки своей политики в киберпространстве (Topor, 2024). Изучение подходов различных государств демонстрирует их поспешные попытки консолидировать власть в соответствии с национальными интересами для защиты своей критически важной инфраструктуры, такой как электросети, финансовые системы и коммуникационные сети, от кибератак, а также для достижения экономических преимуществ за счет имеющихся возможностей в цифровой среде.

Следует отметить, что наличие мощных технологических возможностей не является обязательным условием для того, чтобы государство преследовало

свои интересы в киберпространстве, поскольку для достижения эффекта не требуется ничего, кроме простых инструментов доступа в Интернет. Это представляет большую опасность для национальных интересов в киберпространстве, поскольку самый слабый пользователь Интернета может нанести серьезный ущерб интересам государства (Abdelkarim, 2024). Таким образом, защита целостности национальных интересов подразумевает признание их кибернетической составляющей, чтобы государство могло использовать наиболее релевантные методы их поддержания. Более того, интересы государства в первую очередь стимулируют приоритетность национальных интересов в киберпространстве (Cox, 2021). Когда киберинститутам государства угрожает опасность, вмешательство государства становится необходимым для защиты целостности национального благосостояния. Это согласуется с фундаментальными принципами суверенитета и защиты национальных интересов в киберпространстве. Кроме того, угрозы государственным интересам в киберпространстве могут привести к кибервойне, характеризующейся взаимными кибератаками через государственные границы для защиты национальных экономических и военных активов (Fang, 2018). Такие угрозы требуют незамедлительного реагирования государства для защиты национальных интересов.

Управление по вопросам подотчетности правительства США в своем официальном отчете подчеркнуло настоятельную необходимость разработки национальной стратегии кибердипломатии для защиты интересов государства в киберпространстве[1]. Этот отчет ознаменовал официальное признание правительством США концепции государственных киберинтересов и ее использование для формирования национальной кибердипломатии. В результате понятие государственного интереса в киберпространстве в настоящее время прочно утвердилось на политической и дипломатической аренах для решения проблем и защиты национальных интересов. Abdelkarim (2024) подтверждает этот вывод, отметив, что понятие государственных интересов в киберпространстве эволюционировало и стало основой государственной киберполитики. Гибкость основных принципов этой концепции, касающихся взаимодействия в киберпространстве, позволяет ей стать определяющим фактором государственной власти в киберпространстве. В том же контексте Reiterer (2022) утверждает, что интересы государства в киберпространстве должны быть основой кибердипломатии для защиты национальной целостности в киберпространстве. Он отмечает, что продолжающееся развитие киберугроз заставляет сосредоточить усилия на внедрении новейших технологий в рамках национальных стратегий противодействия этим угрозам. По мнению того же автора, общие интересы в киберпространстве, например, защита критически важной инфраструктуры и другие проблемы национальной безопасности стали основой многостороннего сотрудничества между Европейским союзом и другими международными партнерами, несмотря на различные национальные интересы отдельных государств (Reiterer, 2022). Таким образом, тесная связь между кибердипломатией и концепцией интересов неоспорима.

[1] US Government Accountability Office. (2024, January). Cyber Diplomacy. State's Efforts Aim to Support U.S. Interests and Elevate Priorities: Report to Congressional Addressees. https://clck.ru/3A7Y99

2. Теория законных интересов

2.1. Основные положения теории законных интересов

Зародившись в рамках немецкой криминологии, теория законных интересов представляет собой подробное аналитическое описание интересов человека, которые должны защищаться правовыми нормами во всей правовой системе по всему миру (Atadjanov, 2019) независимо от национальной принадлежности. Традиционно ТЗИ применяется к любым интересам или ценностям, признанным национальным законодательством. Следовательно, законные интересы являются основанием для криминализации нарушений их защищенного статуса. Таким образом, акт, затрагивающий этот статус, должен быть рассмотрен в рамках ТЗИ, чтобы определить, какие ответные меры следует предпринять для поддержания целостности законных интересов (Atadjanov, 2019; Tianyang, 2024), что дает законодателям функциональное нормативное применение ТЗИ. Это дало основание Atadjanov (2019) обосновать появление ТЗИ в немецкой криминологии доктриной, которая рассматривает преступление как нарушение субъективных прав, а не только правовых норм. Аналогичным образом, Ambos (2015) ранее утверждал, что ТЗИ с помощью юридической науки устранила недостатки теории прав, позволив криминализировать нарушения других законных интересов, которые не считаются правами в традиционном смысле. Таким образом, он утверждал, что концепция законных интересов подразумевает необходимые условия и цели для свободного развития личности, реализации ее основных прав и надлежащего функционирования государственных институтов, необходимых для достижения этих целей. Он также настаивал на том, что нормативная точка зрения ТЗИ способствует воплощению в жизнь других правовых принципов, таких как принцип причинения вреда. Тем самым она обосновывает причины процесса криминализации и устанавливает необходимые критерии правовых концепций. Кроме того, адаптируемость ТЗИ и ее сочетаемость с другими правовыми принципами обеспечивает гибкий подход, который способствует преодолению правовой неопределенности и укреплению норм права (Ambos, 2015).

Lanz (2023) показал, что термин «охраняемый законом интерес» имеет два измерения: описательное или нормативное. В описательном смысле это юридические интересы, гарантируемые существующими уголовными законами. С нормативной точки зрения он означает законные интересы, которые, согласно определенным взглядам на уголовную политику, должны защищаться уголовным законодательством. С другой стороны, Tianyang (2024) пришел к выводу, что принцип защищенных законных интересов заложен в самой сути уголовного законодательства. Являясь важнейшим правовым инструментом поддержания общественного порядка и защиты прав граждан, этот принцип является неотъемлемой частью законодательного процесса. Благодаря четкому определению преступных деяний, установлению соответствующих наказаний и адаптации к социальным изменениям уголовное законодательство обеспечивает эффективную реализацию этого принципа. Такой подход не только уважает права личности, но и подчеркивает роль уголовного права в поддержании общественного порядка.

Atadjanov (2019) утверждал, что немецкое понимание теории законных интересов является всеобъемлющим, что оно может быть расширено в качестве нормативного

и включать другие категории интересов, даже те, которые превосходят прогнозы представителей юридической науки и практики. Защищенные законом интересы – это детерминанты, которые направляют политиков и законодателей к подходу, гарантирующему национальные интересы. Таким образом, ТЗИ может вобрать в себя новые концепции и термины, поскольку они дают преимущества определенному государству и, следовательно, отражают фундаментальные ценности и интересы. Согласно Atadjanov, это напрямую вытекает из нормативного аспекта ТЗИ.

Несмотря на это, Wilenmann (2019) раскритиковал немецких ученых за научное местничество и шовинизм. Он охарактеризовал эту теорию как замкнутую в себе и самореферентную, но стремящуюся оказать существенное влияние на глобальные исследования в области уголовного права. По его словам, авторы позиционировали ТЗИ как образец для изучения уголовного права на международном уровне, который часто игнорирует точки зрения других правовых традиций. По сути, эта критика подчеркивает необходимость более глобального и инклюзивного подхода при обсуждении правовых теорий. Atadjanov (2019) многое сделал для введения ТЗИ в англоязычный научный оборот, однако он привел нормативное обоснование этой теории как полезной для юридической практики, тогда как ТЗИ обеспечивает теоретическую основу для понимания концепции законных интересов. В его обзоре подчеркивалось, что простого определения законных интересов недостаточно; необходим поиск обоснования для обеспечения правовой защиты определенных интересов, поскольку без такой нормативной основы весь подход остается скорее теоретическим, чем практическим. Таким образом, соблюдение баланса между нормативными и практическими аспектами ТЗИ является необходимым условием сохранения функциональности этого вклада немецких ученых в теорию права.

2.2. Вклад теории в развитие правовых систем

ТЗИ служит инструментом для распространения официальных правовых мер реагирования на уголовные и неуголовные инциденты с целью обеспечить целостность защищаемых интересов в соответствии с правовыми нормами, что является необходимым условием мирного сосуществования в обществе. Более того, Tianyang (2024) утверждает, что теория защиты прав человека является важнейшей основой для принципа защиты законных интересов. Права человека, включая право на человеческое достоинство, представляют собой ключевую ценность, которую нельзя упускать из виду в любой правовой системе. Являясь важным механизмом ограничения прав граждан, уголовное законодательство должно соответствовать принципу защиты прав человека, чтобы гарантировать, что при борьбе с преступной деятельностью не будут нарушены законные права и интересы граждан (Lanz, 2023; Tianyang, 2024). Проще говоря, придерживаясь принципа защиты законных интересов, необходимо обеспечить, чтобы уголовное законодательство, добиваясь справедливости, наказывало за преступления, но не ущемляло прав и интересов невинных людей. Следует отметить, что упомянутые законные интересы представляют собой интересы, на защиту которых и направлено уголовное законодательство. Они могут быть материальными (например, жизнь, здоровье или собственность) или нематериальными (например, достоинство личности, неприкосновенность частной жизни или свобода), что и составляет суть ТЗИ. Это нормативный аспект ТЗИ, который выходит за рамки простого описания

статус-кво и дает рекомендации по надлежащему образу действий. Кроме того, ТЗИ предлагает конституционную гарантию обеспечения законности судебного разбирательства путем защиты прав и интересов сторон судебного процесса (Olha, 2024). Тем самым становится невозможным лишить какого-либо гражданина интереса или права без явного юридического обоснования. ТЗИ вводит набор нормативно определенных и организационно формализованных методов и средств, обеспечивающих фактическую реализацию прав, свобод и обязанностей отдельных лиц и граждан (Olha, 2024). Кроме того, ТЗИ представляет собой отражение правового сознания общества и осознания справедливости его членами, что повышает надежность и беспристрастность правовой защиты, предоставляемой действующим процессуальным законодательством.

Функциональное приложение ТЗИ позволило государствам, независимо от собственной идеологии (Atadjanov, 2019), разрабатывать уникальные инструменты защиты законных интересов, которые должны опираться на действующие государственные механизмы, такие как законодательство, дипломатия и даже военная сила. В результате скептики критиковали ТЗИ за отсутствие минимального уровня беспристрастности, необходимого для правовых теорий, поскольку некоторые режимы использовали положения ТЗИ для оправдания своей расистской политики, в противоположность естественному общему благу, к которому стремится закон. Однако критика не подорвала прочного правового положения ТЗИ. Ее вклад в развитие уголовного права и защиту основных законных интересов показал Atadjanov (2019). Поскольку защита законных интересов является основополагающим элементом уголовного законодательства, основная ее цель заключается в обеспечении полного уважения и защиты законных прав и интересов каждого гражданина при разработке и применении уголовного законодательства, в том числе иных законодательных актов (Tianyang, 2024). Более того, ТЗИ доказывает свою эффективность в качестве критерия конституционности положений уголовного права, когда они оспариваются в Конституционном суде Германии, поскольку она содержит твердые и рациональные положения для обоснования судебных решений (Ambos, 2015).

Суды внесли значительный вклад в укрепление ТЗИ, поскольку судебное толкование положений уголовного права разъясняет значение и сферу применения принципа защиты законных интересов (Tianyang, 2024). На практике судьи полагаются на эти толкования при решении вопросов защиты законных интересов в конкретных делах, обеспечивая соблюдение данного принципа. Судебные толкования учитывают социальные реалии и потребности судебной системы, обеспечивая углубленный анализ и рекомендации. Это помогает судьям правильно применять данный принцип и дает гражданам четкие юридические рекомендации по защите их прав. Уголовный кодекс, поправки и судебные толкования – все это воплощает указанный принцип в законодательстве и практике. Таким образом, постоянное судебное толкование обеспечивает эффективное применение ТЗИ для поддержания социальной справедливости и стабильности в отношении применения правовых норм.

3. Интересы государства в киберпространстве как охраняемые законом интересы

3.1. Применимость теории законных интересов в киберпространстве

Как указывалось ранее, ТЗИ была создана в Германии как национальная теория, определяющая преступные деяния, которые являлись преступлениями в рамках конкретного сообщества. Работа Atadjanov (2019) доказывает, что немецкие ученые никогда не намеревались использовать эту теорию в международной юридической практике. Таким образом, попытка использовать его для защиты интересов государства в киберпространстве предполагает расширение сферы применения ТЗИ с внутреннего уголовного права на неуголовное международное право, а также на политику и дипломатию.

Использование национальной теории уголовного права для обоснования политики государства по защите национальных интересов в киберпространстве допустимо, поскольку международная правовая практика свидетельствует о принятии международными судами общих принципов права, будь то уголовное или международное право (Atadjanov, 2019), без учета их происхождения. Внедрение общеправовых теорий придает им прочный правовой статус, применимый к нескольким сферам права. Кроме того, непосредственное использование теорий уголовного права, в частности ТЗИ, устраняет законодательный вакуум при рассмотрении новых правовых вопросов, что является естественным вкладом доктрины уголовного права. По мнению Atadjanov (2019), практика международных уголовных трибуналов свидетельствует о том, что они прибегают к основным принципам уголовного права для устранения любых пробелов, препятствующих разрешению судебных споров. Таким образом, ТЗИ, созданная как внутригосударственная немецкая теория, может быть использована для регулирования практики государств в отношении национальных интересов в киберпространстве, которое представляет собой международную виртуальную среду, при условии, что национальное законодательство основано на тех же правовых принципах, что признаны в международном праве. Аналогичным образом, Международный уголовный суд разрешил выносить международные судебные решения на основе национальных правовых принципов, если они согласуются с фундаментальными целями Суда[2]. Определяющим фактором в данном случае является объективное соответствие ценностей между принципом внутреннего законодательства и международным правом.

Другое обоснование кроется в природе самого уголовного права. ТЗИ может быть применена в киберпространстве благодаря экспансивной природе уголовного права; принципы уголовного права носят управленческий характер, что свидетельствует о продолжающемся расширении сферы управления человеческими взаимодействиями (Bidasolo, 2023). Согласно указанному исследованию, юридическая практика показала, что точное и новаторское толкование принципов уголовного права практикующими юристами расширяет их применимость к другим сферам человеческой деятельности, помимо уголовных деяний. Martín de la Cuerda (2023) считает, что расширение принципов уголовного права является прямым следствием доминирующих процессов глобализации в киберпространстве. Эти процессы

[2] ICC, Prosecutor v. Mathleu Ngudjolo Chui, 18 December 2012, ICC-01/04-02/12.

предполагают переосмысление отношения к новым видам деятельности, создающим риски, и использование инструментов мягкого права. По мнению указанного автора, наднациональная экономическая интеграция, эволюция рынка, киберпреступность и транснациональная организованная преступность представляют собой ощутимые социальные риски глобализации. Без этих факторов не возникло бы необходимости криминализировать новые правонарушения или реформировать существующие. Таким образом, применение теории уголовного права к другим аспектам человеческой деятельности согласуется с подходом, который ограничивается соображениями разумности, требованиями необходимости и достижением общей цели удовлетворения потребностей. Поскольку государство может использовать различные инструменты для защиты национальных интересов (Thomas, 2023), теория в рамках уголовного права, т. е. ТЗИ, должна иметь приоритет по сравнению с этими методами, так как она узаконивает меры, принимаемые государством для защиты интересов в киберпространстве.

Так как политика государств в киберпространстве строится с учетом их интересов, ТЗИ повысит стабильность мирового порядка, определяя, когда и как государство должно вмешиваться в цифровую сферу для защиты национальных интересов. В рамках этой задачи ТЗИ придерживается буквального толкования концепции интереса, как это было объяснено Onditi (2023). Ограничивающая роль этой теории в уголовном праве способствует достижению поставленной цели, особенно учитывая отсутствие в международном праве консенсусного механизма, регулирующего этот вопрос (Abdelkarim, 2024). Действительно, различия во взглядах государств на концепцию интересов вызывают юридические трения, связанные с толкованием охраняемых правовых интересов. Достижение единого или, по крайней мере, консенсусного понимания положений ТЗИ среди ученых значительно снижает вероятность возникновения таких трений, учитывая огромный потенциал киберпространственных технологий и неравные возможности государств в киберпространстве. Эта теория отражает естественную космополитическую роль теорий уголовного права.

3.2. Приложение теории законных интересов к концепции киберпространственных интересов государства

Как политическая концепция, интересы способствуют выявлению особенностей и последствий национальных стратегий и политики государств на международной арене (Metea, 2020; Wang, 2022), поскольку они обеспечивают удовлетворение национальных потребностей. Это подразумевает, что для того, чтобы интересы были юридически нормативными, они должны удовлетворять определенному критерию, состоящему из правовых принципов, которые возводят интересы в ранг охраняемых законом. Поскольку ТЗИ представляет собой набор правовых требований, применимых к данному понятию, интересы должны удовлетворять требованиям ТЗИ и пользоваться максимальной правовой защитой, предоставляемой этой теорией.

Из предыдущего объяснения концепции интересов и современного понимания ТЗИ следует, что концепция охраняемого законом интереса состоит из следующих нескольких конкретных элементов:

1) цель – удовлетворить потребность определенной группы,
2) необходимость – важное условие для достижения этой цели,
3) технический результат – добиться желаемого изменения для этой группы.

Следовательно, национальные интересы в киберпространстве должны соответствовать этим принципам, которые должны быть закреплены в ТЗИ как охраняемые законом интересы, тем самым обязывая государственные органы защищать их в этой виртуальной среде. Интересы в киберпространстве должны отвечать конкретным потребностям граждан государства, повышать уровень их жизни, быть необходимыми для достижения непрерывного развития общества, а их воздействие на граждан должно быть позитивным и реалистичным. При соблюдении этих требований национальные интересы в киберпространстве квалифицируются как охраняемые законом интересы, поддержание которых отвечает общим целям теорий уголовного права, касающимся обеспечения мирного сосуществования и безопасности в киберпространстве. Этот подход повторяет логику Atadjanov (2019), который в качестве охраняемого законом интереса в рамках ТЗИ рассматривает человечность, являющуюся философской социальной концепцией, поскольку человечность удовлетворяет определенным требованиям, о которых он упоминает.

Управление политикой государств в киберпространстве с целью обеспечения безопасности и мирного сосуществования – это необходимость, подразумевающая подчинение национальной политики в киберпространстве строгой правовой теории, такой как ТЗИ. Без стремления к достижению этой цели поиск правовой основы для национальной политики, защищающей интересы государств в киберпространстве, становится бессмысленным; эта цель представляет собой логическое обоснование использования национальной теории уголовного права в области политики государств в киберпространстве, учитывая всеобщий научный консенсус в отношении концепции интересов. Общепризнано, что отсутствие норм, регулирующих киберполитику государств, угрожает всеобщему миру и безопасности, поскольку односторонняя политика приводит к межгосударственным конфликтам; это негативное последствие, которого следует избегать. Более того, Atadjanov (2019) утверждал, что очевидная побочная цель имеет решающее значение для применения ТЗИ, поскольку простого описания законного интереса оказывается недостаточно для применения этой теории. Функциональный аспект является доминирующим фактором в этом отношении.

Кроме того, гибкость концепции киберинтересов государства, которая, согласно Abdelkarim (2024), является свойством, отвечающим технической природе киберпространства, позволяет использовать вышеупомянутый механизм для определения их как охраняемых законом интересов в соответствии с ТЗИ, поскольку гибкость в этом контексте способствует применению инструментов юридической логики, таких как индукция, аналогия, анализ и заключение, что позволяет определить применимость правовых теорий к политическим концепциям.

Таким образом, ТЗИ влияет на современное понимание государственных интересов в киберпространстве, поскольку способствует развитию возможностей государств по выявлению киберпространственных интересов, заслуживающих правовой защиты, таких как конфиденциальность, целостность данных, суверенитет и экономическая стабильность, а также способствует разработке политики для обеспечения их целостности. Применение этой теории повышает управляемость киберпространства, превращая его из вакуума беззакония в сферу, где правовые теории оказываются функциональными.

Заключение

Исследование показало, что концепция государственных интересов технически эволюционировала и может применяться в киберпространстве, где она оказывается основополагающей для разработки национальной политики, направленной на защиту национальных интересов. Реалистичность этой концепции выходит за рамки традиционного политического понимания и создает прочную правовую базу. Поскольку односторонние действия могут привести к конфликтам, в исследовании предпринята попытка разработать юридическую теорию для анализа и определения концепции киберинтересов государства. Применение уголовно-правовой теории об охраняемых законом интересах к концепции интересов государства в киберпространстве является эффективным благодаря широкой применимости принципов уголовного права в различных правовых сферах. Соответственно, ТЗИ может внести вклад в формирование концепции государственных интересов в киберпространстве в качестве охраняемых законом интересов. Таким образом, защита национальных интересов в киберпространстве получает всеобъемлющую правовую базу. Это составляет основу правового аспекта концепции государственных интересов.

Подводя итог, можно сказать, что ТЗИ дает возможность проанализировать концепцию государственных интересов в киберпространстве с юридической точки зрения. По мере развития цифровых технологий правовая теория адаптируется, а поиск сбалансированных решений укрепляет верховенство закона в киберпространстве.

Список литературы

Abdelkarim, Y. A. (2024). A Literature Review of the Evolution of Sovereignty and Borders Concepts in Cyberspace. *International Cybersecurity Law Review*, *5*, 365–372. https://doi.org/10.1365/s43439-024-00118-0

Ambos, K. (2015). The Overall Function of International Criminal Law: Striking the Right Balance Between the Rechtsgut and the Harm Principles: A Second Contribution Towards a Consistent Theory of ICL. *Criminal Law and Philosophy*, *9*, 301–329. https://doi.org/10.1007/s11572-013-9266-1

Atadjanov, R. (2019). *Humanness as a Protected Legal Interest of Crimes Against Humanity: Conceptual and Normative Aspects*. TMC Asser Press. https://doi.org/10.1007/978-94-6265-299-6

Bidasolo, M. C. (2023). Is It Possible to Limit the Penal Intervention in the Twenty-First Century? In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 3–16). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_1

Cox, L. (2021). *Nationalism: Themes, Theories, and Controversies*. Palgrave Macmillan. https://doi.org/10.1007/978-981-15-9320-8

de la Cuerda Martín, M. (2023). The Impact of Soft Law on the Expansion of Criminal Law. In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 231–249). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_13

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Foulon, M., & Meibauer, G. (2024). How Cyberspace Affects International Relations: The Promise of Structural Modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Huntington, S. (1997). The Erosion of American National Interests. *Foreign Affairs*, *76*(5), 28–49. https://doi.org/10.2307/20048198

Lanz, J. G. (2023). The Attack on the Protected Legal Interests: A Criminalisation Principle and an Element of the Criminal Offence. *Ius Novem*, *17*(3), 19–31. https://doi.org/10.2478/in-2023-0019

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199207800.001.0001

Metea, I. (2020). National Interest: Terminology and Directions of Approach. In *International Conference Knowledge-Based Organization*, *26*(1), 75–79. https://doi.org/10.2478/kbo-2020-0011

Olha, M. (2024). The Concept of Effectiveness of Ensuring the Rights and Legal Interests of a Person in Pre-trial Criminal Proceedings. *Visegrad Journal on Human Rights*, *1*, 56–63. https://doi.org/10.61345/1339-7915.2024.1.9

Onditi, F. (2023). Introduction: Diplomatic Thought and Practice. In F. Onditi et al. (Eds.), *The Palgrave Handbook of Diplomatic Thought and Practice in the Digital Age* (pp. 1–31). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-28214-0_1

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.), *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges* (pp. 17–39). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Thomas, A. J. (2023). The Open World Ethos. In *The Open World, Hackbacks and Global Justice* (pp. 15–36). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-19-8132-6_2

Tianyang, L. (2024). The Embodiment and Practice of the Principle of Legal Interest Protection in Criminal Legislation. *International Journal of Frontiers in Sociology*, *6*(3), 44–50. https://doi.org/10.25236/ijfs.2024.060308

Topor, L. (2024). Sovereignty, Power, International Security and a Lack of International Law. In *Cyber Sovereignty. Global Power Shift* (pp. 45–73). Springer Cham. https://doi.org/10.1007/978-3-031-58199-1_3

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Wilenmann, J. (2019). A New Legal Science with an Old Aftertaste. *The University of Toronto Law Journal*, *69*(4), 540–556. https://doi.org/10.3138/utlj.2019-0057

Сведения об авторе



Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре, Министерство юстиции Египта; магистр права, Школа права в Лидсе, Лидский университет Беккета
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел; LS1 3HE, Великобритания, г. Лидс, городской кампус
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

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: 10.15.41 / Государственный суверенитет
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 3 октября 2024 г.
Дата одобрения после рецензирования – 15 октября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:342.1:004
EDN: https://elibrary.ru/bbsqnh
DOI: https://doi.org/10.21202/jdtl.2024.39

A Rechtsgutstheorie Lens on the Legal Aspects of the States' Cyber Interest Concept

Yassin Abdalla Abdelkarim

Luxor Elementary Court, Luxor, Egypt
Leeds Beckett University, Leeds, United Kingdom

Keywords

criminal law,
cyber diplomacy,
cyber interests,
cyberspace,
digital technologies,
human rights,
international judicial practice,
national interests,
state interests,
theory of legitimate interests

Abstract

Objective: to show the evolution of the state interests concept and its application in cyberspace, where it turns out to be fundamental for the development of state military policy aimed at protecting national interests.

Methods: the research is based on the intersection of the theory of law and the concept of cyber interests of the state through the prism of the theory of legitimate interests (Rechtsgutstheorie). The latter was originally developed within the criminal law science, but with prospects for studying the concept of state interests in cyberspace. The application of the theory of legitimate interests made it possible to study the state cyber interests concept and determine its legal classification and applications. In particular, the theory of legitimate interests in this study is used to explore the legal perspectives of the concept of state interests in cyberspace as interests subject to legal protection.

Results: it is determined that in the dynamic landscape of cyberspace, there are multifaceted interests of states related to national security, economic prosperity, sovereignty and diplomacy. To ensure their protection, states initiate strategies that generate a variety of political and legal consequences in international relations. This fact determines the importance of studying the concept of state interests from a legal viewpoint, as well as their legal status and consequences. Parallels are drawn between the concept of protected legal interests within the theory of legitimate interests and cyber interests that states seek to protect. The theory requires balancing the competing interests; hence, its applicability to the actions of the state in cyberspace is

© Abdelkarim Y. 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.

considered. The obstacles are identified, that hinder applying the theory of legitimate interests to cyberspace, including difficulties of attribution, damage thresholds and the need for global consensus. The author shows the evolution of the concept of state interests, which determines the possibility of its application in cyberspace, where it serves the purposes of developing state policy aimed at protecting national interests.

Scientific novelty: it is expressed in the reflection of the theory of legitimate interests to the formation of the legal concept of cyber interests of the state, which serves as a sufficient justification for the protection of specific cyber interests.

Practical significance: the main conclusions outlined in the article can be used to identify cyberspace interests subject to legal protection (such as confidentiality, data integrity, sovereignty, and economic stability). They may also improve legal mechanisms for protecting national interests in cyberspace, ensure uniformity of relevant international judicial practice, and improve the efficiency and quality of state policy management in cyberspace in order to ensure security and peaceful coexistence.

For citation

Abdelkarim, Y. A. (2024). A Rechtsgutstheorie Lens on the Legal Aspects of the States' Cyber Interest Concept. *Journal of Digital Technologies and Law, 2*(4), 782–801. https://doi.org/10.21202/jdtl.2024.39

References

Abdelkarim, Y. A. (2024). A Literature Review of the Evolution of Sovereignty and Borders Concepts in Cyberspace. *International Cybersecurity Law Review*, *5*, 365–372. https://doi.org/10.1365/s43439-024-00118-0

Ambos, K. (2015). The Overall Function of International Criminal Law: Striking the Right Balance Between the Rechtsgut and the Harm Principles: A Second Contribution Towards a Consistent Theory of ICL. *Criminal Law and Philosophy*, *9*, 301–329. https://doi.org/10.1007/s11572-013-9266-1

Atadjanov, R. (2019). *Humanness as a Protected Legal Interest of Crimes Against Humanity: Conceptual and Normative Aspects*. TMC Asser Press. https://doi.org/10.1007/978-94-6265-299-6

Bidasolo, M. C. (2023). Is It Possible to Limit the Penal Intervention in the Twenty-First Century? In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 3–16). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_1

Cox, L. (2021). *Nationalism: Themes, Theories, and Controversies*. Palgrave Macmillan. https://doi.org/10.1007/978-981-15-9320-8

de la Cuerda Martín, M. (2023). The Impact of Soft Law on the Expansion of Criminal Law. In E. C. Demetrio et al. (Eds.), *Crisis of the Criminal Law in the Democratic Constitutional State, Legal Studies in International, European and Comparative Criminal Law* (Vol. 6, pp. 231–249). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-13413-5_13

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Foulon, M., & Meibauer, G. (2024). How Cyberspace Affects International Relations: The Promise of Structural Modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Huntington, S. (1997). The Erosion of American National Interests. *Foreign Affairs*, *76*(5), 28–49. https://doi.org/10.2307/20048198

Lanz, J. G. (2023). The Attack on the Protected Legal Interests: A Criminalisation Principle and an Element of the Criminal Offence. *Ius Novem*, *17*(3), 19–31. https://doi.org/10.2478/in-2023-0019

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199207800.001.0001

Metea, I. (2020). National Interest: Terminology and Directions of Approach. In *International Conference Knowledge-Based Organization*, *26*(1), 75–79. https://doi.org/10.2478/kbo-2020-0011

Olha, M. (2024). The Concept of Effectiveness of Ensuring the Rights and Legal Interests of a Person in Pre-trial Criminal Proceedings. *Visegrad Journal on Human Rights*, *1*, 56–63. https://doi.org/10.61345/1339-7915.2024.1.9

Onditi, F. (2023). Introduction: Diplomatic Thought and Practice. In F. Onditi et al. (Eds.), *The Palgrave Handbook of Diplomatic Thought and Practice in the Digital Age* (pp. 1–31). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-28214-0_1

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.), *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges* (pp. 17–39). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Thomas, A. J. (2023). The Open World Ethos. In *The Open World, Hackbacks and Global Justice* (pp. 15–36). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-19-8132-6_2

Tianyang, L. (2024). The Embodiment and Practice of the Principle of Legal Interest Protection in Criminal Legislation. *International Journal of Frontiers in Sociology*, *6*(3), 44–50. https://doi.org/10.25236/ijfs.2024.060308

Topor, L. (2024). Sovereignty, Power, International Security and a Lack of International Law. In *Cyber Sovereignty. Global Power Shift* (pp. 45–73). Springer Cham. https://doi.org/10.1007/978-3-031-58199-1_3

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Wilenmann, J. (2019). A New Legal Science with an Old Aftertaste. *The University of Toronto Law Journal*, *69*(4), 540–556. https://doi.org/10.3138/utlj.2019-0057

Author information



Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice; LLM Master of Laws, Leeds Law School, Leeds Beckett University
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt; LS1 3HE, City Campus, Leeds, United Kingdom
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflict of interest

The author declare 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 – October 3, 2024
Date of approval – October 15, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:347:004.4
EDN: https://elibrary.ru/clzzkx
DOI: https://doi.org/10.21202/jdtl.2024.40

Перспективы применения цифровых технологий в системе отправления правосудия в Зимбабве

Таурай Мупарадзи
Зимбабвийский университет, Хараре, Зимбабве
Технологический университет Тшване, Претория, ЮАР

Рикки Муньярадзи Муконза
Технологический университет Тшване, Претория, ЮАР

Ключевые слова

автоматизация,
отправление правосудия,
право,
суд,
судебная система,
судопроизводство,
цифровые технологии,
электронное правительство,
электронное правосудие,
электронный документооборот

Аннотация

Цель: в настоящее время в глобальном масштабе идет интенсивное обсуждение цифровизации и автоматизации предоставления услуг в государственных учреждениях, соответствующей технологическому масштабу Четвертой промышленной революции. Применение цифровых технологий имеет решающее значение для создания оптимизированной системы предоставления услуг. В африканских странах все больше внимания уделяется вопросам автоматизации и цифровизации судебной деятельности, что обусловлено опасениями по поводу рисков влияния на системы отправления правосудия. В свете этого целью данной статьи стало формирование перспективной модели внедрения и реализации процесса цифровизации в судах Зимбабве.

Методы: исследование базируется на методах научного анализа и синтеза, дедукции и индукции, правового моделирования, формально-юридическом и сравнительно-правовом методах.

Результаты: в статье представлен обзор принятых мер по цифровизации системы отправления правосудия в различных государствах, исследован передовой опыт. Выявлена сущность цифровизации судебной системы в Зимбабве, определены основные существующие и перспективные направления влияния цифровизации на судебную систему Зимбабве, показаны способы оперативного и эффективного перевода системы отправления правосудия в цифровой формат. Установлены преимущества цифровой обработки данных в судебных органах, и выявлены препятствия на пути использования цифровых систем

✉ Корреспондирующий автор
© Мупарадзи Т., Муконза Р. М., 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.

при отправлении правосудия, вследствие чего сохраняется недостаточная оптимальность Интегрированной электронной системы ведения дел (Integrated Electronic Case Management System, IECMS).

Научная новизна: в исследовании выстраивается оптимальная модель внедрения цифровых технологий в систему судопроизводства в Зимбабве, направленная на повышение эффективности цифровизации судов и преобразование системы отправления правосудия. Обосновывается, что для достижения этой цели решающее значение имеют вспомогательная инфраструктура информационно-коммуникационных технологий, уровень образования и осведомленности граждан, а также проводимая государственно-правовая политика.

Практическая значимость: ожидается, что предложенная в работе модель внедрения и повышения эффективности цифровизации судов Зимбабве позволит осуществить комплексное и бесперебойное внедрение IECMS.

Для цитирования

Мупарадзи, Т., Муконза, Р. М. (2024). Перспективы применения цифровых технологий в системе отправления правосудия в Зимбабве. *Journal of Digital Technologies and Law*, *2*(4), 802–834. https://doi.org/10.21202/jdtl.2024.40

Содержание

Введение
1. Результаты исследования
   1.1. Постановка проблемы
   1.2. Методология исследования
   1.3. Теоретические основы
      1.3.1. Модель принятия технологий (TAM)
2. Обзор литературы
   2.1. Выгоды, связанные с цифровизацией судов, и ожидаемые выгоды от внедрения Интегрированной электронной системы управления делами (IECMS) в Зимбабве
   2.2. Влияние цифровизации на доступ к правосудию
   2.3. Проблемы, связанные с цифровизацией судов, и последствия для доступа к правосудию
   2.4. Эмпирические данные о цифровизации систем отправления правосудия в отдельных странах
      2.4.1. Основные результаты предоставления услуг электронного правосудия в Великобритании
      2.4.2. Основные результаты предоставления услуг электронного правосудия в Южно-Африканской Республике
      2.4.3. Основные результаты предоставления услуг электронного правосудия в Руанде
3. Анализ и подробное обсуждение результатов исследования
   3.1. Понятие цифровизации судебных систем в Зимбабве

3.2. Преимущества, связанные с цифровизацией судебных систем
3.3. Проблемы, связанные с цифровизацией судов в Зимбабве
3.4. Практическая реализация IECMS в Зимбабве
4. Модель эффективного перехода к цифровым технологиям в отправлении правосудия
Заключение
Список литературы

Введение

В XXI в. произошли значительные изменения в сфере предоставления государственных услуг благодаря внедрению информационно-коммуникационных технологий (далее – ИКТ). Эти технологии лежат в основе парадигмы цифрового управления (Digital Governance Paradigm, DGP), которая подчеркивает центральную роль технологий в предоставлении услуг. Целью большинства судебных инноваций и реформ стало повышение эффективности работы судов (Krishna, 2018). Однако процессуальные неудобства, связанные с бумажным документооборотом судов в Зимбабве и других странах, а также множество незавершенных и текущих судебных дел создают проблемы для судебных систем во всем мире. Чтобы решить эту проблему, некоторые страны обращаются к информационным технологиям (далее – ИТ) как средству активизации отправления правосудия. Цифровизация судебной деятельности признана важнейшим компонентом электронного управления и набирает обороты (Monga, 2008). Судебную систему часто критикуют за несвоевременное отправление правосудия (Poshai & Vyas-Doorgapersad, 2023). Звучат также обвинения в пристрастности судов (Hanzi & Baeyens, 2021) и ущемлении независимости судебной власти со стороны государства в Зимбабве (Tembo & Singh, 2023). Внедрение цифровых технологий для решения проблемы накопления нерассмотренных дел дает надежду, что оно будет успешнее, чем все предыдущие попытки перестроить сектор отправления правосудия. Общепризнано, что цифровые инновации обладают потенциалом для обновления системы правосудия.

Однако внедрение электронных судебных систем сталкивается с многочисленными проблемами. Первоначально использование ИКТ в судах было встречено скептически, а затраты, связанные с созданием электронных материалов дел и обучением сотрудников судебных органов новым навыкам, оказались серьезным препятствием (Deming, 1985; Fleer, 2018; Poshai & Vyas-Doorgapersad, 2023). Несмотря на эти трудности, такие страны, как Великобритания, быстро преодолели их, создав необходимую инфраструктуру и обязав использовать технологии во всех секторах судебной системы (Deming, 1985). Преимущество заключается в том, что технологии позволяют судам эффективно распространять, анализировать, хранить, передавать и извлекать информацию (Fleer, 2018). В России достигнут прогресс в области интеграции искусственного интеллекта (далее – ИИ) в управление деятельностью судов, что подтверждает передовые позиции Российской Федерации в области ИКТ (Dneprovskaya & Abramitov, 2020). В частности, российские ученые показали, что цифровые технологии способствуют эффективному отправлению правосудия, ускоряют документооборот, экономят время и ресурсы. В Соединенных Штатах на уровне правительства признано, что электронные суды обеспечивают повышенную

безопасность оборота секретной информации, и электронные судебные процессы стали внедряться по всей стране. Так, в округе Лейк штата Флорида электронное управление документами стало эффективным способом борьбы с ограничениями на доступ к публичным документам, таким как материалы судебных разбирательств (Parrish & Courtney, 2007). Однако отсутствие стандартизированных подходов и моделей представляло проблему на ранних этапах создания электронных судебных систем (Chipeva et al., 2018). В Канаде внедрение автоматизированных систем и средств электронной коммуникации в Верховном суде заметно повысило эффективность его административной деятельности (Goulard et al., 1991). Аналогичные тенденции зафиксированы и в других странах.

Азиатские страны, такие как Малайзия и Сингапур, были одними из первых, кто внедрил электронные судебные системы, причем в Малайзии начали с электронной классификации дел, а в Сингапуре – с электронной записи судебных процессов (Cassim, 2017). В Европе и Латинской Америке электронные системы ведения дел широко распространились благодаря эффективности, непредвзятости и оперативности рассмотрения дел (Rooze, 2010). Внедрение этих систем в таких странах, как Италия, Австрия, Польша и Южная Корея, позволило решить накопившиеся проблемы и предотвратить потери данных. Среди стран Африки в применении электронных судебных систем лидером стала Кения, за ней последовали Танзания, Южно-Африканская Республика, Египет, Алжир и Марокко (Alami, 2015). Танзания и ЮАР развивались быстрее благодаря существующей инфраструктуре, при этом система Южной Африки оказалась более высокоорганизованной (Kabir et al., 2015; Naidoo, 2017).

Как подчеркивали предыдущие исследователи (Nzaro & Magidi, 2014; Mawela et al., 2017), положительное влияние ИКТ на преобразование системы государственных услуг повлияло на внедрение этих технологий в судебные системы во всем мире. В Зимбабве официальное использование систем электронного судопроизводства первоначально происходило медленно из-за неадекватной инфраструктуры, хотя заметное распространение получили доказательства с использованием ноутбуков, видеокамер, телефонов и голосовых заметок. Однако кризисная ситуация в связи с Covid-19 ускорила внедрение ИКТ в судах Зимбабве. Пандемия нарушила деловую деятельность в целом и работу отдельных судов, что привело к необходимости разработки стратегий для обеспечения непрерывности бизнеса (Muparadzi & Rodze, 2021), постоянного доступа к правосудию и предотвращения затягивания процессов. В результате в Зимбабве была внедрена электронная судебная система в соответствии с рекомендациями Всемирного банка по совершенствованию судебной деятельности и сокращению числа нерассмотренных дел (Wallace, 2019).

В настоящей статье рассматривается влияние цифровизации на судебную систему Зимбабве. Показаны способы быстрого перевода всей системы отправления правосудия в цифровой формат. Статья отвечает на ключевые вопросы в данной сфере, в том числе о сущности цифровизации судебной системы в Зимбабве, преимуществах цифровой обработки данных в судах, эффективности цифровой обработки данных при предоставлении услуг, о препятствиях на пути эффективной цифровой обработки данных и наилучшей модели внедрения и использования цифровых систем при предоставлении судебных услуг.

1. Результаты исследования

1.1. Постановка проблемы

Использование ИКТ для улучшения предоставления услуг в государственном секторе представляет собой глобальную тенденцию (Zhurkina et al., 2021). Внедрение систем электронного правительства в секторе отправления правосудия Зимбабве направлено на оптимизацию услуг по отправлению правосудия. Благодаря таким технологическим достижениям, как Интегрированная электронная система управления делами (Integrated Electronic Case Management System, IECMS), организация судебных дел осуществляется более эффективно. В судах Зимбабве внедрение электронных систем было очень своевременным из-за наличия большого количества незавершенных дел и трудностей работы с файлами. Кроме того, эффективность работы старой системы очных судебных заседаний была низка из-за серьезных проблем, связанных с Covid-19. Эта инициатива является частью усилий правительства по улучшению предоставления услуг и борьбе с коррупцией (Poshai & Vyas-Doorgapersad, 2023)[1]. Несмотря на это, проблемы, влияющие на цифровизацию и использование цифровых систем, не исчезли.

Несмотря на внедрение электронной системы управления делами (IECMS), система отправления правосудия по-прежнему сталкивается с такими проблемами, как накопление дел и задержки, которые препятствуют эффективному предоставлению услуг правосудия в Зимбабве. Проблема в том, что дела по-прежнему подаются вручную в цифровой среде (Procopiuck, 2018). Кроме того, основная проблема с IECMS в Зимбабве состоит в том, что существует норма, позволяющая сторонам судебного процесса выбирать между виртуальным или очным судебным разбирательством в полностью цифровой судебной системе. Это связано с ненадежностью системы и тем, что инновации не оправдывают ожиданий и вынуждают суды прибегать к традиционным системам бумажного документооборота и управления судопроизводством, а они являются медленными и неэффективными. Эти недостатки указывают на основные упущения в разработке и внедрении IECMS и проблемы с пропускной способностью, которые препятствуют оптимальному использованию систем электронного управления в системе отправления правосудия. Также остается неясным, сможет ли цифровизация судов действительно улучшить доступ к правосудию в Зимбабве. Это происходит из-за серьезных препятствий, мешающих бесперебойной работе IECMS, таких как отсутствие необходимой инфраструктуры, недостаточный потенциал системы, сохраняющиеся проблемы цифрового неравенства, неграмотность в области ИКТ (Poshai & Vyas-Doorgapersad, 2023), бюрократические проволочки и отсутствие литературы по цифровизации судов в Зимбабве, за исключением недавней выдающейся работы Poshai и Vyas-Doorgapersad (2023). Следует еще раз подчеркнуть, что если процесс цифровизации всей судебной системы в Зимбабве не будет ускорен, то страна останется в хвосте процесса внедрения цифрового правосудия в Африке. Таким образом, авторы данного исследования ставят вопрос: каковы основные требования для успешной реализации проектов по цифровизации в секторе отправления правосудия в Зимбабве? В работе предлагаются идеи, которые могут способствовать эффективной и успешной

[1] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

цифровизации в секторе отправления правосудия, предотвращая при этом полный крах недавно внедренной системы электронного ведения дел (ECMS). В следующем разделе изложена методология исследования, использованная для ответа на поставленный выше вопрос.

1.2. Методология исследования

В данном разделе описывается методология исследования, основанная на рекомендациях работ Creswell (2009, 2013, 2014) и Sekaran и Bougie (2010). Исследователи использовали качественный подход, который был признан наиболее подходящим для решения исследовательских вопросов и понимания того, как цифровизация системы правосудия улучшает работу судов в Зимбабве. Этот подход способствовал более глубокому пониманию процесса перехода к цифровым технологиям в судах Зимбабве и был направлен на разработку модели для совершенствования отправления правосудия. Опираясь на результаты предыдущих исследований, авторы подробно изучили вопрос цифровизации судебной системы с точки зрения потенциала для улучшения ее функционирования.

Для достижения этой цели использовался метод тематического исследования в соответствии с рекомендациями Neuman (2014) и Davies (2007). Этот подход способствует углубленному изучению процесса перехода зимбабвийских судов на цифровые технологии, при этом подчеркивая важность совершенствования судебной системы под руководством государства. По мнению Cohen с соавторами (2007), тематический метод обеспечивает конкретизацию данных, повышая их надежность в выбранной области. Тем не менее важно понимать, что результаты этого исследовательского проекта в основном относятся к конкретной ситуации.

Обзор точек зрения различных ученых способствовал всестороннему пониманию цифровизации судов, ее преимуществ для системы отправления правосудия в Зимбабве и проблем, связанных с ее внедрением.

В работе использовалась научная литература, периодика, официальные документы, газетные статьи и онлайн-публикации, служащие доступным источником справочной информации (Ahmed, 2010). Для изучения документальных свидетельств был применен контент-анализ. Соответствующие целям работы материалы были тщательно проанализированы, необходимые данные извлечены для дальнейшего анализа. Документальные свидетельства и теоретическая база служили для подтверждения или опровержения ключевых выводов исследования. Использование нескольких источников данных при единстве метода дает возможность исследователям собрать необходимую информацию и критически проанализировать полученные результаты, согласно подходам Bans-Akutey и Tiimub (2021) и Carter с соавторами (2014). Такая конвергенция информации из разных источников (триангуляция источников данных) позволила авторам подтвердить результаты исследования, представленные в статье.

Исследование опирается на вторичные данные и имеет ряд ограничений. Было выявлено, что в Зимбабве очень мало исследований по цифровизации судов, поэтому авторы сочли полезным представить мнения ученых из различных регионов для восполнения этого пробела. Однако, несмотря на эти ограничения, данное исследование представляет собой попытку обобщить опыт Зимбабве в реализации проектов по цифровизации в секторе отправления правосудия и дает информацию, которая может быть использована для дальнейших исследований.

1.3. Теоретические основы

1.3.1. Модель принятия технологий (TAM)

Для детального объяснения процесса принятия и использования технологий в системе отправления правосудия в Зимбабве авторы настоящего исследования опирались на модель принятия технологий (Technology Acceptance Model, далее – TAM), предложенную Фредом Дэвисом и соавторами в 1989 г. (Ajibade, 2018). Модель направлена на прогнозирование и объяснение приемлемости информационных систем и технологий отдельными пользователями (Kim & Crowston, 2011). TAM показывает, что принятие технологии пользователем зависит от ее воспринимаемой полезности (perceived usefulness, PU) и воспринимаемой простоты использования (perceived ease of use, PEOU), а также от наличия благоприятных условий. Следуя подходу, изложенному в работе Davis с соавторами (1989), мы изучили гипотезу о повышении эффективности работы судов, сокращению задержек и улучшению ведения дел в результате внедрения цифровых технологий. Кроме того, это позволило провести тщательный анализ существующих и отсутствующих условий для цифровизации судов в Зимбабве. Использование метода TAM способствует внедрению цифровых технологий, поэтому мы связываем эту концепцию с ожидаемым расширением доступа к отправлению правосудия даже для маргинализированных групп и граждан. Оптимизация процессов отправления правосудия является одной из целей внедрения цифровых технологий в судебные системы Зимбабве. Метод TAM показывает, как судебные процессы потенциально могут быть оптимизированы за счет сокращения бумажного документооборота и автоматизации рутинных задач. Кроме того, цифровизация способствует повышению прозрачности, достижению экономии средств, улучшению управления данными и внедрению виртуальных судов. Наконец, повышение производительности судебных органов и продвижение общей цифровой трансформации в системе отправления правосудия также являются важными целями внедрения ИКТ в судебную систему Зимбабве. Соответственно, TAM объясняет, каким образом цифровые технологии способны повысить прозрачность и подотчетность в судебных разбирательствах, эффективность управления судебными данными, помочь внедрению виртуальных судов, снижению рабочей нагрузки на персонал и модернизации системы правосудия в Зимбабве. На рис. 1 представлена модель внедрения технологии на основе работы Davis с соавторами (1989).

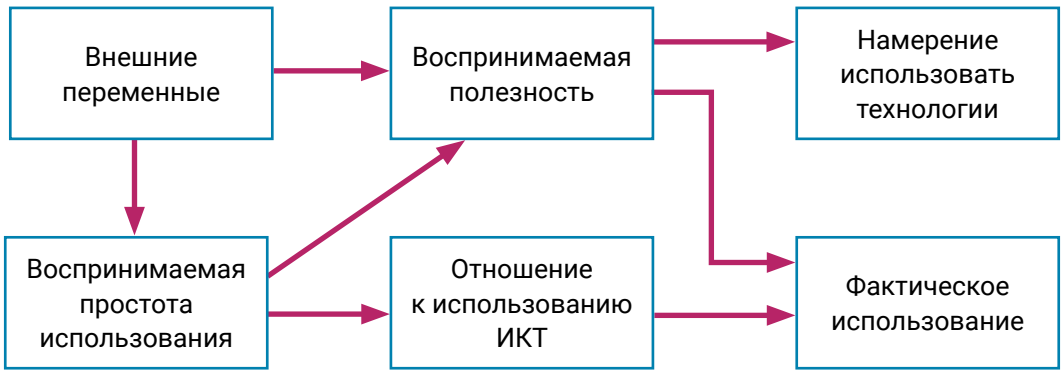


Рис. 1. Модель принятия технологий

Источник: (Davis et al., 1989).

На диаграмме из работы Davis с соавторами (1989) показаны ключевые элементы TAM. Внешние факторы влияют на восприятие полезности и простоты использования, определяя отношение к электронным судебным системам. Таким образом, внедрение цифровых систем в систему правосудия зависит от социальных, экономических и политических факторов. TAM предполагает наличие связи между намерением использовать технологию и преимуществами системы электронного правосудия. Цель исследования – оценить, соответствует ли внедрение цифровых систем правосудия этой модели.

2. Обзор литературы

2.1. Выгоды, связанные с цифровизацией судов, и ожидаемые выгоды от внедрения Интегрированной электронной системы управления делами (IECMS) в Зимбабве

В литературе широко рассматриваются преимущества цифровизации, в частности, в работе Poshai и Vyas-Doorgapersad (2023) подчеркиваются ожидаемые преимущества внедрения IECMS в Зимбабве. Авторы отмечают такие преимущества IECMS, как повышение эффективности, доступности и модернизации судебной системы. IECMS также устраняет узкие места в операционной деятельности, снижает коррупцию, облегчает подачу судебных документов и доказательств, повышает доверие общественности к судебной системе, делает судебную систему более гибкой и устойчивой, а также повышает прозрачность процедур. Это мнение согласуется с наблюдениями таких авторов, как Munyoro[2], Gatsi[3], Tshuma[4], Malaba[5] и Machaya[6]. В работах таких ученых, как Muparadzi с соавторами (2024), Muparadzi (2024), Bwalya (2018), Bannister (2015), Undi-Phiri и Phiri (2022), а также Twizeyimana и Anderson (2019), описаны различные преимущества, которые ИКТ и системы электронного правительства предоставляют в распоряжение государственных учреждений. Среди них увеличение пропускной способности судов, децентрализация управления, автоматизация и трансформация рабочих процессов, быстрота предоставления государственных услуг, повышение производительности и конкурентоспособности, улучшение процесса принятия решений и изменение организационных структур. Не подлежит сомнению, что ИКТ являются незаменимой движущей силой организационных и социальных изменений.

---

2 Munyoro, F. (2022, February 7). Zimbabwe: Virtual court to be commissioned today. All Africa. https://clck.ru/3EqaSY

3 Gatsi, D. (2022, August 11). Rights lawyers challenge judicial amendment bill – Says provisions may hinder right to fair trial. New Zimbabwe. https://clck.ru/3EqaUD; Machaya, P. (2023). Zimbabwe's labour, administrative courts go digital. https://clck.ru/3EqaWK

4 Tshuma, M., (2022). IECM to be launched. Sunday News. https://goo.su/S4u8

5 Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

6 Gatsi, D. (2022, August 11). Rights lawyers challenge judicial amendment bill – Says provisions may hinder right to fair trial. New Zimbabwe. https://clck.ru/3EqaUD; Machaya, P. (2023). Zimbabwe's labour, administrative courts go digital. https://clck.ru/3EqaWK

Цифровизация судебной системы показывает, что традиционные процедуры подачи документов в суды сопряжены с различными ограничениями и рисками, включая человеческие ошибки, коррупцию, утерю файлов и задержки в их передаче. Это делает цифровизацию судов неотложной задачей для решения этих проблем. В работе Turner (2002) подчеркивается, что электронная подача документов кардинально изменила функционирование судов. Аналогичным образом, Muhammad с соавторами (2023) отмечают, что цифровизация значительно ускорила подачу заявлений и передачу судебных документов, что привело к более быстрому рассмотрению дел. Shah и Gupta (2017) считают, что электронная подача документов и интернет-сервисы сокращают бумажный документооборот и улучшают взаимодействие между заинтересованными сторонами, тем самым облегчая отправление правосудия. Исследования показывают, что цифровизация позволяет персоналу судов работать более эффективно, сокращая время и усилия, необходимые для ведения дел. Она также сокращает затраты на хранение и поиск файлов, экономит бумагу, одновременно повышая прозрачность процесса.

В системе правосудия Малайзии цифровизация судебных процессов и систем управления делами способствовала повышению прозрачности, производительности, результативности и сокращению числа нерассмотренных дел (Haider, 2013). В частности, система Малайзии может похвастаться внедрением четырех интегрированных систем: это система электронной регистрации (Electronic Filing System, EFS), система управления делами (Case Management System, CMS), система записи и расшифровки судебных заседаний (Court Recording and Transcribing, CRT) и система управления очередностью (Queue Management System, QMS). Аналогичным образом, цифровая судебная система Руанды, имея превосходные возможности подачи и хранения документов, считается лучшей и наиболее функциональной[7] (Poshai & Vyas-Doorgapersad, 2023). Очевидно, что в этом отношении нет сомнений в больших возможностях ИКТ.

Для судов крайне важно использовать потенциал информационно-коммуникационных технологий для обеспечения бесперебойного доступа к правосудию. Этот аргумент перекликается с доводом Svitlychnyy с соавторами (2023) о том, что электронное правосудие действовало как всеобъемлющий механизм удаленного доступа во время пандемии Covid-19, доказав свою эффективность даже в период кризиса. Действительно, роль ИКТ в обеспечении непрерывности бизнеса также отмечена в работах Poshai и Vyas-Doorgapersad (2023) и Muparadzi и Rodze (2021). Таким образом, цифровая трансформация судебной системы может предоставить Зимбабве программное решение, которое объединит различные суды в рамках единой технологической платформы, оптимизируя весь жизненный цикл рассмотрения дел от подачи до принятия решения и апелляции. Однако, хотя уже известно, что система отправления правосудия в Зимбабве может выиграть от применения электронных систем правосудия, устойчивость недавно внедренной системы остается под вопросом. Подробных исследований по Зимбабве в этой области недостаточно; существующие исследования в основном посвящены другим странам, таким как Южная Африка. Последнее исследование Poshai и Vyas-Doorgapersad (2023), хотя и полезно, однако не

[7] Nkusi, F. (2017, July 16). Rwanda's electronic case management system and SDG, The New Times. https://clck.ru/3ErSz2

дает исчерпывающего представления об использовании IECMS; поэтому в настоящей работе мы представляем дополнительные подробные сведения о цифровых судебных системах.

В судебных системах многих стран мира отсутствует единая платформа для ведения дел, которая могла бы отражать текущие процессы, взаимодействовать со смежными системами и обеспечивать надежный доступ заинтересованных лиц. Это препятствует эффективной обработке и своевременному разрешению дел (Drossos et al., 2018; Adeola & Evans, 2020). Цифровизация судов вводит новые инструменты для анализа в режиме реального времени, мониторинга эффективности и принятия решений на основе фактических данных, что было особенно важно во время пандемии Covid-19. В настоящее время очевидным требованием стал доступ к правосудию для граждан и предприятий в любое время и из любого места. В работе Caserta (2022) это требование было связано с появлением юридических онлайн-платформ. Оптимизация и совершенствование процессов за счет цифровой трансформации с использованием технологий и передового опыта приводит к повышению производительности, прозрачности, доступа к правосудию, снижению транзакционных издержек и сокращению сроков судебного разбирательства (Drossos et al., 2018; Kudo, 2015). Кроме того, электронные рабочие процессы в судах позволяют ускорить рассмотрение дел и упростить доступ к судебной системе (Muscalu & Hulpus, 2016). Такие ученые, как Adeola и Evans (2020), Bajandas и Ray[8], Drossos с соавторами (2018), сходятся во мнении, что общие преимущества цифровизации в системе отправления правосудия реальны. По мнению авторов данного исследования, Зимбабве, очевидно, еще предстоит реализовать некоторые из этих преимуществ.

По опыту Bajandas и Ray[9] и Poshai и Vyas-Doorgapersad (2023), цифровизация судов дает возможность усовершенствовать процедуры подачи документов, представления доказательств, ведения документации и судебные процессы в целом. Ожидается повышение производительности, оптимизация процедуры рассмотрения дел, сокращение времени и повышение качества обработки материалов. С помощью ECMS и систем электронной подачи документов можно создать единую систему электронного правосудия или электронного суда, которая заменит отдельные несовершенные системы и автоматизирует судебные процессы. Сократится время на ввод и поиск данных; упростится обмен данными между судами и партнерами. Однако для работы с электронными доказательствами требуется специальная подготовка (Insa, 2007). Беспокойство вызывают нехватка экспертов по компьютерной криминалистике и отсутствие стандартов по работе с электронными доказательствами в Зимбабве.

Кроме того, цифровизация судов оказывает влияние на управление архивами. В работах Papagianneas и Junius (2023) и Rooze (2010) показано, что протоколы архивов должны обеспечивать подлинность, надежность, целостность и удобство использования архивного контента в судебной системе. Документооборот в судебной системе играет центральную роль в практике архивирования, определяя этапы проверки правильности осуществления судебных процессов.

---

8 Bajandas, F. F., & Ray, G. K. (2018, May 23). Implementation and use of electronic case management systems in Federal Agency adjudication: Administrative Conference of the United States. https://clck.ru/3Eug67

9 Там же.

2.2. Влияние цифровизации на доступ к правосудию

Преимущества и проблемы, связанные с цифровизацией судебных процессов, нельзя рассматривать изолированно (Aaltonen & Tammela, 2019). Крайне важно оценить их влияние на доступ к правосудию. Поэтому необходимо оценить текущие усилия в области цифровой трансформации с точки зрения стандартов доступа к правосудию на национальном, региональном и международном уровнях (Adeola & Evans, 2020). Понятие доступа к правосудию охватывает различные права человека, включая право добиваться возмещения ущерба, право доступа в помещение суда, право на получение информации, право на справедливое судебное разбирательство, право на неприкосновенность частной жизни, равенство и недискриминацию, как закреплено в конституциях разных стран (Poshai & Vyas-Doorgapersad, 2023).

Статья 7 Африканской хартии прав человека и народов гласит, что каждый человек имеет право на то, чтобы его дело было рассмотрено, включая право обращаться в суды и добиваться возмещения ущерба. Благодаря цифровизации системы правосудия работа судов постоянно трансформируется (Maseh, 2015). Ранее документы в Верховный суд подавались в печатном виде, но внедрение электронной подачи документов требует от пользователей судов адаптации к подаче документов через цифровые платформы. Однако важно учитывать реалии, с которыми сталкиваются пользователи судебной системы. Для цифрового взаимодействия необходимы такие устройства, как смартфоны или ноутбуки (Yin, 2009; Maseh, 2015). Кроме того, для доступа к цифровым платформам требуется доступ в Интернет. Остается неясным, располагают ли суды Зимбабве необходимыми цифровыми средствами для внедрения системы электронного правосудия, что вызывает вопросы о готовности страны к цифровой трансформации. Предыдущие исследования, например, Muparadzi (2024), Zinyama и Nhema (2016), Rajah (2015), Heeks (2002), Mukonza (2014) и Muparadzi с соавторами (2019) подчеркивают, что, помимо иных факторов, успешная цифровизация основывается на готовности к управлению, институциональной, культурной, инфраструктурной, политической и лидерской деятельности (электронной готовности). По мнению авторов данной статьи, внедрение цифровых инноваций в судебные системы Зимбабве может иметь негативные последствия для маргинализированных сельских общин.

Цифровая трансформация судебных систем негативно сказалась на доступе к правосудию, особенно в сфере виртуальных судебных разбирательств, которые становятся все более распространенными (Chipeva et al., 2018). В то время как цифровизация может облегчить проведение виртуальных судебных слушаний, сократив время и транспортные расходы сторон процесса, многие граждане Зимбабве не имеют необходимых устройств и доступа в Интернет для виртуального участия (Poshai & Vyas-Doorgapersad, 2023). В работе Sung (2020) указано, что электронные суды могут быть недружественными и недоступными для тех, кто не пользуется ИКТ, но стремится получить доступ к правосудию. Это напрямую влияет на осуществление права на доступ к правосудию (Maseh, 2015; Adeola & Evans, 2020; Cordella & Contini, 2020). Аналогичным образом, подача цифровых доказательств затруднена для тех, у кого нет доступа к электронным устройствам и подключения к Интернету (Cassim, 2017). Качество доступного Интернета также влияет на возможность эффективной подачи доказательств, поскольку для непрерывного взаимодействия и представления доказательств в виртуальной среде необходима широкополосная связь.

Потенциальное положительное или отрицательное влияние внедрения цифровых систем в Зимбабве на систему отправления правосудия остается неопределенным, и данное исследование призвано дать ответы на эти вопросы.

Что касается прозрачности судебной системы, то судебные органы обязаны проводить свои судебные разбирательства открыто и гласно. Этот принцип вытекает из представления о том, что правосудие должно не только свершиться, но и быть явным (Cordella & Contini, 2020; Oakes & Davies, 2016; Poshai & Vyas-Doorgapersad, 2023)[10]. Прозрачность судебной системы повышает осведомленность общественности, способствует подотчетности судей, снижает риск коррупции и позволяет общественности оспаривать предположительно неправомерные решения. Однако виртуальные судебные слушания создают проблемы, связанные с прозрачностью и принятием произвольных и неясных решений, которые, как правило, решаются открытыми судами (Meyerson, 2015; Cordella & Contini, 2020). В отличие от очных слушаний, где общественность и пресса могут наблюдать за ходом разбирательства, виртуальные слушания часто проводятся только с участием заинтересованных сторон и проходят вне поля зрения общественности. Без всеобъемлющей стратегии обеспечения доступности и прозрачности виртуальных судов принцип прозрачности судебного процесса может быть поставлен под угрозу[11]. Способность электронных систем повышать прозрачность судебной системы в развивающихся странах окончательно не установлена, что побудило авторов данного исследования к изучению конкретных преимуществ и ограничений в контексте судебной системы Зимбабве.

2.3. Проблемы, связанные с цифровизацией судов, и последствия для доступа к правосудию

Онлайн судебные системы стали мощными инструментами в сфере доступности правосудия (Sung, 2020). Однако развитие цифровых судов сталкивается с множеством проблем, связанных с инфраструктурой, информационной грамотностью, политикой, организацией, структурой и энергоснабжением (Sousa & Guimaraes, 2017; Pillot et al., 2019; Poshai & Vyas-Doorgapersad, 2023). В Зимбабве серьезным препятствием на пути цифровизации является дефицит инфраструктуры (Poshai & Vyas-Doorgapersad, 2023). Это подчеркивает важность обеспечения готовности к цифровым технологиям до начала реализации проектов электронного правительства (Muparadzi et al., 2024) и позволяет странам, оснащенным ИКТ, использовать эти инвестиционные возможности при прочих равных условиях.

Основой успешной цифровизации судебной системы является наличие соответствующей инфраструктуры. Во многих развивающихся странах, включая Зимбабве, недостаточная инфраструктура препятствует внедрению электронных услуг (Masenya & Ntengenyane, 2022). В то время как некоторые страны используют центры предоставления государственных услуг для снижения затрат на приобретение

[10] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

[11] Bajandas, F. F., & Ray, G. K. (2018, May 23). Implementation and use of electronic case management systems in Federal Agency adjudication: Administrative Conference of the United States. https://clck.ru/3Eug67

ИТ-инфраструктуры для цифровизации, во многих развивающихся странах по-прежнему отсутствует необходимая инфраструктура для внедрения электронных услуг в судебной системе. Эта проблема сохраняется и в Зимбабве, что препятствует внедрению цифровой системы правосудия.

Проблемы с электроснабжением создают дополнительные препятствия для работы компьютерных систем во всем мире. Зимбабве, наряду с такими странами, как Южная Африка, Замбия и Индия, сталкивается с серьезными проблемами с электроснабжением, что приводит к задержкам в цифровизации судебных процессов (Vasista, 2018). Важность проблем с электроснабжением, препятствующих эффективному внедрению цифровых систем в секторе отправления правосудия, очевидна, как отмечают Muparadzi с соавторами (2024). Что касается Зимбабве, то, по мнению исследователей, существующая инфраструктура электроснабжения значительно ограничена в своих возможностях по поддержке надежной системы электронного судопроизводства.

Технологическая неграмотность среди судебных чиновников представляет собой серьезную проблему для цифровизации судебных процессов (Bosire et al., 2017; Poshai & Vyas-Doorgapersad, 2023). Для решения этой проблемы необходимы учебные программы, обеспечивающие передачу знаний и эффективное использование инструментов ИКТ в цифровых судебных процессах (Bosire et al., 2017; Cassim, 2017). Недостаточная ИТ-грамотность, особенно в Зимбабве, сказывается на государственных проектах в области ИКТ в различных секторах. Несмотря на инициативы Комиссии по судебным услугам (Judicial Services Commission, JSC) по обучению сотрудников судов, среди них сохраняется дефицит компетенций и навыков в области ИКТ. В результате рядовые граждане лишены доступа к таким важным системам, как IECMS (Poshai & Vyas-Doorgapersad, 2023). Понимание функциональности и преобразующего потенциала приложений ИКТ в секторе правосудия имеет решающее значение для полноценного использования преимуществ, которые они предлагают (Zhang et al., 2024).

Политические решения африканских стран также подвергаются критике, так как часто оказываются неудачными (Cloete, 2005). Значительным препятствием для перехода судебных процессов на цифровые технологии является отсутствие надежных законов, поддерживающих технологическую интеграцию в систему правосудия (Thalib et al., 2017). Политические реформы необходимы, чтобы активизировать усилия по цифровизации с привлечением ключевых заинтересованных сторон, таких как судьи, сотрудники судов и юристы (Weers, 2016). В Зимбабве для повышения эффективности систем электронного правосудия необходимо создать соответствующую политическую основу. Для этого требуется обновить существующую политику в области ИКТ и обеспечить последовательное развитие электронного правительства (Muparadzi et al., 2024; Mukonza et al., 2016).

Структурные проблемы создают еще более значительные препятствия для цифровой трансформации судебных процессов в Зимбабве и других африканских странах. Переходу на цифровые системы мешают такие проблемы, как неадекватные организационные планы по управлению документооборотом, недостаток знаний по управлению документами и архивами, а также отсутствие законодательства и политики, регулирующих управление документами (Maseh, 2015). Безопасность

и конфиденциальность данных в системе электронного правосудия имеют первостепенное значение, что требует внедрения норм контроля доступа и соблюдения стандартов безопасности (Han et al., 2024). Защита конфиденциальности пользователей в условиях цифровых данных и коммуникаций требует строгих мер, что подчеркивает необходимость всеобъемлющей и эффективной организационной и национальной внутренней политики, регулирующей использование информации в рамках системы отправления правосудия в Зимбабве.

2.4. Эмпирические данные о цифровизации систем отправления правосудия в отдельных странах

2.4.1. Основные результаты предоставления услуг электронного правосудия в Великобритании

В Великобритании произошел переход от альтернативного разрешения споров (alternative dispute resolution, ADR) к разрешению споров онлайн (online dispute resolution, ODR), который показал, что технология в первую очередь функционирует как инструмент поддержки разрешения споров, в том числе в кризисных ситуациях (Sourdin, 2020), а не как независимая система, способная автоматически обрабатывать и разрешать споры (Morison & Harkens, 2019). В работе Prescott (2017) отмечается, что в залах судебных заседаний Великобритании внедрены цифровые системы, включая такие технологии, как видеоконференции для удаленной дачи показаний, онлайн-заполнение формуляров, установление очередности оказания услуг, мобильный доступ и онлайн-системы разрешения дел. Также в работе Donoghue (2017) подчеркивается, что проведение судебных процессов с видеозаписью с помощью таких новых технологий, как ноутбуки, компьютеры и видеомагнитофоны, в Великобритании было успешным, результатом чего стало внедрение перекрестных допросов с предварительной видеозаписью в общенациональном масштабе. Успех цифровых судебных систем в Великобритании объясняется наличием ИТ-инфраструктуры и цифровой грамотности, что способствовало реализации инициатив по реформированию судебной системы. Это говорит о том, что, когда в стране имеется необходимая ИТ-инфраструктура, цифровизация судебных систем, как правило, протекает гладко. Развивающиеся страны, такие как Зимбабве, могут извлечь уроки из этого опыта и работать над внедрением цифровых технологий в свои судебные системы для повышения эффективности отправления правосудия.

2.4.2. Основные результаты предоставления услуг электронного правосудия в Южно-Африканской Республике

Южно-Африканская Республика, как и другие страны Южной Африки, довольно успешно внедряет цифровые судебные системы для улучшения отправления правосудия. Используя новые эффективные методы, бумажный документооборот и другие судебные процедуры были переведены в цифровой формат (Cordella & Contini, 2020). В работе Satirah и Haider (2013) описаны такие меры цифровизации, как отправка уведомлений о судебных заседаниях с помощью мобильных СМС-сообщений вместо бумажных документов. Онлайн-инструменты используются для подачи документов, проведения слушаний, подписания и передачи документов, что повышает доступность системы правосудия.

Внедрение электронной системы ведения дел в Южно-Африканской Республике повысило безопасность и эффективность работы с файлами, упростив отслеживание и поиск информации[12]. Виртуальные суды, особенно во время пандемии, предотвратили затягивание рассмотрения дел, обеспечив своевременное принятие решений (Sourdin et al., 2020)[13]. В работе Hassan с соавторами (2016) указано, что внедрение этих инноваций начиналось с электронной системы подачи дел (ECFS) по гражданским делам и позже распространилось на патентные дела. Несмотря на такие трудности, как большое количество отложенных дел и проблемы с энергоснабжением, Южно-Африканская Республика эффективно внедряет цифровое управление судопроизводством[14].

2.4.3. Основные результаты предоставления услуг электронного правосудия в Руанде

Руанда признана образцом для подражания в области предоставления услуг электронного правосудия в Африке (Poshai & Vyas-Doorgapersad, 2023). Система IECMS в Руанде служит единой точкой входа во все учреждения, осуществляющие правосудие. Судебный сектор страны не использует ручные процедуры рассмотрения дел и бумажный документооборот. К примечательным особенностям IECMS в Руанде относятся ее способность объединять институты отправления правосудия, включая судебные органы, Министерство юстиции, Национальную прокуратуру, Департамент уголовных расследований[15] и исправительные службы[16]. IECMS помогает автоматизировать обработку судебной документации, устраняет дублирование информации, способствует своевременному и удобному открытию и закрытию судебных дел, обеспечивает мгновенную связь со сторонами в судебном процессе. Дополнительное преимущество заключается в наличии цифровой платформы, которая обеспечивает мониторинг и доступ к судебным отчетам и решениям. Чтобы достичь этого уровня развития, Руанда инвестировала значительные средства в инфраструктуру ИКТ и подключение к Интернету.

В целом, по нашему мнению, Великобритания, Южно-Африканская Республика и Руанда добились значительного прогресса во внедрении систем электронного правосудия. Их опыт подчеркивает важность инфраструктуры ИКТ, цифровой грамотности и, как показано в работе Li и Peng (2023), интеграции технологий в судебные процессы для эффективного и доступного отправления правосудия. Развивающиеся страны могут извлечь ценные уроки из этих примеров на пути совершенствования своих судебных систем за счет перехода на цифровые технологии.

---

12 Bajandas, F. F., & Ray, G. K. (2018, May 23). Implementation and use of electronic case management systems in Federal Agency adjudication: Administrative Conference of the United States. https://clck.ru/3Eug67

13 Там же.

14 Department of Justice and Constitutional Development. (2024). Judiciary Annual Report. Pretoria: Department of Justice and Constitutional Development.

15 Там же.

16 Nkusi, F. (2017, July 16). Rwanda's electronic case management system and SDG. The New Times. https://clck.ru/3ErSz2

3. Анализ и подробное обсуждение результатов исследования

3.1. Понятие цифровизации судебных систем в Зимбабве

В нашем исследовании мы стремились рассмотреть концепцию цифровизации судебных систем путем изучения различных точек зрения на цифровизацию судов в Зимбабве, отраженных в научной литературе. Результаты свидетельствуют о единодушии ученых в понимании цифровизации судебных систем. Из полученных результатов следует, что цифровизация предполагает использование информационно-коммуникационных технологий для улучшения отправления правосудия и перехода к безбумажному документообороту. Тем самым внедрение ИКТ четко увязывается с повышением операционной эффективности, что согласуется с рекомендацией TAM. Кроме того, было показано, что цифровизация судов в Зимбабве принимает различные формы, среди которых электронное ведение дел и электронные системы управления делами (ECMS). Существует общее мнение, что электронная подача дел способна заменить ручную подачу, сокращая количество ошибок, задержек и коррупции. Она также позволяет подавать дела в режиме 24/7, автоматически генерировать номера дел и квитанции, упрощать судебный процесс. В системе электронного документооборота дела классифицируются, что приводит к устранению задержек, улучшению управления делами и своевременной обработке материалов. Таким образом, автоматизация систем управления делами с помощью цифровых технологий повышает производительность, улучшает управление потоками и сокращает задержки.

Понимание цифровизации в судебных системах также выходит за рамки отдельных определений и отражает различные проявления. Интегрированная система электронного ведения дел (IECM) определяется как комплексный пакет инструментов, охватывающий весь судебный процесс. Ее внедрение в Зимбабве позволило осуществить стратегии цифровизации для своевременного отправления правосудия посредством онлайн-планирования и обеспечения прозрачности. Очевидно, что ИКТ играют ключевую роль в усилиях по цифровизации в секторе правосудия, решая проблемы с предоставлением услуг в судах Зимбабве.

Внедрение электронного документооборота и ECMS рассматривается как смелый шаг на пути к повышению эффективности системы отправления правосудия. Так, IECM служит комплексным решением, охватывающим весь жизненный цикл рассмотрения дел. Несмотря на то, что работа по внедрению цифровых технологий в судах Зимбабве находится на ранней стадии, она обещает решить проблемы с предоставлением услуг. Интеграция технологий, в частности ИКТ, дает преимущества с точки зрения эффективности, прозрачности и улучшения взаимодействия между подразделениями, задействованными в секторе правосудия.

3.2. Преимущества, связанные с цифровизацией судебных систем

В нашем исследовании мы также рассматривали преимущества внедрения цифровых судебных систем. Были выявлены многочисленные преимущества, связанные с цифровизацией судебных систем в Зимбабве. Рассмотрим их ниже.

Во-первых, результаты исследования указывают на то, что внедрение цифровых систем в судебные системы Зимбабве потенциально может повысить эффективность и результативность работы и помочь судам, несмотря на их ограниченные ресурсы, преодолеть перегрузки, возникающие из-за откладывания дел. В этом отношении

электронные судебные системы способствуют повышению эффективности, устраняя ненужные задержки с подачей дел, управлением ими и оформлением документов. Бумажные системы устарели, и внедрение информационных технологий позволяет обеспечить безопасное хранение информации в облачных системах, устраняя эти проблемы. В работе Wallace (2019) была точно подмечена основная выгода от внедрения ИКТ в судебную систему – экономия времени. Авторы данной статьи придерживаются мнения, что все функциональные возможности IECMS должны быть доступны пользователю из дома или офиса, но проблема в том, что некоторые функции остаются по-прежнему недоступными или неудобными.

Одной из важных функций IECMS являются электронная регистрация и планирование рассмотрения дел. Это обеспечивает такие преимущества, как подотчетность, прозрачность, минимизация коррупции и упрощение передачи, хранения и поиска информации. Положительное влияние цифровых систем на работу судов широко признано, поэтому автоматизация судов в Зимбабве – это текущий проект, инициированный Комиссией по судебным услугам (Judicial Service Commission, JSC) и реализуемый поэтапно. На начальном этапе основное внимание уделяется ключевым судам, а последующие этапы охватывают другие суды. Внедрение цифровых судебных систем направлено на повышение эффективности системы отправления правосудия, однако на каждом этапе перехода к онлайн-системам возникают сложности.

Результаты исследования также показали, что полное внедрение цифровых судебных систем в Зимбабве потенциально может повысить доверие общественности к судебным системам. Ученые, труды которых упомянуты в статье, в целом согласны с тем, что внедрение цифровых систем повышает доверие общественности к судам. Мы убеждены, что именно традиционная бумажная система виновата в значительных задержках, в результате которых граждане отзывали свои иски или перестали добиваться их рассмотрения. Таким образом, использование ИКТ рассматривается как средство обеспечения качественного информирования граждан о работе судов, процедурах, рассмотрении дел и онлайн-доступе к решениям по делам, тем самым повышая доверие общественности. Кроме того, по нашему мнению, задержки, вызванные бумажной волокитой, могут привести к неэтичному поведению при рассмотрении дел, что приведет к постепенному подрыву доверия к системе. Таким образом, внедрение цифровых технологий способно повысить доверие к отправлению правосудия в стране.

Полученные результаты также свидетельствуют о том, что использование цифровых судебных систем расширяет доступ к услугам, что, в свою очередь, повышает доверие людей к этой системе. Важным выводом является то, что цифровизация судов не только обещает сделать судебную систему более прозрачной и эффективной, но и устраняет причину, которая в настоящее время подрывает прозрачность и доверие к судебной системе.

Проанализированные мнения ученых свидетельствуют о том, что цифровизация судов Зимбабве потенциально может повысить качество принятия решений по судебным делам. Внедрение информационных технологий в судебные системы позволяет быстро и эффективно передавать, извлекать и хранить информацию, решая проблемы своевременной организации рассмотрения дел и потери информации. Это экономит время на судебные разбирательства и вынесение судебных решений. Еще одно важное мнение, отмеченное в этом исследовании, заключается в том, что теперь можно очень быстро получать судебные приказы, поскольку система просто извлекает ваш проект приказа, если в нем

нет изменений. Технология также позволяет использовать видео- и аудиозаписи в качестве первичных доказательств, повышая качество принимаемых решений. Однако необходимо разработать механизмы борьбы с проявлениями неуважения к суду, возникающими в результате фальсификации или манипулирования такими доказательствами, в том числе с помощью поддельных видео- и текстовых доказательств. Эти выводы согласуются с работой Wallace (2019), где подчеркивается, что электронные системы ведения дел улучшают предоставление услуг и сокращают задержки, что приводит к принятию своевременных решений и повышению их качества. За счет выделения большего количества времени на слушания, расследования и представление доказательств административные задачи сводятся к минимуму, что позволяет сосредоточиться на ключевых аспектах дел.

В более ранних исследованиях было показано, что внедрение электронных судебных систем является средством обеспечения доступа к правосудию. Доступ к правосудию считается важнейшим элементом судебной системы, а использование ИКТ в судах потенциально способствует ему. Автоматизация судов облегчает обмен информацией, отслеживание и мониторинг дел, устраняет барьеры, создаваемые ненужными процедурами и задержками. Ожидается, что после окончательного внедрения цифровизации граждане смогут проверять статус своих дел, получать уведомления о слушаниях и просматривать судебные решения. Однако следует отметить, что в Зимбабве трудно проводить полноценные судебные процессы с помощью видео из-за проблем с подключением и низкой распространенности вспомогательных устройств. Это еще больше отодвигает рядовых граждан на периферию доступа к правосудию.

Результаты исследования также указывают на то, что использование цифровых систем в судебной системе Зимбабве повышает прозрачность и подотчетность. Цифровизация повышает прозрачность, устраняя ручные манипуляции, позволяя отслеживать ход дела, сокращая задержки и коррупцию. Также становится возможным вести запись судебных заседаний, передавать данные контролирующим органам и облегчать управление служебной деятельностью. Это способствует прозрачности и обеспечивает общественный контроль за деятельностью судебных должностных лиц, позволяя гражданам и надзорным органам оценивать достижение ожидаемых результатов. Этот аргумент поддерживается Агентством США по международному развитию (United States Agency for International Develo pment, USAID (2021), которое согласно с тем, что автоматизация судов способствует прозрачности и подотчетности. Случайное распределение дел с помощью цифровых систем помогает бороться с коррупцией, устраняя финансовую заинтересованность, существующую при ручном распределении. Кроме того, технологии позволяют гражданам получать доступ к конфиденциальной информации в режиме онлайн, повышая ответственность судей за свои действия. Это способствует установлению взаимосвязи между заинтересованными сторонами и облегчает предоставление услуг через структуру сетевого управления. Гражданам рекомендуется сообщать о ненадлежащем управлении, а надзорные органы могут привлекать судебные органы к ответственности за их работу, как уже отмечалось в работах Poshai и Vyas-Doorgapersad (2023) и Wallace (2019).

Наконец, ученые согласны в том, что цифровизация судебных систем улучшает доступ к данным в интересах граждан и иных сторон. Обеспечивая своевременный и безопасный доступ к данным, цифровые системы способствуют разработке политики, основанной на фактических данных. Например, данные, поступающие из судов, могут служить основой для разработки политики, связанной с тем или иным

видом преступлений, предоставляя данные о количестве зарегистрированных дел. Внедрение цифровых систем в судах Зимбабве повышает прозрачность, подотчетность и доступ к данным, что в конечном итоге улучшает отправление правосудия.

3.3. Проблемы, связанные с цифровизацией судов в Зимбабве

В данном разделе рассматриваются проблемы и практика реализации цифровых судебных систем в Зимбабве. Цифровизация судов направлена на повышение прозрачности, подотчетности и доступа к правосудию. Однако, как было показано в работе Poshai и Vyas-Doorgapersad (2023), эффективному внедрению цифровых систем препятствуют несколько ключевых проблем. Главная из них заключается в отсутствии надлежащей инфраструктуры, включая ограниченный доступ к Wi-Fi, подключению к Интернету, компьютерам, планшетам и другим необходимым устройствам в залах судебных заседаний. Кроме того, существенным препятствием для успешного внедрения цифровых технологий является отсутствие финансирования (Watson et al., 2017). Далее, процесс цифровизации сталкивается с проблемой перебоев в подаче электроэнергии. Несмотря на эти препятствия, важно изучить практические шаги, которые могут быть предприняты для внедрения цифровых систем в судах Зимбабве. В этом разделе рассматриваются выявленные проблемы и практические стратегии, которые могут помочь преодолеть сложности, связанные с цифровизацией судебных систем в Зимбабве.

Результаты нашего исследования еще раз подчеркивают, что основной проблемой является отсутствие надлежащей ИТ-инфраструктуры. В залах судебных заседаний отсутствуют такие важные ресурсы, как Wi-Fi, доступ в Интернет, компьютеры, планшеты и другие устройства, необходимые для подключения к Интернету. По мнению исследователей, нынешняя ситуация закрепляет монополию на правосудие за теми, кто может позволить себе доступ к Интернету, в результате чего большинство граждан не могут воспользоваться этой возможностью.

Неадекватность ИТ-инфраструктуры в судебной системе Зимбабве подтверждается мнениями экспертов, например, работами Malaba[17] и Weers (2016). В первой из них показано, что поэтапное внедрение электронных судебных систем обусловлено ожидаемыми трудностями и отсутствием необходимой инфраструктуры. В статье Vasista (2018) утверждается, что развивающиеся страны часто сталкиваются с препятствиями при внедрении электронных судебных систем из-за недостаточной инфраструктуры. Таким образом, не будет преувеличением предположить, что цифровизация судов в Зимбабве не застрахована от этих проблем.

Результаты исследования свидетельствуют о том, что отсутствие достаточного финансирования является существенным препятствием на пути к повышению эффективности цифровой системы правосудия в Зимбабве. Нельзя сбрасывать со счетов решающую роль финансовых средств в ее внедрении в судах. По нашему мнению, судебная система Зимбабве слишком интенсивно взялась за цифровизацию, не принимая во внимание финансовые трудности, с которыми она сталкивается. Исследование также показало, что электронные судебные системы в Зимбабве все еще находятся на ранней стадии развития, им не хватает полной функциональности

[17] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

и доступности. Как следствие, малоимущие граждане оказались лишены доступа к правосудию, тогда как целью было расширение такого доступа с помощью технологий. Работа Tonn с соавторами (2012) также подтверждает, что недостаточное финансирование является основным препятствием, снижающим эффективность цифровизации в системе отправления правосудия. Крайне важно, чтобы внедрение цифровых систем сопровождалось достаточным финансированием для обеспечения успешного процесса внедрения, практической реализации и модернизации электронного правосудия в Зимбабве.

Еще один вывод из нашего исследования состоит в том, что серьезной проблемой является недостаточное электроснабжение. Авторы убеждены, что работа системы не будет налажена до тех пор, пока не будут устранены проблемы с электроснабжением. Это согласуется с выводом Muparadzi с соавторами (2024) о том, что дефицит электроэнергии в Зимбабве по-прежнему велик. Устройства ИКТ, используемые в электронных судебных системах, требуют постоянного электропитания для надлежащего функционирования. Следует признать, что перебои в подаче электроэнергии нарушают непрерывные судебные процессы, приводя к внезапным остановкам судебных разбирательств. Таким образом, для успешной цифровизации судов в Зимбабве необходимо принять срочные меры по устранению проблем с электроснабжением.

3.4. Практическая реализация IECMS в Зимбабве

Изучив стратегии по внедрению цифровых технологий в систему правосудия Зимбабве, мы должны еще раз подчеркнуть необходимость создания развитой инфраструктуры для обеспечения успешного внедрения ИКТ. Как показано в работе Muhammad с соавторами (2023), развивающиеся страны часто терпят неудачу в реализации принятых решений из-за неадекватной инфраструктуры. Аналогичным образом, мы отмечаем важность таких элементов инфраструктуры, как информационные технологии, электроснабжение и устройства для доступа в Интернет, а также соответствующая правовая база. Взаимодействие с заинтересованными сторонами также является важнейшим фактором успеха. Участие всех заинтересованных сторон создает экосистему для эффективного внедрения инноваций, способствуя коллективному принятию решений и поддержке на местном уровне. В работе Malaba[18] показано, что Комиссии по судебным услугам удалось привлечь к участию различные заинтересованные стороны, включая правительственные органы, представителей судебной системы и граждан. Кроме того, внедрение технологий потребовало проведения обширных образовательных и просветительских кампаний. Комиссия по судебным услугам запустила учебные программы для устранения дефицита грамотности среди заинтересованных сторон в судебной системе[19]. Мы предлагаем дополнить их созданием онлайн-платформ, например, на канале YouTube[20], для размещения обучающих видеороликов. Кроме того, было бы целесообразно создать бесплатную горячую линию и справочную службу для

[18] Malaba, L. (2022). Digital transformation of judiciaries in Africa and experiences in the face of the COVID-19 pandemic. The Judicial Service Commission of Zimbabwe. https://clck.ru/3Eufbq

[19] Там же.

[20] Иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации.

запросов и обратной связи. Эти клиентоориентированные меры соответствуют принципам цифрового управления. Итак, важнейшими мерами для успешного внедрения цифровых систем в системе отправления правосудия в Зимбабве мы считаем развитие инфраструктуры, вовлечение заинтересованных сторон и создание комплексных образовательных инициатив.

4. Модель эффективного перехода к цифровым технологиям в отправлении правосудия

Предлагаемая нами модель (рис. 2) описывает семь важнейших этапов разработки цифровой судебной системы. Для успешной цифровизации необходима адаптация требований на каждом этапе. Особое внимание уделяется пониманию функций суда и политического ландшафта, так как оно имеет решающее значение для снижения сопротивления изменениям и обеспечения эффективности системы.

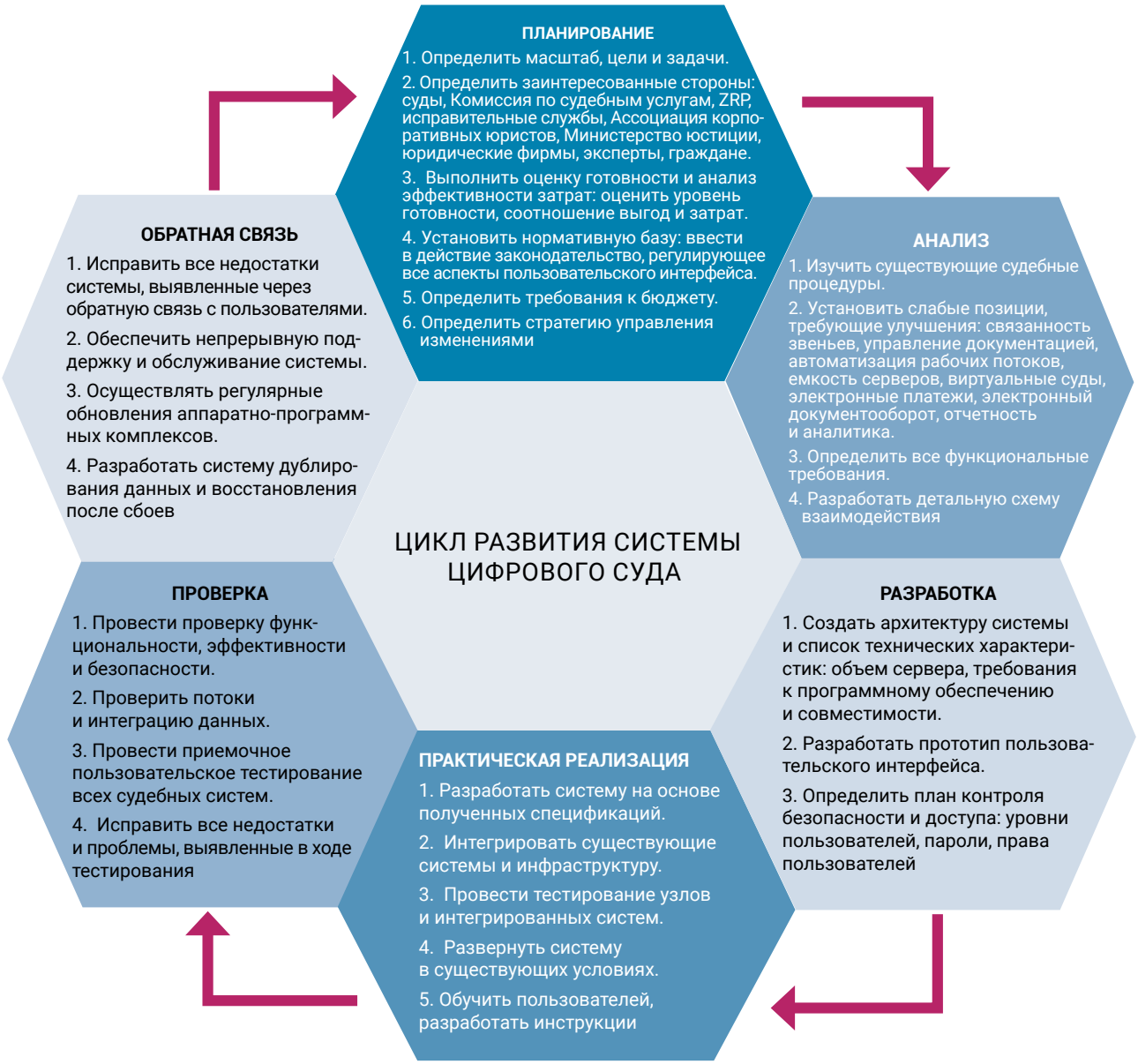


Рис. 2. Цикл развития системы цифрового суда

Источник: адаптировано из «Цикла развития систем».

В Зимбабве начало этого процесса предполагает всестороннюю оценку готовности к использованию электронных средств с учетом потребностей пользователей, учреждений и системы в целом. Необходимо провести оценку пользователей с точки зрения навыков, грамотности и образовательных потребностей в области ИКТ. В то же время институциональная оценка охватывает такие аспекты, как динамика организации, инфраструктура, лидерство, политика в области ИКТ, управление изменениями, взаимное обучение и финансирование. Успешная разработка системы зависит от аппаратного обеспечения, программного обеспечения, своевременных обновлений, лицензирования и выбора подрядчика. Тестирование в пользовательской среде включает в себя этапы входа пользователя в систему, функционального тестирования, подачи документов, отслеживания обращений, доступа к информации, оформления отчетности и выполнения аналитики. Оценка результатов по критериям прозрачности, эффективности и удобства для пользователей влечет за собой организацию обратной связи для постоянного совершенствования системы перед ее окончательным развертыванием; при этом обратная связь определяет текущие улучшения и модернизацию.

Заключение

Результаты представленного исследования дают важную информацию в аспекте понимания и внедрения цифровых технологий в судебной системе Зимбабве и говорят о необходимости интеграции ИКТ для улучшения документооборота, сокращения задержек и совершенствования отправления правосудия в стране. Полученные результаты подчеркивают потенциал цифровых технологий для улучшения работы судов, а также для повышения качества принимаемых решений и расширения доступа к правосудию в Зимбабве. Работа еще раз показала, что цифровые технологии способны повысить прозрачность и подотчетность в судебной системе Зимбабве. Они позволяют осуществлять общественный контроль, бороться с коррупцией, повышают подотчетность государственных должностных лиц и улучшают доступ к данным для разработки политики, основанной на фактических данных. Однако исследование также подтвердило, что отсутствие надлежащей ИТ-инфраструктуры является основной проблемой цифровизации судов в Зимбабве. Отсутствие необходимых ресурсов ограничивает внедрение и эффективность цифровых технологий, затрудняя доступ к правосудию. Кроме того, широко разрекламированная система IECMS как передовая технологическая инновация для судов Зимбабве не оправдала надежд из-за сохраняющихся сложных проблем, которые могут привести к полному краху инициатив по цифровизации, принятых и реализованных на сегодняшний день. Поэтому авторы считают, что предлагаемая модель может оказаться идеальной для ускорения процесса цифровизации судов в Зимбабве, и призывают принять предложенные практические подходы к внедрению цифрового правосудия.

Направления будущих исследований

Данное исследование не содержит подробного эмпирического анализа по различным регионам. Кроме того, оно основывалось на вторичных данных. В дальнейшем необходимо всестороннее сравнительное исследование с использованием первичных материалов. Приведенная выше модель, разработанная исключительно на основе качественного подхода, требует расширения за счет количественных данных, демонстрирующих взаимосвязь между достижениями в области цифровизации судов в Зимбабве и ключевыми факторами успеха внедрения цифровых технологий в этой области.

Список литературы

Aaltonen, I., & Tammela, K. (2019). Envisioning e-justice for the criminal justice chain in Finland. *Electronic Journal of E-Government*, *13*(1), 56–66.

Adeola, O., & Evans, O. (2020). ICT, infrastructure, and tourism development in Africa. *Tourism Economics*, *26*(1), 97–114. https://doi.org/10.1177/1354816619827712

Ahmed, J. U. (2010). Documentary Research Method: New Dimensions. *Indus Journal of Management and Social Sciences*, *4*(1), 1–14.

Ajibade, P. (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. *Library Philosophy and Practice (e-journal)*, 1941.

Alami, S. A. (2015). Research within the field of applied linguistics: Points to consider. *Theory and Practice in Language Studies*, *5*(7), 1330–1337. https://doi.org/10.17507/tpls.0507.03

Bans-Akutey, A., & Tiimub, B. M. (2021). Triangulation in Research. *Academia Letters*, 1–6, 3392. https://doi.org/10.20935/AL3392

Bannister, F. (2015). Deep E-Government: Beneath the carapace. In *E-government: Information, technology, and transformation* (pp. 49–67). Routledge. https://doi.org/10.4324/9781315704906-11

Bwalya, K. J. (2018). *Decolonization of E-government Research and Practice: Exploring Contextual Issues and Opportunities in Africa*. Cape Town: AOSIS ltd.

Bosire, E. M., Kivoi, D., & Nduvi, S. (2017). Effects of judicial transformation framework (2012–2016) on the performance of the judiciary in Kenya. *Archives of Business Research*, *5*(12), 349–364. https://doi.org/10.14738/abr.512.4050

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.onf.545-547

Caserta, S. (2022). The Sociology of the Legal Profession in the Digital Age. *International Journal of the Legal Profession*, *29*(3), 319–334. https://doi.org/10.1080/09695958.2021.1920417

Cassim, F. (2017). The use of Electronic Discovery and Cloud-computing Technology by Lawyers in Practice: Lessons from Abroad. *Journal for Juridical Science*, *42*(1). https://doi.org/10.18820/24150517/JJS42.v1.2

Chipeva, P., Cruz-Jesus, F., Oliveira, T., & Irani, Z. (2018). Digital divide at individual level: Evidence for Eastern and Western European countries. *Government Information Quarterly*, *35*(3), 460–479. https://doi.org/10.1016/j.giq.2018.06.003

Cloete, F. (2005). Maximising the potential of transforming policy failure into policy success: E-government, the digital divide & E-development. In G. Petroni, & F. Cloete (Eds.), *New Technologies in Public Administration, International Institute of Administrative Sciences (IIAS)* (pp. 113–132). ISO Press, Brussels.

Cordella, A., & Contini, F. (2020). *Digital Technologies for Better Justice: A Toolkit for Action*. http://dx.doi.org/10.18235/0002297

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. New York: SAGE Publications.

Creswell, J. W. (2014). *Research design: Qualitative, Quantitative and Mixed Methods* (4th ed.). California: Sage Publishers.

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA: Sage.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). New York: Routledge. https://doi.org/10.4324/9780203029053

Davies, M. B. (2007). *Key Concepts in Social Research Methods*. New York: Palgrave, Macmillan Ltd.

Davis, F. D., Baggozi R. P., & Warshaw, P. R. (1989). User of Computer Technology: comparison two theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.Org/10.1287/mnsc.35.8.982

Deming, W. E. (1985). Transformation of western style of management. *Interfaces*, *15*(3), 6–11. https://doi.org/10.1287/inte.15.3.6

Dneprovskaya, M. A., & Abramitov, S. A. (2020). Digital Technologies in Activities of Russian Courts: Prospects of Artificial Intelligence Application. In *Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)*. https://doi.org/10.2991/aebmr.k.200502.034

Donoghue, J. (2017). The Rise of Digital Justice: Courtroom Technology, Public Participation, and Access to Justice. *The Modern Law Review*, *80*(6), 995–1026. https://doi.org/10.1111/1468-2230.12300

Drossos, D., Lekakos, G., Doukidis, G. I., & Tsatsa, N. (2018). Public-sector Digitization: An Analytical Cost-Effective Framework. In *The 12th Mediterranean Conference on Information Systems (MCIS)*, Corfu, Greece.

Fleer, P. (2018). Conclusion: digitization and the continuities of change in administrative information processing. *Administration and Society*, *50*(9), 1335–1359. https://doi.org/10.1177/0095399718791540

Goulard, G. Y., Alain, C., & Clarke, G. (1991). Computerization and Electronic Communications in the Supreme Court of Canada. *International Review of Law, Computers & Technology*, *5*(1), 74–95. https://doi.org/10.1080/13600869.1991.9966307

Haider, A. (2013). E-Court: Information and Communication Technologies for Civil Court Management. In *Proceedings of PICMET '13: Technology Management for Emerging Technologies* (pp. 2296–2304).

Han, W., Shen, J., Liu, Y., Shi, Z., Xu, J., Hu, F., Chen, H., Gong, Y., Yu, X., Wang, H., Liu, Z., Yang, Y., Shi, T., & Ge, M. (2024). LegalAsst: Human-centered and AI-empowered Machine to Enhance Court Productivity and Legal Assistance. *Information Sciences*, *679*, 3–18. https://doi.org/10.1016/j.ins.2024.121052

Hanzi, R., & Baeyens, A. (2021). *Concerns over Judicial Independence in Zimbabwe*. Washington DC: Human Rights Institute.

Hassan, K. H., Yusoff, S. S. A., Mokhtar, M. F., & Khalid, A. T. K. (2016). The use of technology in the transformation of business dispute resolution. *European Journal of Law and Economics*, *42*, 369–381. https://doi.org/10.1007/s10657-012-9375-7

Heeks, R. (2002). e-Government in Africa: Promise and practice. *Information Polity*, *7*(2, 3), 97–114. https://doi.org/10.3233/ip-2002-0008

Insa, F. (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*, *1*(4), 285–289. https://doi.org/10.1080/15567280701418049

Kabir, M. A., Saidin, S. Z., & Ahmi, A. (2015). Adoption of E-Payment Systems: A Review of Literarure. In *Proceeding of the International Conference on E-Commerce (ICoEC)* (pp. 112–120).

Kim, Y., & Crowston, K. (2011). Technology adoption and use theory review for studying scientists continued use of cyber-infrastructure. *Proceedings of the American Society for Information Science and Technology*, *48*(1), 1–10. https://doi.org/10.1002/meet.2011.14504801197

Krishna, O. (2018). Structural Reforms for Overcoming Delays in Justice Delivery. *Journal of Constitutional Law and Jurisprudence*, *1*(1), 32–41.

Kudo, H. (2015). Does e-Government Guarantee Cost-effectiveness? An Experience from Japan and Italy. *Public Administration Quarterly*, *32*(1) 93–120. https://doi.org/10.1177/073491490803200103

Li, W., & Peng, Q. (2023). Digital courts and corporate investment in sustainability: Evidence from China. *International Review of Financial Analysis*, *88*, 2–19. https://doi.org/10.1016/j.irfa.2023.102682

Maseh, E. (2015). Managing court records in Kenya. *African Journal of Library, Archives & Information Science*, *25*(1), 77–87.

Masenya, T. M., & Ntengenyane, K. (2022). The Management of Digital Court Records for Justice Delivery in the South African High Courts. *Mousaion: South African Journal of Information Studies*, *40*(3). https://doi.org/10.25159/2663-659X/12691

Mawela, T., Ochara, M. N., & Twinomurinzi, L. (2017). e-Government implementation: a reflection on South African municipalities. *South African Computer Journal*, *29*(3), 23–44. https://doi.org/10.18489/sacj.v29i1.444

Meyerson, D. (2015). Why Should Justice Be Seen to Be Done? *Criminal Justice Ethics*, *34*(1), 64–86. https://doi.org/10.1080/0731129X.2015.1019780

Monga, A. (2008). E-government in India: Opportunities and challenges. *JOAAG*, *3*(2), 14–29.

Morison, J., & Harkens, A. (2019). Re-engineering justice? Robot judges, computerized courts and (semi) automated legal decision-making. *Legal Studies*, *39*(4), 618–635. https://doi.org/10.1017/lst.2019.5

Muhammad, D., Aziz, F., Ar-Rasyid, Y., & Asi-Sayyis, I. A. (2023). Assessing the Impact of Electronic Court Systems on the Efficiency of Judicial Processes in the Era of Digital Transformation. *Jurnal Ilmu Hukum dan Konstitusi*, *6*(1), 1–18. https://doi.org/10.24090/volksgeist.v6i1.8082

Mukonza, R. M. (2014). E-Governance: A New Paradigm in Public Administration. *Journal of Public Administration*, *49*(2), 499–511.

Mukonza, R. M., Maserumule, M. H., & Moeti, K. B. (2016). A Critical Examination of Socioeconomic and Demographic factors as Determinants of Egovernment Adoption Among Redidents in Zimbabwe's Two Local Authorities. *Africa Insight*, *46*(2), 60–75.

Muparadzi, T., Nyikadzino, T., & Nhema, A. (2019). A Critical Reflection on the Role of E-governance in Reinvigorating Public Sector Operations in Zimbabwe. *Zambezia*, *46*(1), 179–197.

Muparadzi, T., & Rodze, L. (2021). Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the Covid-19 Global Crisis. *Open Journal of Business and Management*, *9*(3), 1169–1197. https://doi.org/10.4236/ojbm.2021.93063

Muparadzi, T., Wissink, H., & McArthur, B. (2024). Towards a Framework for Accelerating E-Government Readiness for Public Service Delivery Improvement in Zimbabwe. *Adminstracio Publica*, *32*(2), 96–119. https://doi.org/10.61967/adminpub/2024.32.2.7

Muparadzi, T. (2024). Rethinking E-Government Implementation in Zimbabwe: Evidence and Lessons from Selected Country Cases. In *Digital Technologies for a Resource Efficient Economy. IGI Global*. https://doi.org/10.4018/979-8-3693-2750-0.ch001

Muscalu, E., & Hulpus, I. A. (2016). The computerization of courts. Implications of judicial management in the assessment of the transparency and accessibility of legal services. *Revista Economică*, *68*(1), 160–177.

Naidoo, G. (2017). Electronic technology as a mechanism to improve service delivery in South Africa. The case for an innovative e-delivery strategy in the Public Service. *South African Journal of Public Administration and Management*, *17*(2), 19–32.

Neuman, L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Harlow: Pearson Education.

Nzaro, R., & Magidi, N. (2014). Assessing the Role of Electronic Payment Systems in Financial Institutions: A Case of a Savings Bank in Zimbabwe. *Global Journal of Management and Business Research*, *14*(2), 11–36.

Oakes, A. R., & Davies, H. (2016). Justice Must Be Seen to Be Done: A Contextual Reappraisal. *Adelaide Law Review*, *37*, 461–494.

Papagianneas, S., & Junius, N. (2023). Fairness and justice through automation in China's smart courts. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *51*, 105897. https://doi.org/10.1016/j.clsr.2023.105897

Parrish, J. L., & Courtney, J. F. (2007). Electronic Records Management in Local Government Agencies: The Case of the Clerk of Courts Office in Lake County Florida. *Information Systems Management*, *24*(3), 223–229. https://doi.org/10.1080/10580530701404272

Pillot, B., Muselli, M., Poggi, P., & Dias, J. B. (2019). Historical trends in global energy policy and renewable power system issues in Sub-Saharan Africa: The case of solar 131 PV. *Energy Policy*, *127*, 113–124. https://doi.org/10.1016/j.enpol.2018.11.049

Poshai, L., & Vyas-Doorgapersad, S. (2023). Digital justice delivery in Zimbabwe: Integrated electronic case management system adoption. *South African Journal of Information Management*, *25*(1), a1695. https://doi.org/10.4102/sajim.v25i1.1695

Prescott, J. J. (2017). Improving access to justice in state courts with platform technology. *Vanderbilt Law Review*, *70*(6), 1993–2050.

Procopiuck, M. (2018). Information Technology and Time of Judgment in Specialized Courts: What is the Impact of Changing from Physical to Electronic Processing? *Government Information Quarterly*, *35*(3), 491–501. https://doi.org/10.1016/j.giq.2018.03.005

Rajah, N. (2015). E-Government in Zimbabwe: An Overview of Progress Made and Challenges Ahead. *Journal of Global Research in Computer Science*, *6*(12), 11–16.

Rooze, E. (2010). Differentiated Use of Electronic Case Management Systems. *International Journal for Court Administration*, *3*(1), 50–60. https://doi.org/10.18352/ijca.53

Satirah Wan Mohd Saman, W., & Haider, A. (2013). E-Shariah in Malaysia: Technology Adoption Within the Justice System. *Transforming Government: People, Process, and Policy*, *7*(2), 256–276. https://doi.org/10.1108/17506161311325396

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business: A skill Building Approach*. New York: John Wiley and Sons.

Shah, K. P., & Gupta, M. (2017). Role of Information Technology in Expediting the Process of Justice: An Assessment of Current Challenges and Future Goals. *International Journal of Multidisciplinary Educational Research*, *6*(6-5), 162–177.

Sourdin, T., Li, B., & McNamara, D. M. (2020). Court Innovations and Access to Justice in Times of Crisis. *Health Policy and Technology*, *9*(4), 447–453. https://doi.org/10.1016/j.hlpt.2020.08.020

Sousa, M. M., & Guimaraes, T. A. (2017). The Adoption of Innovations in Brazilian Labor Courts from the Perspective of Judges and Court Managers. *Revista de Administração*, *52*(1), 103–113. https://doi.org/10.1016/j.rausp.2016.09.008

Sung, H. (2020). Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China. *Computer Law and Security Review*, *39*, 105461. https://doi.org/10.1016/j.clsr.2020.105461

Svitlychnyy, O. P., Matselyukh, I. A., Yaselska, N. M., Glugovska, S. L., & Dyshleva, O. I. (2023). Electronic justice as a mechanism for ensuring the right of access to justice in a pandemic: the experience of Ukraine and the EU. *International Review of Law, Computers & Technology*, *37*(3), 325–340. https://doi.org/10.1080/13600869.2023.2221820

Tembo, S., & Singh, A. (2023). Mutilation of the Independence of the Judiciary: Threats, Indimidation and Conctituional Amendments in Zimbabwe. *Obiter*, *44*(3), 546–560. https://doi.org/10.17159/obiter.v44i3.14675

Thalib, H., Rahman, S., Mamulai, M., & Djanggih, H. (2017). Verification Through the Electronic Media (teleconference) on the Court in the Criminal Judicial System. *ADRI International Journal of Law and Social Science*, *1*(1), 1–9.

Tonn, B., Stiefel, D., Scheb, J. M., Glennon, C., & Sharma, H. K. (2012). Future of the Courts: Fixed, Flexible, and Improvisational Frameworks. *Futures*, *44*(9), 802–811. https://doi.org/10.1016/j.futures.2012.07.005

Turner, J. C. (2002). Changes in the Courthouse-Electronic Records, Filings and Court Dockets: Goals, Issues and the Road Ahead. *Legal Reference Services Quarterly*, *21*(4), 275–299. https://doi.org/10.1300/J113v21n04_03

Twizeyimana, J. D., & Anderson, A. (2019). The Public Value of E-Government – A Literature Review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Undi-Phiri, B., & Phiri, J. (2022). Assessing Factors Affecting the Adoption of E-Government Services in Developing Countries for Transport Sector, Amidst the Covid-19 Pandemic. *Communications and Network*, *14*, 69–90. https://doi.org/10.4236/cn.2022.142006

Vasista, T. (2018). SaaS Based E-Court Applications in E-Governance in India. *International Journal of Managing Public Sector Information and Communication Technologies*, *9*(3), 1–17. https://doi.org/10.5121/ijmpict.2018.9301

Wallace, A. (2019). Ten questions for Dory Reiling – Developing IT for courts. *International Journal for Court Administration*, *10*(1), 1–3. https://doi.org/10.18352/ijca.293

Watson, A., Rukundakuvuga, R., & Matevosyan, A. (2017). Integrated Justice: An Information Systems Approach to Justice Sector Case Management and Information Sharing Case Study of the Integrated Electronic Case Management System for the Ministry of Justice in Rwanda. *International Journal for Court Administration*, *8*(3), 1–9. https://doi.org/10.18352/ijca.233

Weers, T. D. (2016). Case flow management net-project – the practical value for civil justice in the international journal for court administration. *International Journal for Court Administration*, *8*(1), 32–42. https://doi.org/10.18352/ijca.216

Yin, R. K. (2009). *Case Study Research: Design and Methods*. Beverly: Hills.

Zhang, M., Cao, X., & Sun, A. (2024). Applications of Satellite Technologies within China's Legal System: A review. *Acta Astronautica*, *219*, 750–760. https://doi.org/10.1016/j.actaastro.2024.03.063

Zhurkina, O., Filippova, E., & Bochkareva, T. (2021). Digitalization of Legal Proceedings: Global Trends. *Advances in Economics, Business and Management Research*, *171*, 119–124. https://doi.org/10.2991/aebmr.k.210318.018

Zinyama, T., & Nhema, G. (2016). E-government and Development in Zimbabwe: An Appraisal. *Public Policy and Administration Research*, *6*(2), 13–23.

Сведения об авторах



Мупарадзи Таурай – PhD (государственное управление), преподаватель, факультет общественных и поведенческих дисциплин, Зимбабвийский университет; постдокторант, кафедра общественно-политических дисциплин, Технологический университет Тшване
Адрес: Зимбабве, MP167, г. Хараре, Маунт Плезант; Южно-Африканская Республика, 0183, г. Претория, Филип Нел Парк, Штаатсартиллерие Роуд
E-mail: tauraimuparadzi@gmail.com
ORCID ID: https://orcid.org/0000-0003-1590-6553
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=58101232900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LWJ-6359-2024
Google Scholar ID: https://scholar.google.com/citations?user=GwueN-QAAAAJ



Муконза Рикки Муньярадзи – доктор технологических наук, доцент в области государственного управления, кафедра общественно-политических дисциплин, Технологический университет Тшване
Адрес: Южно-Африканская Республика, 0183, г. Претория, Филип Нел Парк, Штаатсартиллерие Роуд
E-mail: MukonzaRM@tut.ac.za
ORCID ID: https://orcid.org/0000-0001-8121-1501
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56157610200
Google Scholar ID: https://scholar.google.com/citations?user=LXj9QUQAAAAJ

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: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 4 ноября 2024 г.
Дата одобрения после рецензирования – 19 ноября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:347:004.4
EDN: https://elibrary.ru/clzzkx
DOI: https://doi.org/10.21202/jdtl.2024.40

Prospects for Implementing Digital Technologies in the Administration of Justice in Zimbabwe

Taurai Muparadzi

University of Zimbabwe, Harare, Zimbabwe
Tshwane University of Technology, Pretoria, South Africa

Ricky Munyaradzi Mukonza

Tshwane University of Technology, Pretoria, South Africa

Keywords

administration of justice,
automation,
court,
digital documentation,
digital government,
digital justice,
digital technologies,
judicial proceedings,
judicial system,
law

Abstract

Objective: an intensive discussion is currently going on globally on digitalization and automation of providing services in public institutions, which corresponds to the technological development of the Fourth Industrial Revolution. The use of digital technologies is crucial to create an optimized service delivery system. In African countries, attention is increasingly paid to the automation and digitalization of judicial activities, due to concerns about the risks of influencing justice systems. In light of this, the article is aimed at forming a promising model for the introduction and implementation of digitalization in Zimbabwe courts.

Methods: the research is based on the methods of scientific analysis and synthesis, deduction and induction, legal modeling, formal legal and comparative legal methods.

Results: the article provides an overview of the measures taken to digitalize the system of administration of justice in various states. It also examines best practices and reveals the essence of digitalization in the judicial system in Zimbabwe. The authors identify the main existing and promising directions of the impact of digitalization on the judicial system of Zimbabwe and show the ways to promptly and effectively convert the system of justice administration into a digital format. The article

✉ Corresponding author
© Muparadzi T., Mukonza R. M., 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.

identifies the advantages of digital data processing in judicial bodies and obstacles to the use of digital systems in the administration of justice. The latter result in the insufficient optimality of the Integrated Electronic Case Management System (IECMS).

Scientific novelty: the study builds an optimal model for the introduction of digital technologies into the judicial system in Zimbabwe, aimed at improving the efficiency of courts digitalization and transforming the justice administration system. The authors proved that the crucial factors of achieving this goal are the auxiliary infrastructure of information and communication technologies, the level of education and awareness of citizens, and the ongoing state and legal policy.

Practical significance: it is expected that the proposed model to implement digitalization in Zimbabwe courts and improve its efficiency will allow for the comprehensive and uninterrupted implementation of IECMS.

For citation

Muparadzi, T., & Mukonza, R. M. (2024). Prospects for Implementing Digital Technologies in the Administration of Justice in Zimbabwe. *Journal of Digital Technologies and Law, 2*(4), 802–834. https://doi.org/10.21202/jdtl.2024.40

Reference

Aaltonen, I., & Tammela, K. (2019). Envisioning e-justice for the criminal justice chain in Finland. *Electronic Journal of E-Government*, *13*(1), 56–66.

Adeola, O., & Evans, O. (2020). ICT, infrastructure, and tourism development in Africa. *Tourism Economics*, *26*(1), 97–114. https://doi.org/10.1177/1354816619827712

Ahmed, J. U. (2010). Documentary Research Method: New Dimensions. *Indus Journal of Management and Social Sciences*, *4*(1), 1–14.

Ajibade, P. (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. *Library Philosophy and Practice (e-journal)*, 1941.

Alami, S. A. (2015). Research within the field of applied linguistics: Points to consider. *Theory and Practice in Language Studies*, *5*(7), 1330–1337. https://doi.org/10.17507/tpls.0507.03

Bans-Akutey, A., & Tiimub, B. M. (2021). Triangulation in Research. *Academia Letters*, 1–6, 3392. https://doi.org/10.20935/AL3392

Bannister, F. (2015). Deep E-Government: Beneath the carapace. In *E-government: Information, technology, and transformation* (pp. 49–67). Routledge. https://doi.org/10.4324/9781315704906-11

Bwalya, K. J. (2018). *Decolonization of E-government Research and Practice: Exploring Contextual Issues and Opportunities in Africa*. Cape Town: AOSIS ltd.

Bosire, E. M., Kivoi, D., & Nduvi, S. (2017). Effects of judicial transformation framework (2012–2016) on the performance of the judiciary in Kenya. *Archives of Business Research*, *5*(12), 349–364. https://doi.org/10.14738/abr.512.4050

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.onf.545-547

Caserta, S. (2022). The Sociology of the Legal Profession in the Digital Age. *International Journal of the Legal Profession*, *29*(3), 319–334. https://doi.org/10.1080/09695958.2021.1920417

Cassim, F. (2017). The use of Electronic Discovery and Cloud-computing Technology by Lawyers in Practice: Lessons from Abroad. *Journal for Juridical Science*, *42*(1). https://doi.org/10.18820/24150517/JJS42.v1.2

Chipeva, P., Cruz-Jesus, F., Oliveira, T., & Irani, Z. (2018). Digital divide at individual level: Evidence for Eastern and Western European countries. *Government Information Quarterly*, *35*(3), 460–479. https://doi.org/10.1016/j.giq.2018.06.003

Cloete, F. (2005). Maximising the potential of transforming policy failure into policy success: E-government, the digital divide & E-development. In G. Petroni, & F. Cloete (Eds.), *New Technologies in Public Administration, International Institute of Administrative Sciences (IIAS)* (pp. 113–132). ISO Press, Brussels.

Cordella, A., & Contini, F. (2020). *Digital Technologies for Better Justice: A Toolkit for Action*. http://dx.doi.org/10.18235/0002297

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. New York: SAGE Publications.

Creswell, J. W. (2014). *Research design: Qualitative, Quantitative and Mixed Methods* (4th ed.). California: Sage Publishers.

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA: Sage.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). New York: Routledge. https://doi.org/10.4324/9780203029053

Davies, M. B. (2007). *Key Concepts in Social Research Methods*. New York: Palgrave, Macmillan Ltd.

Davis, F. D., Baggozi R. P., & Warshaw, P. R. (1989). User of Computer Technology: comparison two theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.Org/10.1287/mnsc.35.8.982

Deming, W. E. (1985). Transformation of western style of management. *Interfaces*, *15*(3), 6–11. https://doi.org/10.1287/inte.15.3.6

Dneprovskaya, M. A., & Abramitov, S. A. (2020). Digital Technologies in Activities of Russian Courts: Prospects of Artificial Intelligence Application. In *Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)*. https://doi.org/10.2991/aebmr.k.200502.034

Donoghue, J. (2017). The Rise of Digital Justice: Courtroom Technology, Public Participation, and Access to Justice. *The Modern Law Review*, *80*(6), 995–1026. https://doi.org/10.1111/1468-2230.12300

Drossos, D., Lekakos, G., Doukidis, G. I., & Tsatsa, N. (2018). Public-sector Digitization: An Analytical Cost-Effective Framework. In *The 12th Mediterranean Conference on Information Systems (MCIS)*, Corfu, Greece.

Fleer, P. (2018). Conclusion: digitization and the continuities of change in administrative information processing. *Administration and Society*, *50*(9), 1335–1359. https://doi.org/10.1177/0095399718791540

Goulard, G. Y., Alain, C., & Clarke, G. (1991). Computerization and Electronic Communications in the Supreme Court of Canada. *International Review of Law, Computers & Technology*, *5*(1), 74–95. https://doi.org/10.1080/13600869.1991.9966307

Haider, A. (2013). E-Court: Information and Communication Technologies for Civil Court Management. In *Proceedings of PICMET '13: Technology Management for Emerging Technologies* (pp. 2296–2304).

Han, W., Shen, J., Liu, Y., Shi, Z., Xu, J., Hu, F., Chen, H., Gong, Y., Yu, X., Wang, H., Liu, Z., Yang, Y., Shi, T., & Ge, M. (2024). LegalAsst: Human-centered and AI-empowered Machine to Enhance Court Productivity and Legal Assistance. *Information Sciences*, *679*, 3–18. https://doi.org/10.1016/j.ins.2024.121052

Hanzi, R., & Baeyens, A. (2021). *Concerns over Judicial Independence in Zimbabwe*. Washington DC: Human Rights Institute.

Hassan, K. H., Yusoff, S. S. A., Mokhtar, M. F., & Khalid, A. T. K. (2016). The use of technology in the transformation of business dispute resolution. *European Journal of Law and Economics*, *42*, 369–381. https://doi.org/10.1007/s10657-012-9375-7

Heeks, R. (2002). e-Government in Africa: Promise and practice. *Information Polity*, *7*(2, 3), 97–114. https://doi.org/10.3233/ip-2002-0008

Insa, F. (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*, *1*(4), 285–289. https://doi.org/10.1080/15567280701418049

Kabir, M. A., Saidin, S. Z., & Ahmi, A. (2015). Adoption of E-Payment Systems: A Review of Literarure. In *Proceeding of the International Conference on E-Commerce (ICoEC)* (pp. 112–120).

Kim, Y., & Crowston, K. (2011). Technology adoption and use theory review for studying scientists continued use of cyber-infrastructure. *Proceedings of the American Society for Information Science and Technology*, *48*(1), 1–10. https://doi.org/10.1002/meet.2011.14504801197

Krishna, O. (2018). Structural Reforms for Overcoming Delays in Justice Delivery. *Journal of Constitutional Law and Jurisprudence*, *1*(1), 32–41.

Kudo, H. (2015). Does e-Government Guarantee Cost-effectiveness? An Experience from Japan and Italy. *Public Administration Quarterly*, *32*(1) 93–120. https://doi.org/10.1177/073491490803200103

Li, W., & Peng, Q. (2023). Digital courts and corporate investment in sustainability: Evidence from China. *International Review of Financial Analysis*, *88*, 2–19. https://doi.org/10.1016/j.irfa.2023.102682

Maseh, E. (2015). Managing court records in Kenya. *African Journal of Library, Archives & Information Science*, *25*(1), 77–87.

Masenya, T. M., & Ntengenyane, K. (2022). The Management of Digital Court Records for Justice Delivery in the South African High Courts. *Mousaion: South African Journal of Information Studies*, *40*(3). https://doi.org/10.25159/2663-659X/12691

Mawela, T., Ochara, M. N., & Twinomurinzi, L. (2017). e-Government implementation: a reflection on South African municipalities. *South African Computer Journal*, *29*(3), 23–44. https://doi.org/10.18489/sacj.v29i1.444

Meyerson, D. (2015). Why Should Justice Be Seen to Be Done? *Criminal Justice Ethics*, *34*(1), 64–86. https://doi.org/10.1080/0731129X.2015.1019780

Monga, A. (2008). E-government in India: Opportunities and challenges. *JOAAG*, *3*(2), 14–29.

Morison, J., & Harkens, A. (2019). Re-engineering justice? Robot judges, computerized courts and (semi) automated legal decision-making. *Legal Studies*, *39*(4), 618–635. https://doi.org/10.1017/lst.2019.5

Muhammad, D., Aziz, F., Ar-Rasyid, Y., & Asi-Sayyis, I. A. (2023). Assessing the Impact of Electronic Court Systems on the Efficiency of Judicial Processes in the Era of Digital Transformation. *Jurnal Ilmu Hukum dan Konstitusi*, *6*(1), 1–18. https://doi.org/10.24090/volksgeist.v6i1.8082

Mukonza, R. M. (2014). E-Governance: A New Paradigm in Public Administration. *Journal of Public Administration*, *49*(2), 499–511.

Mukonza, R. M., Maserumule, M. H., & Moeti, K. B. (2016). A Critical Examination of Socioeconomic and Demographic factors as Determinants of Egovernment Adoption Among Redidents in Zimbabwe's Two Local Authorities. *Africa Insight*, *46*(2), 60–75.

Muparadzi, T., Nyikadzino, T., & Nhema, A. (2019). A Critical Reflection on the Role of E-governance in Reinvigorating Public Sector Operations in Zimbabwe. *Zambezia*, *46*(1), 179–197.

Muparadzi, T., & Rodze, L. (2021). Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the Covid-19 Global Crisis. *Open Journal of Business and Management*, *9*(3), 1169–1197. https://doi.org/10.4236/ojbm.2021.93063

Muparadzi, T., Wissink, H., & McArthur, B. (2024). Towards a Framework for Accelerating E-Government Readiness for Public Service Delivery Improvement in Zimbabwe. *Adminstracio Publica*, *32*(2), 96–119. https://doi.org/10.61967/adminpub/2024.32.2.7

Muparadzi, T. (2024). Rethinking E-Government Implementation in Zimbabwe: Evidence and Lessons from Selected Country Cases. In *Digital Technologies for a Resource Efficient Economy. IGI Global*. https://doi.org/10.4018/979-8-3693-2750-0.ch001

Muscalu, E., & Hulpus, I. A. (2016). The computerization of courts. Implications of judicial management in the assessment of the transparency and accessibility of legal services. *Revista Economică*, *68*(1), 160–177.

Naidoo, G. (2017). Electronic technology as a mechanism to improve service delivery in South Africa. The case for an innovative e-delivery strategy in the Public Service. *South African Journal of Public Administration and Management*, *17*(2), 19–32.

Neuman, L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Harlow: Pearson Education.

Nzaro, R., & Magidi, N. (2014). Assessing the Role of Electronic Payment Systems in Financial Institutions: A Case of a Savings Bank in Zimbabwe. *Global Journal of Management and Business Research*, *14*(2), 11–36.

Oakes, A. R., & Davies, H. (2016). Justice Must Be Seen to Be Done: A Contextual Reappraisal. *Adelaide Law Review*, *37*, 461–494.

Papagianneas, S., & Junius, N. (2023). Fairness and justice through automation in China's smart courts. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *51*, 105897. https://doi.org/10.1016/j.clsr.2023.105897

Parrish, J. L., & Courtney, J. F. (2007). Electronic Records Management in Local Government Agencies: The Case of the Clerk of Courts Office in Lake County Florida. *Information Systems Management*, *24*(3), 223–229. https://doi.org/10.1080/10580530701404272

Pillot, B., Muselli, M., Poggi, P., & Dias, J. B. (2019). Historical trends in global energy policy and renewable power system issues in Sub-Saharan Africa: The case of solar 131 PV. *Energy Policy*, *127*, 113–124. https://doi.org/10.1016/j.enpol.2018.11.049

Poshai, L., & Vyas-Doorgapersad, S. (2023). Digital justice delivery in Zimbabwe: Integrated electronic case management system adoption. *South African Journal of Information Management*, *25*(1), a1695. https://doi.org/10.4102/sajim.v25i1.1695

Prescott, J. J. (2017). Improving access to justice in state courts with platform technology. *Vanderbilt Law Review*, *70*(6), 1993–2050.

Procopiuck, M. (2018). Information Technology and Time of Judgment in Specialized Courts: What is the Impact of Changing from Physical to Electronic Processing? *Government Information Quarterly*, *35*(3), 491–501. https://doi.org/10.1016/j.giq.2018.03.005

Rajah, N. (2015). E-Government in Zimbabwe: An Overview of Progress Made and Challenges Ahead. *Journal of Global Research in Computer Science*, *6*(12), 11–16.

Rooze, E. (2010). Differentiated Use of Electronic Case Management Systems. *International Journal for Court Administration*, *3*(1), 50–60. https://doi.org/10.18352/ijca.53

Satirah Wan Mohd Saman, W., & Haider, A. (2013). E-Shariah in Malaysia: Technology Adoption Within the Justice System. *Transforming Government: People, Process, and Policy*, *7*(2), 256–276. https://doi.org/10.1108/17506161311325396

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business: A skill Building Approach*. New York: John Wiley and Sons.

Shah, K. P., & Gupta, M. (2017). Role of Information Technology in Expediting the Process of Justice: An Assessment of Current Challenges and Future Goals. *International Journal of Multidisciplinary Educational Research*, *6*(6-5), 162–177.

Sourdin, T., Li, B., & McNamara, D. M. (2020). Court Innovations and Access to Justice in Times of Crisis. *Health Policy and Technology*, *9*(4), 447–453. https://doi.org/10.1016/j.hlpt.2020.08.020

Sousa, M. M., & Guimaraes, T. A. (2017). The Adoption of Innovations in Brazilian Labor Courts from the Perspective of Judges and Court Managers. *Revista de Administração*, *52*(1), 103–113. https://doi.org/10.1016/j.rausp.2016.09.008

Sung, H. (2020). Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China. *Computer Law and Security Review*, *39*, 105461. https://doi.org/10.1016/j.clsr.2020.105461

Svitlychnyy, O. P., Matselyukh, I. A., Yaselska, N. M., Glugovska, S. L., & Dyshleva, O. I. (2023). Electronic justice as a mechanism for ensuring the right of access to justice in a pandemic: the experience of Ukraine and the EU. *International Review of Law, Computers & Technology*, *37*(3), 325–340. https://doi.org/10.1080/13600869.2023.2221820

Tembo, S., & Singh, A. (2023). Mutilation of the Independence of the Judiciary: Threats, Indimidation and Conctituional Amendments in Zimbabwe. *Obiter*, *44*(3), 546–560. https://doi.org/10.17159/obiter.v44i3.14675

Thalib, H., Rahman, S., Mamulai, M., & Djanggih, H. (2017). Verification Through the Electronic Media (teleconference) on the Court in the Criminal Judicial System. *ADRI International Journal of Law and Social Science*, *1*(1), 1–9.

Tonn, B., Stiefel, D., Scheb, J. M., Glennon, C., & Sharma, H. K. (2012). Future of the Courts: Fixed, Flexible, and Improvisational Frameworks. *Futures*, *44*(9), 802–811. https://doi.org/10.1016/j.futures.2012.07.005

Turner, J. C. (2002). Changes in the Courthouse-Electronic Records, Filings and Court Dockets: Goals, Issues and the Road Ahead. *Legal Reference Services Quarterly*, *21*(4), 275–299. https://doi.org/10.1300/J113v21n04_03

Twizeyimana, J. D., & Anderson, A. (2019). The Public Value of E-Government – A Literature Review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Undi-Phiri, B., & Phiri, J. (2022). Assessing Factors Affecting the Adoption of E-Government Services in Developing Countries for Transport Sector, Amidst the Covid-19 Pandemic. *Communications and Network*, *14*, 69–90. https://doi.org/10.4236/cn.2022.142006

Vasista, T. (2018). SaaS Based E-Court Applications in E-Governance in India. *International Journal of Managing Public Sector Information and Communication Technologies*, *9*(3), 1–17. https://doi.org/10.5121/ijmpict.2018.9301

Wallace, A. (2019). Ten questions for Dory Reiling – Developing IT for courts. *International Journal for Court Administration*, *10*(1), 1–3. https://doi.org/10.18352/ijca.293

Watson, A., Rukundakuvuga, R., & Matevosyan, A. (2017). Integrated Justice: An Information Systems Approach to Justice Sector Case Management and Information Sharing Case Study of the Integrated Electronic Case Management System for the Ministry of Justice in Rwanda. *International Journal for Court Administration*, *8*(3), 1–9. https://doi.org/10.18352/ijca.233

Weers, T. D. (2016). Case flow management net-project - the practical value for civil justice in the international journal for court administration. *International Journal for Court Administration*, *8*(1), 32–42. https://doi.org/10.18352/ijca.216

Yin, R. K. (2009). *Case Study Research: Design and Methods*. Beverly: Hills.

Zhang, M., Cao, X., & Sun, A. (2024). Applications of Satellite Technologies within China's Legal System: A review. *Acta Astronautica*, *219*, 750–760. https://doi.org/10.1016/j.actaastro.2024.03.063

Zhurkina, O., Filippova, E., & Bochkareva, T. (2021). Digitalization of Legal Proceedings: Global Trends. *Advances in Economics, Business and Management Research*, *171*, 119–124. https://doi.org/10.2991/aebmr.k.210318.018

Zinyama, T., & Nhema, G. (2016). E-government and Development in Zimbabwe: An Appraisal. *Public Policy and Administration Research*, *6*(2), 13–23.

Authors information



Taurai Muparadzi – PhD (Public Administration), Lecturer, Faculty of Social and Behavioral Sciences, University of Zimbabwe; Postdoctoral Fellow, Department of Public Affairs, Tshwane University of Technology
Address: P.O.Box MP167, Mt Pleasant, Harare, Zimbabwe; Staatsartillerie Rd, Philip Nel Park, 0183 Pretoria, South Africa
E-mail: tauraimuparadzi@gmail.com
ORCID ID: https://orcid.org/0000-0003-1590-6553
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58101232900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LWJ-6359-2024
Google Scholar ID: https://scholar.google.com/citations?user=GwueN-QAAAAJ



Ricky Munyaradzi Mukonza – DTech in Public Management, Associate Professor of Public Management, Department of Public Affairs, Tshwane University of Technology
Address: Staatsartillerie Rd, Philip Nel Park, 0183 Pretoria, South Africa
E-mail: MukonzaRM@tut.ac.za
ORCID ID: https://orcid.org/0000-0001-8121-1501
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56157610200
Google Scholar ID: https://scholar.google.com/citations?user=LXj9QUQAAAAJ

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 – November 4, 2024
Date of approval – November 19, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:349.2:004.8
EDN: https://elibrary.ru/fhnkjq
DOI: https://doi.org/10.21202/jdtl.2024.41

Юридические аспекты наделения искусственного интеллекта субъектностью: перспективы использования роботов в юридической практике в Нигерии

Олувасейе О. Икубанни ✉
Университет Джозефа Айо Бабалолы, Икеджи-Аракеджи, Нигерия

Адереми О. Ойебанджи
Университет Джозефа Айо Бабалолы, Икеджи-Аракеджи, Нигерия

Аладе А. Ойебаде
Университет Джозефа Айо Бабалолы, Икеджи-Аракеджи, Нигерия

Ключевые слова

автоматизация,
искусственный интеллект,
онлайн-разрешение споров,
право,
правосубъектность,
правосудие,
робот-юрист,
цифровые технологии,
юридическая практика,
юридическое образование

Аннотация

Цель: определить потенциал и допустимость применения искусственного интеллекта в юридической деятельности по праву Нигерии.

Методы: в основу исследования положены метод научного анализа, а также формально-юридический, сравнительно-правовой, историко-правовой и системно-функциональный методы. Круг исследования представлен нормами законодательства, включая утратившие силу нормативные правовые акты, а также научной монографической и периодической литературой.

Результаты: было установлено, что искусственный интеллект и роботы-юристы являются неизбежными инновациями юридической практики многих стран, включая Нигерию. Применение указанных цифровых технологий доказало свою высокую эффективность в деятельности, связанной с отправлением правосудия, оказывая содействие в четырех областях юридических услуг: консультировании и руководстве, поиске материалов, анализе данных и прогнозировании результатов судебного процесса. Технологии значительно облегчают труд юристов, учитывая масштабы юридических услуг. Кроме того, было установлено, что, хотя применение искусственного интеллекта в целом может быть признано оправданным, привлечение

✉ Корреспондирующий автор
© Икубанни О. О., Ойебанджи А. О., Ойебаде А. 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.

роботов-юристов к юридической практике в Нигерии сталкивается как с юридическими, так и с этическими барьерами. Законы о юридическом образовании и юридической практике, действующие в этой стране, не признают роботов-юристов лицами, имеющими лицензию на юридическую практику в Нигерии. Юристы-роботы должны быть наделены статусом личности, прежде чем они смогут полностью реализовать свой потенциал в правореализационной практике Нигерии.

Научная новизна: обусловлена прежде всего постановкой исследовательской задачи по определению возможности выступления робота в качестве практикующего юриста в рамках правовой базы юридической практики в Нигерии.

Практическая значимость: сформулированные в работе выводы о неизбежности использования искусственного интеллекта и роботов-юристов в юридической практике, а также о текущем состоянии законов, регулирующих юридическую практику в Нигерии, будут полезны при рассмотрении вопроса о внесении поправок в законодательство для его адаптации к современному уровню развития цифровых технологий.

Для цитирования

Икубанни, О. О., Ойебанджи, А. О., Ойебаде, А. А. (2024). Юридические аспекты наделения искусственного интеллекта субъектностью: перспективы использования роботов в юридической практике в Нигерии. *Journal of Digital Technologies and Law*, *2*(4), 835–856. https://doi.org/10.21202/jdtl.2024.41

Содержание

Введение
1. Искусственный интеллект и появление роботов-юристов в юридической практике
2. Правовые основы юридической практики в Нигерии
   2.1. Квалификации, необходимые для юридической практики в Нигерии
   2.2. Квалификации, необходимые роботу-юристу для юридической практики в Нигерии
Заключение
Список литературы

Введение

Новые технологии – это продукт глобализации, который на протяжении многих лет играет важную роль в комплексных изменениях во всех сферах человеческой жизни (Antonio & Estrella, 2020) и является связующей нитью для цивилизации в XXI веке (Contini, 2020). Развитие технологий повлияло на все аспекты человеческих взаимоотношений и способствовало смене парадигмы от жесткой системы к гибкой (Aidonojie et al., 2020). Возможность обмениваться идеями, заключать деловые сделки и даже общаться с людьми в разных уголках мира, не встречаясь с ними лицом к лицу, является результатом той гибкости, которую принес миру технический прогресс (Ikubanni & Aidonojie, 2021). Быстрый доступ к информации и данным сегодня является одним из множества преимуществ развития технологий (Halima, 2016).

Использование сложных технологических средств, таких как искусственный интеллект, беспилотные летательные аппараты (Gallese, 2023), системы глобального позиционирования (GPS), автомобили с автономным управлением, камеры видеонаблюдения (CCTV) и многое другое, способствует дальнейшему развитию технологий во всем мире[1]. Сегодня это ключевой фактор, влияющий на организации государственного сектора, поскольку технологии используются для управления общественной инфраструктурой и предоставления услуг (Jiya et al., 2023).

Искусственный интеллект также оказывает влияние на юридическую практику (Xu, 2022). Практикующие юристы – это высококвалифицированные профессионалы, которые ведут судебные процессы, оценивают факты, выносят решения, предлагают юридические консультации, готовят документы и пр., используя свои специальные навыки и интуицию (Alarie et al., 2018; Aidonojie et al., 2021). Предполагается, что эти услуги требуют высокого интеллекта, которым могут обладать только люди (Alarie et al., 2018). Таким образом, характер этих услуг, а также навыки и время, необходимые для их оказания, часто определяют их стоимость (Alarie et al., 2018). Интересно, что сегодня технологии с помощью искусственного интеллекта используются для выполнения функций человека и, возможно, превосходят их (Alarie et al., 2016). Самым удивительным в этих машинах является тот факт, что, в отличие от людей, они функционируют идеально, безошибочно и с высокой точностью, хотя большинство из них практически не контролируются человеком (Aidonojie et al., 2020).

Сегодня, несомненно, технологии стали важным аспектом юридической деятельности в Нигерии (Aidonojie et al., 2021) и других юрисдикциях (Obianyo & Ater, 2022). Это положительно влияет на юридическую практику, а также способствует эффективному отправлению правосудия (Aniekwe, 2021). Искусственный интеллект является одним из наиболее широко используемых технологических средств в юридической деятельности. Он облегчает работу юристов, главным образом, в таких областях, как юридические исследования[2], анализ документов, оценка рисков, составление проектов юридических документов и т. д. В ряде стран применение искусственного интеллекта в судебных процессах достигло выдающегося уровня (Richard & Solow-Niederman, 2019).

В феврале 2018 г. в конкурсе на экспертизу обычных коммерческих контрактов победила, обогнав 20 лучших юристов в этой области, система искусственного интеллекта, созданная компанией Lawgeex – израильским стартапом в области юридических технологий. Кроме того, средний показатель точности системы был на 9 % выше, чем у людей[3]. В течение конкурса система решала за 26 секунд задачи, на выполнение которых у человека ушло бы 92 минуты. Таким образом, с точки зрения скорости и эффективности она выиграла у людей всухую (Hu & Lu, 2019).

---

1 Mcmillian, J. (2013). The Impact of Technology on Administrative Justice System: a speech presented to AIAL National Administrative Law Forum, Canberra on 18th July 2013. AIAL Forum No. 75. https://goo.su/xtU7H

2 Law Pavilion Electronic Law Report is a notable artificial intelligence usually used by lawyers in Nigeria for the research of decided cases by courts of law in Nigeria.

3 Verma, U. (2018, February 26). Israeli AI Software Whips Expert Lawyers in Contract Analysis. https://clck.ru/3F5BHx

Искусственный интеллект полностью изменил облик судебной системы (Giuffrida et al., 2018; Kioko et al., 2022), помогая судьям повышать точность вынесения решений (Wang, 2020; Sanctis, 2021). Высказываются предположения, что вскоре роботы-судьи могут заменить судей-людей, хотя остается неясным, как в конечном итоге изменятся способы вынесения судебных решений, профессия юриста и право в целом (Cooper, 2011). Интересно, что одним из последних технологических достижений в этой сфере является внедрение роботов в юридическую практику в Соединенных Штатах Америки. С момента появления роботов-юристов в Калифорнии отмечалось несколько противоречий относительно их способности заниматься юридической практикой. Нужно отметить, что если технологическая инновация добилась значительного успеха в одной стране, она с большей вероятностью будет принята в другой стране[4].

Именно в этом контексте мы рассматриваем в данной статье право юристов-роботов заниматься юридической практикой в соответствии с законодательством Нигерии. Мы коснемся двух основных законов, регулирующих юридическую практику в Нигерии, и попытаемся ответить на вопрос: признает ли нигерийское законодательство в его нынешнем виде робота субъектом, который может заниматься юридической практикой. Работа юристов-роботов в Соединенных Штатах не является предметом рассмотрения в данной статье, хотя мы вскользь затронем ее, чтобы подкрепить изложенные тезисы.

1. Искусственный интеллект и появление роботов-юристов в юридической практике

Технология искусственного интеллекта (далее – ИИ) не имеет точного определения, поскольку это сопряжено с множеством трудностей (Alarie et al., 2018). Однако ИИ часто описывается как использование технологии для автоматизации задач, которые обычно требуют человеческого интеллекта. Другое определение – это способность цифрового компьютера или робота, управляемого компьютером, выполнять действия, которые обычно ассоциируются с разумным существом[5]. Сюда относится разработка систем, наделенных характеристиками человека с точки зрения мышления[6]. Искусственный интеллект связан с созданием технологического устройства для автоматического выполнения сложных задач, которые могут выполнять и люди (Surden, 2019).

Искусственный интеллект, без сомнения, предполагает разработку машинных технологий для имитации человеческого интеллекта, что позволяет добиться большей эффективности при выполнении задач, которые до сих пор выполнялись людьми (Ilegieuno et al., 2021). Это компьютерный интеллект, который не использует когнитивные способности, отображаемые устройствами, в отличие от естественных когнитивных способностей, проявляющихся как у людей, так и у животных (McCorduck & Cfe, 2004). Искусственный интеллект также описывается как теория и применение систем, используемых для моделирования, расширения и углубления возможностей человеческого интеллекта (Xu & Wang, 2019). Понятие искусственного интеллекта

4 Oluwatobi, O. E. (2023, March 15) Can Robots Practice Law in Nigeria? https://clck.ru/3F5BNk

5 Copeland, B. J. Artificial Intelligence. Britannica. https://goo.su/bCjq

6 Там же.

также относится к способности компьютера имитировать разумное поведение человека, особенно его когнитивные функции, такие как способность рассуждать, находить смысл, обобщать и учиться на опыте (Gravett, 2020).

Вызывает серьезную озабоченность тот факт, что, хотя ИИ облегчает жизнь людей (Dekker et al., 2017), он также все больше сокращает количество рабочих мест (Huang & Rust, 2018). Это объясняется тем, что машины предназначены для выполнения сложных действий, как сложилось в цифровом мире на протяжении многих лет (Robinson, 2018), хотя считается, что ИИ не удалось полностью заменить потребность в человеческом опыте при принятии решений[7]. На протяжении десятков лет много говорилось об искусственном интеллекте. Однако до недавнего времени о значении ИИ для юридической практики было написано не так много (Katyal, 2019). Влияние ИИ на юридическую практику в настоящее время и даже в будущем невозможно переоценить. В целом появление искусственного интеллекта и современные тенденции его применения в юридической сфере по всему миру свидетельствуют о том, что искусственный интеллект не только изменил облик юридической отрасли, но и способен вытеснить юристов-людей (Hu & Lu, 2019).

Примечательно, что одним из примеров, демонстрирующих, как искусственный интеллект угрожает работе юриста, является ситуация с нарушениями правил парковки в г. Йорк. Теперь нарушители могут решить спор, выбрав автоматизированную систему онлайн-урегулирования (Hu & Lu, 2019), причем процесс имеет гораздо меньше этапов, требующих помощи юристов (Hu & Lu, 2019). Эта тенденция довольно очевидна даже на фоне низкой производительности современного искусственного интеллекта (Hu & Lu, 2019). Одним из наиболее впечатляющих мотивов для интеграции ИИ и области права является тот факт, что ИИ, как было описано, способен оказывать помощь в четырех областях юридических услуг, а именно: консультировании и руководстве, поиске файлов, анализе данных, прогнозировании результата судебного процесса (Greenleaf et al., 2018). Это, без сомнения, сильно упрощает работу юристов, учитывая масштаб юридических услуг. Отмечается, что роботы-юристы с искусственным интеллектом могут помочь в таких важных аспектах юридических услуг, как анализ доказательств, ознакомление с материалами дела, и ускорить переход от сбора доказательств к выстраиванию защиты (Greenleaf et al., 2018).

Появление роботов-юристов вновь вызвало споры о том, до каких пределов ИИ может быть использован для выполнения определенных задач. Робот-юрист – это технологическое устройство в виде компьютерной программы, предназначенное для автоматизированного выполнения задач юриста, включая большинство задач, связанных с юридической практикой[8]. Это компьютер на базе искусственного интеллекта, который использует технологию обработки естественного языка (Natural Language Processing, NLP) для понимания юридических вопросов и выработки соответствующих закону ответов. Робот спроектирован таким образом, чтобы иметь возможность выполнять ряд функций, таких как предоставление юридических консультаций, создание юридических документов, поиск судебной практики и многое другое.

---

7 Commerford, B. P., Dennis, S. A., Joe, J. R., & Ulla, J. W. (2021, June 21). Man Versus Machine: Complex Estimates and Auditor Reliance on Artificial Intelligence. https://goo.su/fo2AVI

8 Nangara, A. (2023, January 10). World's First robot Lawyer to Defend Human in Court. The exchange. https://clck.ru/3F5BV5

Кроме того, считается, что появление таких роботов в юридической сфере неизбежно, поскольку они, в частности, способны решить проблему дисбаланса в ресурсах юридических служб. Ученые утверждают, что идея сочетания искусственного интеллекта и права посредством изобретения роботов-судей для устранения правовой неопределенности (D'amato, 1976) вынашивалась с 1970-х гг. (Castell, 2018). Однако другие исследователи считают, что роботы должны скорее помогать судьям и адвокатам, а не заменять их (McGinnis & Pearce, 2014).

Сегодня роботы, несомненно, являются неотъемлемой частью нашей повседневной жизни. Они используются в качестве бытовой техники в домах, самоуправляемых автомобилях, системах безопасности, ресторанах и т. д. Нельзя отрицать, что появление роботов в целом упростило жизнь. Однако необходимо подчеркнуть, что идея внедрения искусственного интеллекта и роботов-юристов в юридическую деятельность изначально заключалась не в том, чтобы заменить людей, а в том, чтобы облегчить их работу (Gravett, 2020). К сожалению, сегодня считается, что машина, созданная для облегчения работы, способна заменить человека-юриста и полностью занять его место.

В 2015 г. Джошуа Браудер (Joshua Browder) разработал робота DoNotPay как чат-бота, предназначенного для оказания юридических услуг. Целью создания робота было оказание юридической помощи малоимущим гражданам, которые не могут позволить себе юридические услуги юристов-людей, в оспаривании мелких нарушений, таких как штрафы за неправильную парковку, небольшие претензии по контрактам и т. д.[9] Изначально DoNotPay был создан Джошуа Браудером для решения его проблемы[10]. Идея создания робота-юриста возникла у него, когда он учился в Стэнфорде. Ему неоднократно выписывали штрафы за неправильную парковку, так как он не включал счетчик[11]. По совету друга он написал письмо, где оспорил эти штрафы, и их сумма была уменьшена[12]. В этот момент ему пришло в голову, сколько людей получают штрафы за неправильную парковку, но не могут оспорить их из-за отсутствия времени или нехватки финансовых ресурсов для привлечения адвоката. С этой целью он предложил решение, которое привело к появлению первого в мире робота-юриста[13].

2. Правовые основы юридической практики в Нигерии

Профессия юриста признана одной из самых уважаемых и престижных; общество в определенной степени доверяет профессионалам в этой области[14]. В нигерийском обществе профессия юриста занимает ключевое положение. Кроме выполнения обычных обязанностей защищать права граждан в суде, юристы активно участвуют

---

9 Alumni, M. (2021, April 21). Machine Learning: The World's First Robot Lawyer. Digital Innovation and Transformation. https://clck.ru/3F5BY2

10 Там же.

11 Там же.

12 Там же.

13 Там же.

14 Yusuf, A. (2015, November 26). The Future of Legal Practice in Nigeria: Regulation and Discipline in the Legal Profession. Paper Presented at the 8th Annual Business Luncheon of S.P.A. Ajibade & Co. https://clck.ru/3F5BYm

в создании юридических организаций и концепций, поддерживающих идеи развития (Oko, 1994; Oguanmanam & Pue, 2006). Юридические услуги оказывают значительное влияние практически на все социальные, экономические и политические структуры страны и формируют их. Юристы становятся все более важными для нормального функционирования нигерийского общества (Oko, 1994). Они формируют основы для надежд нации на социальный и экономический прогресс (Shaeeb et al., 2023).

Хотя не вызывает сомнений, что судебные разбирательства являются краеугольным камнем юридической практики, благодаря социальным изменениям роль юристов в современном мире расширяется, выходя за рамки судебных разбирательств[15]. Так, в судебном решении по делу Anozia v. AG Lagos State[16] об обязанностях юристов говорится следующее: «Общеизвестно, что практикующий юрист несет обременительную обязанность поддерживать и блюсти верховенство закона, продвигать и укреплять дело правосудия, поддерживать высокие стандарты профессионального поведения и, следовательно, не должен совершать никаких действий, которые недостойны представителя этой почетной и престижной профессии»[17].

Юридический словарь «The Black's Law Dictionary» (Garner, 2004) определяет юридическую практику как профессиональную деятельность должным образом лицензированного юриста, охватывающую широкий спектр услуг, таких как ведение дел в судах, подготовка документов, необходимых для совершения различных сделок, от передачи земли до слияния компаний, подготовка юридических заключений по различным вопросам права, составление завещаний и других документов по операциям с недвижимостью, а также консультирование клиентов по юридическим вопросам. Этот термин также включает в себя деятельность, которой занимается сравнительно небольшое число юристов, но которая требует юридических знаний, например, разработку законодательства и судебных регламентов.

Приведенное выше определение юридической практики указывает на то, что лицо, оказывающее такие услуги, должно быть лицензированным юристом. Поэтому необходимо изучить законы, регулирующие юридическую практику в Нигерии. Постановление Верховного суда от 1876 г. имело решающее значение для юридической профессии в Нигерии, поскольку это был первый закон, регулирующий юридическую практику в стране. Постановлением признавались две категории лиц, которые могут заниматься юридической практикой в Нигерии. Согласно ст. 76, к первой категории относятся лица, прошедшие подготовку в качестве барристера или поверенного в делах в Соединенном Королевстве из-за отсутствия в Нигерии юридических учебных заведений (Orojo, 1979). Однако вторая категория – это лица, которые не имели формального юридического образования, но в силу своего опыта приобрели юридические знания и навыки. Эти лица назывались «местными адвокатами» (Adegoke et al., 2014).

Нехватка квалифицированных юристов-практиков в колонии усилила необходимость того, чтобы Верховный судья по своему усмотрению признал вторую категорию[18].

---

15 Chinaka, C. (2022, September 14). What Constitutes Legal Practice in Nigeria? The Sun. https://clck.ru/3F5BaT

16 Anozia v AG Lagos State. (2010). https://goo.su/ZZ396T1

17 Там же.

18 Section 74 of the Supreme Court Ordinance of 1876.

Однако сначала местные адвокаты были подвергнуты экзамену, чтобы проверить их знания новых законов Англии и Колонии[19]. Если Верховный судья давал свое одобрение, такие лица зачислялись на юридическую практику сроком на шесть месяцев, которая могла быть продлена еще на шесть месяцев. К сожалению, протесты квалифицированных юристов против выдачи лицензий местным адвокатам привели к прекращению такой практики. Поэтому в 1908 г. Верховный судья прекратил выдачу лицензий неквалифицированным лицам, или местным адвокатам, хотя те, у кого срок действия лицензий не истек, продолжали пользоваться ими до истечения срока их действия (Okoye, 2015).

На смену Постановлению Верховного суда от 1876 г. пришло Постановление Верховного суда от 1943 г. Соответственно, Регламент Верховного суда (гражданский процесс) от 1945 г. установил новые требования к юридической практике в Нигерии[20]. Что касается квалификации юристов, положение 1 Приказа 16 Регламента Верховного суда (гражданский процесс) от 1945 г. предусматривало, что:

«Верховный судья может по своему усмотрению утверждать, допускать и зачислять на практику в качестве барристера и поверенного в делах в суде:

а) любого, кто имеет право практиковать в качестве барристера в Англии, Ирландии или адвоката в Шотландии;

б) кто представит свидетельства, достаточные для того, чтобы убедить Верховного судью в том, что является человеком с хорошей репутацией;

в) в течение как минимум одного года выступал в качестве практикующего барристера или адвоката со стажем работы более пяти лет или практиковал в судах страны, в которой он был призван или допущен, по крайней мере, в течение двух лет после призыва или допуска, или

г) после призыва в коллегию адвокатов или допуска в качестве адвоката выступал в Нигерии в качестве практикующего барристера со стажем работы более десяти лет в течение, по крайней мере, двух лет или

д) практиковал в качестве барристера или поверенного в делах в судах британской колонии или протектората не менее двух лет...»[21]

Вышеуказанные требования к юридической практике негативно сказались на эффективности работы юристов в Нигерии, поскольку подготовка, полученная в Англии, была недостаточной для учета особенностей нигерийского общества (Adegoke et al., 2014). Следовательно, необходима была перестройка юридической сферы в Нигерии. В 1959 г. Комитет Ансворта, созданный для рассмотрения этих проблем, вынес ряд рекомендаций, которые привели к принятию Закона о юридическом образовании 1962 г. и Закона о практикующих юристах 1962 г. (Adegoke et al., 2014).

Принятие этих законов привело к созданию в 1962 г. Нигерийской юридической школы для подготовки кандидатов в юристы. Стало обязательным требование, чтобы лица, желающие заниматься юридической практикой в Нигерии, сначала получили степень юриста в любом признанном университете внутри страны или за рубежом

19 Order 8 Rules 1-4 of the Supreme Court (Civil Procedure) Rules 1876.

20 Там же.

21 Там же.

и лишь затем поступали в Нигерийскую юридическую школу (Okoye, 2015). В Нигерии срок получения диплома юриста для поступающих напрямую составляет четыре года, а для студентов, поступающих через Объединенную приемную комиссию (Joint Admissions Matriculations Board, JAMB), – пять лет. Закон о юридическом образовании и Закон о практикующих юристах 1962 г. изменили облик нигерийской юридической сферы и системы юридического образования, установив новые стандарты и квалификационные требования для юридической практики (Adegoke et al., 2014).

Закон о юридическом образовании 1962 г. с соответствующими поправками[22] является действующим законом в Нигерии. В настоящее время этот закон известен как Закон о юридическом образовании (консолидации и т. д.)[23]. На смену Закону о практикующих юристах 1962 г. пришел Закон о практикующих юристах 1975 г.[24], который устанавливает, кто и на каких условиях может заниматься юридической практикой в Нигерии. Статья 24 этого Закона определяет практикующего юриста как «лицо, имеющее право в соответствии с положениями Закона практиковать в качестве адвоката или в качестве барристера и поверенного в делах как в целом, так и для целей какой-либо конкретной организации или судебного разбирательства»[25].

2.1. Квалификации, необходимые для юридической практики в Нигерии

Как уже говорилось ранее, юридическая практика в Нигерии законодательно регулируется как Законом о юридическом образовании (консолидации и т. д.), так и Законом о практикующих юристах. Согласно разделу 2(1) Закона о практикующих юристах, в Нигерии две категории лиц могут заниматься юридической практикой. К этим категориям относятся:

1. Лицо, фигурирующее в реестре практикующих юристов, который ведет секретарь Верховного суда Нигерии. Лицо, относящееся к этой категории, должно иметь юридическое образование, полученное в признанном университете Нигерии или за рубежом, посещать Нигерийскую юридическую школу или быть освобожденным от нее, получить квалификационный сертификат от Совета по юридическому образованию, быть призванным в Коллегию адвокатов Нигерии, получить сертификат о приеме в адвокатуру от Судебной Коллегии и быть включенным в реестр практикующих юристов, который ведет секретарь Верховного суда Нигерии (Okoye, 2015). Эти требования были подтверждены в решении суда по делу Mobil Oil Nigeria Plc v Yusuf[26].

2. Если, по мнению Председателя Верховного суда, данному лицу целесообразно разрешить действовать в качестве адвоката для целей разбирательства, описанного в заявлении, то Председатель Верховного суда может на основании имеющегося у него ордера уполномочить это лицо, после уплаты сбора за регистрацию, размер которого не превышает пятидесяти найр, как указано в ордере, действовать в качестве адвоката для целей этого разбирательства и апелляций, поданных в связи с этим разбирательством.

---

22 В Закон вносились поправки в 1963, 1966, 1967, 1970, 1973, 1974, 1976, 1977 и 1985 гг.

23 Cap. L10, Laws of the Federation of Nigeria, 2010.

24 Cap 207 Laws of Federation of Nigeria 1990 now Cap L11 Laws of Federation of Nigeria 2004.

25 Там же.

26 Mobil Oil Nigeria PLC v Yusuf. (2012). https://clck.ru/3FACRw

В Нигерии прием в Коллегию адвокатов является подтверждением того, что данное лицо обладает квалификацией и лицензией на занятие юридической практикой. Любое лицо, будь то гражданин[27] или не гражданин[28] Нигерии, может быть принято в Коллегию адвокатов Нигерии при условии соответствия критериям, которые включают следующее:

1) представить квалификационный сертификат для Коллегии судей или справку об освобождении от учебы в юридической школе;

2) убедить Коллегию судей в своей хорошей репутации;

3) оплатить вызов в соответствии с требованиями Коллегии судей[29];

4) присутствовать на трех обеденных сессиях, как это предусмотрено Коллегией судей[30].

2.2. Квалификации, необходимые роботу-юристу для юридической практики в Нигерии

Общественные обсуждения многочисленных положений Закона о юридическом образовании и Закона о практикующих юристах, которые являются двумя основными нормативными актами, регулирующими юридическую практику в Нигерии, показывают, что робот не рассматривается как «лицо», которое может заниматься юридической практикой в Нигерии. Исторический опыт нигерийской юридической практики и обсуждаемые законодательные акты показывают, что по закону лицензию на юридическую практику в Нигерии может получить только человек[31]. Об этом говорит критический анализ требований для работы в адвокатуре, установленных разделом 4 Закона о практикующих юристах. Робот не может соответствовать этим критериям.

Кроме того, в положениях Закона о практикующих юристах и Закона о юридическом образовании (консолидации и т. д.) подчеркивается, что лицензию на юридическую практику в Нигерии может получить только физическое лицо. В настоящее время искусственный интеллект, в отличие от человека, не обладает качествами, которые, как правило, считаются необходимыми для признания личности в юридической сфере. К ним относятся сознание, эмоции и способность общаться способом, подобным человеческому языку. В результате большинство правовых систем не признают ИИ как лицо.

В решениях Верховного суда Нигерии много раз отмечалось, что человек является либо физическим, либо искусственным лицом (например, юридическим лицом)[32]. Робот не квалифицируется как физическое или искусственное лицо в соответствии

---

27 Section 4(1)(a) of the Legal Practitioners Act.

28 Там же. Section 4(2)(a); Section 1 of the Legal Practitioners (Amendment) Decree No. 1 of 1992.

29 Section 4 of the Legal Practitioners Act.

30 Section 18(4) of the Body of Benchers Regulations cited in Obi Okoye (n 47) 15.

31 Atoyebi, O. M. (2023, January 24). A Legal Perspective of the Robot Lawyer under the Nigerian Legal System. https://goo.su/QMZoz

32 The Administrator of the Estate of General Sani Abacha v Eke Spiff. (2009). 7 NWLR (Pt, 1139) 97 at P. 136 Para. E; Fawehinmi v Nigerian Bar Association (No. 2). (1989). 2 NWLR (Pt. 105) 558 at 595; Access Bank Plc v Agege Local Government & Anor. (2016). NGCA 35.

с нигерийской правовой системой. Однако, даже если бы робот был искусственным лицом, по Закону о практикующих юристах и Закону о юридическом образовании (консолидации и т. д.) искусственное лицо не может заниматься юридической практикой в Нигерии. Такие требования, как получение юридического образования в каком-либо признанном университете Нигерии или за рубежом, получение квалификационного сертификата от Совета по юридическому образованию после успешного окончания юридической школы и требование иметь хорошую репутацию, являются обязательными и указывают на то, что эти законы предусматривают физическое лицо.

Очевидно, что пока ИИ не будет облачен в форму личности и признан в соответствии с правовым режимом соответствующей юрисдикции, он не будет признан лицом, способным заниматься юридической практикой. Это вызывает растущий интерес к изучению возможности предоставления ИИ статуса личности. Поскольку технология искусственного интеллекта продолжает развиваться и становится все более совершенной, некоторые исследователи утверждают, что ИИ, возможно, заслуживал бы того же правового статуса, что и люди, если бы смог развить определенные характеристики, сходные с человеческими, такие как самосознание, эмоции и способность принимать решения.

Одним из аргументов в пользу наделения ИИ субъектностью является то, что это потенциально приведет к расширению доступа к юридическим услугам (Bryson, 2020). ИИ может быть запрограммирован для выполнения ряда юридических задач, таких как поиск материалов, составление документов и даже представление интересов клиентов в суде. Потенциально это может сделать юридические услуги более доступными для более широкого круга людей. Кроме того, наделение ИИ субъектностью может привести к более объективному и последовательному принятию юридических решений. Искусственный интеллект не подвержен тем предубеждениям, которые могут влиять на принятие решений человеком, и потенциально способен анализировать юридические данные и принимать решения более объективно и справедливо.

Однако существуют также опасения по поводу потенциальных последствий предоставления ИИ статуса личности. Например, если ИИ будет предоставлен тот же правовой статус, что и людям, он также может быть привлечен к юридической ответственности за свои действия (Bhattacharya, 2021). В связи с этим возникает вопрос, кто будет нести ответственность, если система искусственного интеллекта допустит ошибку, которая приведет к причинению вреда клиенту. Существуют также опасения по поводу этических последствий разрешения ИИ заниматься юридической практикой. Обучающиеся машины и искусственный интеллект, как правило, не способны сопереживать клиентам и понимать нюансы человеческих эмоций и поведения. Это может привести к тому, что машины будут предоставлять неадекватные юридические консультации или принимать решения, которые не отвечают наилучшим интересам их клиентов.

В том, чтобы позволить ИИ выполнять юридические задачи[33], есть потенциальные преимущества, однако существуют опасения по поводу возможных последствий в области юридической ответственности и принятия этических решений. В конечном

[33] Parnham, R., Sako, M., & Armour, J. (2021, December) AI-assisted lawtech: its impact on law firms. Oxford: University of Oxford. https://goo.su/zfB2Au

счете любое решение о наделении ИИ субъектностью должно приниматься после тщательной проработки этих вопросов и с учетом наилучших интересов клиентов, юристов и общества в целом (Gunkel & Wales, 2021). В заключение хотелось бы отметить, что вопрос о том, можно ли наделить ИИ статусом личности и разрешить ему заниматься юридической практикой, является сложным и поднимает ряд юридических и этических проблем. В настоящий момент нигерийское законодательство не позволяет субъектам, не имеющим статуса юридического лица, заниматься юридической практикой.

Заключение

Исследование показало, что глобализация и развитие технологий оказали значительное влияние на юридическую практику во всем мире, в том числе и в Нигерии. Технологии, особенно искусственный интеллект, положительно повлияли на юридическую практику. Однако два основных закона, регулирующих адвокатскую деятельность и юридическую практику в Нигерии, в целом не рассматривают робота как лицо, которое может заниматься юридической практикой. Робот не является физическим лицом, которому предоставляется право заниматься юридической практикой при выполнении квалификационных требований. Появление такого права зависит от внесения как в Закон о юридическом образовании (консолидации), так и в Закон о практикующих юристах поправок, которые предоставили бы такое право искусственному лицу, например роботу. Соответствующие положения обоих законодательных актов о требованиях к квалификации юриста могут быть пересмотрены, чтобы приспособить их к роботам, особенно человекоподобным. Как известно, такие роботы имеют сходство с людьми и обладают рядом человеческих черт. Примером может служить первый робот-гуманоид София, разработанный гонконгской компанией Hanson Robotics. София обладает высоким интеллектом, у нее есть кредитная карта, и правительство Саудовской Аравии предоставило ей полное подданство этой страны[34]. София стала первым роботом, у которого есть паспорт и который может имитировать 62 выражения лица человека[35]. Это первый в мире робот-амбассадор Программы ООН по развитию инноваций[36]. Однажды появившись, искусственный интеллект все больше входит в жизнь человека. Важность его для юридической практики трудно переоценить. Однако, хотя искусственный интеллект может быть использован для поиска юридических материалов, составления документов и т. д., выдача роботам лицензий для юридической практики пока невозможна.

Список литературы

Adegoke, O. A., Badejogbin, R. E., & Onoriode, M. E. (2014). *Law in Practice*, 12–13.

Aidonojie, P. A., Anne, O. O., & Oladele, O. O. (2020). An Empirical Study of the Relevance and Legal Challenges of an E-contract of Agreement in Nigeria. *Cogito Multidisciplinary Research Journal*, *12*(3), 170–192.

[34] Should Robots be Citizens? British Council. https://clck.ru/3FABkD

[35] Там же.

[36] Sophia. Hanson robotics. https://clck.ru/3FABmg

Aidonojie, P. A., Anne, O. O., Ikubanni, O. O., Oyebade, A. A, Oyedeji, A. I., & Okuonghae, N. (2021). The Challenges and Impact of Technological Advancement to the Legal Profession in Nigeria Given the Covid-19 Pandemic. *KIU Journal of Humanities*, *6*(4), 5–19.

Alarie, B. Niblett, A., & Yoon, A. H. (2016). Law in the Future. *University of Toronto Law Journal*, *66*(4), 423. https://doi.org/10.3138/utlj.4005

Alarie, B., Niblett, A., & Yoon, A. T. (2018). How Artificial Intelligence Will Affect the Practice of Law. *The University of Toronto Law Journal*, *68*, 106–124. https://doi.org/10.3138/utlj.2017-0052

Aniekwe, C. A. (2021). Legal Framework for The Use of Information and Communications Technology (ICT) in the Nigerian Justice System: A call For Review. *International Journal of Comparative Law and Legal Philosophy*, *1*(3), 125–132.

Antonio, S., & Estrella, T. A. (2020). Business and Labour Culture Changes in Digital Paradigm: Rise and Fall of Human Resources and The Emergence of Talent Development. *Cogito Multidisciplinary Research Journal*, *12*(3), 225–243.

Bhattacharya, S. (2021). Granting Legal Personhood to Artificial Intelligence Systems and Traditional Veil Piercing Concepts to Impose Liability. *Journal of Law and Legal Studies*, *2*(1), 1–10. https://doi.org/10.2139/ssrn.3857504

Bryson, J. J. (2020). AI and Legal Personhood. In K. Frankish, & W. M. Ramsey (Eds.), *Cambridge Handbook of Artificial Intelligence* (pp. 107–122). Cambridge University Press.

Castell, S. (2018). The Future Decisions of Robot Judge HHJ Arthur Ian Blockchain: Dread, Delight or Derision? *Computer Law & Security Review*, *34*(4), 739–753. https://doi.org/10.1016/j.clsr.2018.05.011

Contini, F. (2020). Artificial Intelligence and the Transformation of Humans, Law and Technology Interactions in Judicial Proceedings. *Law, Technology and Humans*, *2*(1), 4–18. https://doi.org/10.5204/lthj.v2i1.1478

Cooper, B. (2011). Judges in Jeopardy: Could IBM's Watson Beat Courts at Their Own Game? *Yale Law Journal*, *121*, 87.

D'Amato, A. (1976). Can/should Computers Replace Judges? *Georgia Law Review*, *11*, 1277–1301.

Dekker, F., Salomons, A., & Van der Waal, J. (2017). Fear of Robots at Work: The Role of Economic Self-interest. *Socio-Economic Review*, *15*(3), 539–562. https://doi.org/10.1093/ser/mwx005

Gallese, N.C. (2023). Legal Aspects of the Use of Artificial Intelligence in Telemedicine. *Journal of Digital Technology and Law*, *1*(2) 313–336. https://doi.org/10.21202/jdtl.2023.13

Garner, B. A. (2004). *Black's Law Dictionary* (9th Ed.). West Publishing Company, Dallas.

Giuffrida, I., Lederer, F., & Vermerys, N. (2018). A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law. *Case Western Reserve Law Review*, *68*(3), 747–781.

Gravett, W. H. (2020). Is the Dawn of the Robot Lawyer upon us? The Fourth Industrial Revolution and the Future of Lawyers. *Potchefstroom Electronic Law Journal*, *23*, 1–37. https://doi.org/10.17159/1727-3781/2020/v23i0a6794

Greenleaf, G., Mowbray, A., & Chung, P. (2018). Building Sustainable Free Legal Advisory Systems: Experiences From the History of AI & Law. *Computer Law & Security Review*, *34*(2), 314–326. https://doi.org/10.1016/j.clsr.2018.02.007

Gunkel, D. J., & Wales, J. J. (2021). Debate: what is personhood in the age of AI? *AI & Society*, *36*(2), 473–486. https://doi.org/10.1007/s00146-020-01129-1

Halima, D. (2016). Enhancing Justice Administration in Nigeria Through Information and Communications Technology. *The John Marshall Journal of Information Technology and Privacy Law*, *32*(2), 90.

Hu, T., & Lu, H. (2019). Study on the Influence of Artificial Intelligence on Legal Profession. *Advances in Economics, Business and Management Research*, *110*, 964–968. https://doi.org/10.2991/aebmr.k.191225.184

Huang, M.-H., & Rust, R. T. (2018). Artificial Intelligence in Service. *Journal of Service Research*, *21*(2), 155–172. https://doi.org/10.1177/1094670517752459

Ikubanni, O. O., & Aidonojie, P. A. (2021). The Legality of Virtual Marriage in Nigeria given the Covid-19 Pandemic Social Distancing: An X-ray of the Matrimonial Causes Act. Madonna University. *Nigeria Faculty of Law Law Journal*, 6(1), 123–129.

Ilegieuno, S., Chukwuani, O., & Adaralegbe, I. (2021). Artificial Intelligence and the Future of Law Practice in Nigeria. In R. Kumar, Y. Wang, T. Poongodi, & A. L. Imoize (Eds.), *Internet of Things, Artificial Intelligence and Blockchain Technology*. Springer, Cham. https://doi.org/10.1007/978-3-030-74150-1_14

Jiya, E. A., Samaila, A. N., & Surajo, Y. (2023). Artificial Intelligence and Technology for Improving the Efficiency of the Judiciary in Nigeria. *International Journal of Research in Applied Sciences*, *8*(5), 80–85. https://doi.org/10.51584/IJRIAS.2023.8509

Katyal, S. K. (2019). Private Accountability in the Age of Artificial Intelligence. *Ucla L. Rev*, *66*, 54.

Kioko, P., Booker, M., Chege, N., & Kimweli, P. (2022). The Adoption of Artificial Intelligence in Newsrooms in Kenya: a Multi-case Study. *European Scientific Journal*, *18*(22), 278. https://doi.org/10.19044/esj.2022.v18n22p278

McCorduck, P., & Cfe, C. (2004). *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence* (2nd ed.). A K Peters/CRC Press. https://doi.org/10.1201/9780429258985

McGinnis, J. O., & Pearce, R. G. (2014). The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, *82*(6), 3041–3066.

Obianyo, C. I., & Ater, S. V. (2022). A Critical Appraisal of the Legal Framework of Artificial Intelligence Governance in Nigeria. *Chukwuemeka Odumegwu Ojukwu University Journal of Private and Public Law*, *4*(1), 48–62.

Oguanmanam, C., & Pue, W. (2006). Lawyers' Professionalism, Colonialism, State Formation and National Life in Nigeria, 1900–1960: 'The Fighting Brigade of the People'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.953313

Oko, O. (1994). Contemporary Law Practice in Nigeria. *Journal of African Law*, *38*(2), 104. https://doi.org/10.1017/s0021855300005477

Okoye, O. (2015). *Law in Practice in Nigeria*. (2nd Ed.). Snaap Press Nigeria Ltd.

Orojo, J. O. (1979). *Conduct and Etiquette for Legal Practitioners*. London: Sweet and Maxwell.

Richard, M., & Solow-Niederman, A. (2019). Developing Artificially Intelligent Justice. *Stanford Technology Law Review*, *22*, 243–289.

Robinson, R. (2018). Artificial Intelligence: Its Importance, Challenges and Application in Nigeria. Direct Research *Journal of Engineering and Information Technology*, *5*(5), 36–41. https://doi.org/10.26765/DRJEIT.2018.4780

Sanctis, F. M. (2021). Artificial Intelligence and Innovation in Brazilian Justice. *International Annals of Criminology*, *59*(1), 1–10. https://doi.org/10.1017/cri.2021.4

Shaeeb, O., Adeola, I., & Akinola, O. B. (2023). Increase in Cases of Impersonation of Lawyers in Nigeria: Making Case for Reforms. *East African Journal of Law and Ethics*, *6*(1), 1–14. https://doi.org/10.37284/eajle.6.1.1118

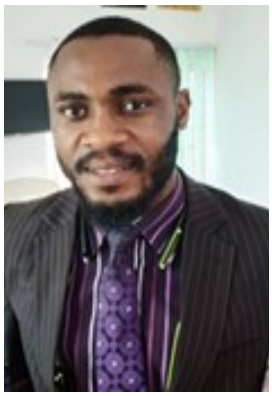
Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4), 1306.

Wang, R. (2020). Legal Technology in Contemporary USA and China. *Computer Law and Security Review*, *39*, 105459. https://doi.org/10.1016/j.clsr.2020.105459

Xu, Ni, & Wang, Kung-Jeng. (2019). Adopting a robot lawyer? The Extending Artificial Intelligence Robot Lawyer Technology Acceptance Model for Legal Industry by an Exploratory Study. *Journal of Management & Organization*, *27*(5), 1–19. https://doi.org/10.1017/jmo.2018.81

Xu, Z. (2022). Human Judges in the Era of Artificial Intelligence: Challenges and Opportunities. *Applied Artificial Intelligence*, *36*(1), 1025–1045. https://doi.org/10.1080/08839514.2021.2013652

Информация об авторах



Олувасейе Олувайоми Икубанни – преподаватель кафедры юриспруденции и государственного права факультета права, Университет Джозефа Айо Бабалолы
Адрес: Нигерия, штат Осун, г. Икеджи-Аракеджи, Акуре Илеша Роуд, 36-й километр
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0000-0003-0558-6373
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57336286500
Google Scholar ID: https://scholar.google.com/citations?user=xKujjJ0AAAAJ



Адереми Олубумни Ойебанджи – старший преподаватель кафедры юриспруденции и государственного права факультета права, Университет Джозефа Айо Бабалолы
Адрес: Нигерия, штат Осун, г. Икеджи-Аракеджи, Акуре Илеша Роуд, 36-й километр
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0009-0003-5907-7803
Google Scholar ID: https://scholar.google.com/citations?user=5267Z3cAAAAJ



Аладе Аденийи Ойебаде – преподаватель кафедры юриспруденции и государственного права факультета права, Университет Джозефа Айо Бабалолы
Адрес: Нигерия, штат Осун, г. Икеджи-Аракеджи, Акуре Илеша Роуд, 36-й километр
E-mail: aaoyebade@jabu.edu.ng
Google Scholar ID: https://scholar.google.com/citations?user=mcP5kO8AAAAJ

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

История статьи

Дата поступления – 11 февраля 2024 г.
Дата одобрения после рецензирования – 26 февраля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:349.2:004.8
EDN: https://elibrary.ru/fhnkjq
DOI: https://doi.org/10.21202/jdtl.2024.41

Legal Aspects of Granting Subjectivity to Artificial Intelligence: Prospects of Using Robots in Legal Practice in Nigeria

Oluwaseye O. Ikubanni ✉
Joseph Ayo Babalola University, Ikeji-Arakeji, Nigeria

Aderemi O. Oyebanji
Joseph Ayo Babalola University, Ikeji-Arakeji, Nigeria

Alade A. Oyebade
Joseph Ayo Babalola University, Ikeji-Arakeji, Nigeria

Keywords

artificial intelligence,
automation,
digital technologies,
justice,
law,
legal education,
legal practice,
online dispute settlement,
robot lawyer,
subjectivity

Abstract

Objective: to determine the potential and acceptability of using artificial intelligence in legal activities according to the Nigerian law.

Methods: the research is based on scientific analysis, as well as formal-legal, comparative-legal, historical-legal and systemic-functional methods. The scope of the research is represented by the norms of legislation, including expired normative legal acts, as well as scientific monographic and periodical literature.

Results: It was found that artificial intelligence and robot lawyers are inevitable innovations in the legal practice of many countries, including Nigeria. The use of these digital technologies has proven to be highly effective in activities related to the administration of justice, providing assistance in four areas of legal services: consulting and guidance, searching for materials, data analysis and forecasting the trial results. Technology greatly facilitates the work of lawyers, given the amount of legal services. In addition, the author show that while the use of artificial intelligence may generally be considered justified, the involvement of robot lawyers in legal practice in Nigeria faces

✉ Corresponding author
© Ikubanni O. O., Oyebanji A. O., Oyebade A. 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.

both legal and ethical barriers. The laws on legal education and legal practice in force in this country do not recognize robot lawyers as persons licensed to practice law in Nigeria. Robot lawyers must be given the status of a person before they can fully implement their potential in the legal practice of Nigeria.

Scientific novelty: this is primarily due to the formulation of a research task to determine the possibility of a robot acting as a practicing lawyer within the legal framework in Nigeria.

Practical significance: the conclusions formulated in the paper, namely, the inevitability of using artificial intelligence and robot lawyers in legal practice and the current legislation governing legal practice in Nigeria, will be useful when considering amendments to legislation in order to adapt it to the current level of digital technology development.

For citation

Ikubanni, O. O., Oyebanji, A. O., & Oyebade, A. A. (2024). Legal Aspects of Granting Subjectivity to Artificial Intelligence: Prospects of Using Robots in Legal Practice in Nigeria. *Journal of Digital Technologies and Law, 2*(4), 835–856. https://doi.org/10.21202/jdtl.2024.41

References

Adegoke, O. A., Badejogbin, R. E., & Onoriode, M. E. (2014). *Law in Practice*, 12–13.

Aidonojie, P. A., Anne, O. O., & Oladele, O. O. (2020). An Empirical Study of the Relevance and Legal Challenges of an E-contract of Agreement in Nigeria. *Cogito Multidisciplinary Research Journal*, *12*(3), 170–192.

Aidonojie, P. A., Anne, O. O., Ikubanni, O. O., Oyebade, A. A., Oyedeji, A. I, & Okuonghae, N. (2021). The Challenges and Impact of Technological Advancement to the Legal Profession in Nigeria Given the Covid-19 Pandemic. *KIU Journal of Humanities*, *6*(4), 5–19.

Alarie, B. Niblett, A., & Yoon, A. H. (2016). Law in the Future. *University of Toronto Law Journal*, *66*(4), 423. https://doi.org/10.3138/utlj.4005

Alarie, B., Niblett, A., & Yoon, A. T. (2018). How Artificial Intelligence Will Affect the Practice of Law. *The University of Toronto Law Journal*, *68*, 106–124. https://doi.org/10.3138/utlj.2017-0052

Aniekwe, C. A. (2021). Legal Framework for The Use of Information and Communications Technology (ICT) in the Nigerian Justice System: A call For Review. *International Journal of Comparative Law and Legal Philosophy*, *1*(3), 125–132.

Antonio, S., & Estrella, T. A. (2020). Business and Labour Culture Changes in Digital Paradigm: Rise and Fall of Human Resources and The Emergence of Talent Development. *Cogito Multidisciplinary Research Journal*, *12*(3), 225–243.

Bhattacharya, S. (2021). Granting Legal Personhood to Artificial Intelligence Systems and Traditional Veil Piercing Concepts to Impose Liability. *Journal of Law and Legal Studies*, *2*(1), 1–10. https://doi.org/10.2139/ssrn.3857504

Bryson, J. J. (2020). AI and Legal Personhood. In K. Frankish, & W. M. Ramsey (Eds.), *Cambridge Handbook of Artificial Intelligence* (pp. 107–122). Cambridge University Press.

Castell, S. (2018). The Future Decisions of Robot Judge HHJ Arthur Ian Blockchain: Dread, Delight or Derision? *Computer Law & Security Review*, *34*(4), 739–753. https://doi.org/10.1016/j.clsr.2018.05.011

Contini, F. (2020). Artificial Intelligence and the Transformation of Humans, Law and Technology Interactions in Judicial Proceedings. *Law, Technology and Humans*, *2*(1), 4–18. https://doi.org/10.5204/lthj.v2i1.1478

Cooper, B. (2011). Judges in Jeopardy: Could IBM's Watson Beat Courts at Their Own Game? *Yale Law Journal*, *121*, 87.

D'Amato, A. (1976). Can/should Computers Replace Judges? *Georgia Law Review*, *11*, 1277–1301.

Dekker, F., Salomons, A., & Van der Waal, J. (2017). Fear of Robots at Work: The Role of Economic Self-interest. *Socio-Economic Review*, *15*(3), 539–562. https://doi.org/10.1093/ser/mwx005

Gallese, N.C. (2023). Legal Aspects of the Use of Artificial Intelligence in Telemedicine. *Journal of Digital Technology and Law*, *1*(2) 313–336. https://doi.org/10.21202/jdtl.2023.13

Garner, B. A. (2004). *Black's Law Dictionary* (9th Ed.). West Publishing Company, Dallas.

Giuffrida, I., Lederer, F., & Vermerys, N. (2018). A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law. *Case Western Reserve Law Review*, *68*(3), 747–781.

Gravett, W. H. (2020). Is the Dawn of the Robot Lawyer upon us? The Fourth Industrial Revolution and the Future of Lawyers. *Potchefstroom Electronic Law Journal*, *23*, 1–37. https://doi.org/10.17159/1727-3781/2020/v23i0a6794

Greenleaf, G., Mowbray, A., & Chung, P. (2018). Building Sustainable Free Legal Advisory Systems: Experiences From the History of AI & Law. *Computer Law & Security Review*, *34*(2), 314–326. https://doi.org/10.1016/j.clsr.2018.02.007

Gunkel, D. J., & Wales, J. J. (2021). Debate: what is personhood in the age of AI? *AI & Society*, *36*(2), 473–486. https://doi.org/10.1007/s00146-020-01129-1

Halima, D. (2016). Enhancing Justice Administration in Nigeria Through Information and Communications Technology. *The John Marshall Journal of Information Technology and Privacy Law*, *32*(2), 90.

Hu, T., & Lu, H. (2019). Study on the Influence of Artificial Intelligence on Legal Profession. *Advances in Economics, Business and Management Research*, *110*, 964–968. https://doi.org/10.2991/aebmr.k.191225.184

Huang, M.-H., & Rust, R. T. (2018). Artificial Intelligence in Service. *Journal of Service Research*, *21*(2), 155–172. https://doi.org/10.1177/1094670517752459

Ikubanni, O. O., & Aidonojie, P. A. (2021). The Legality of Virtual Marriage in Nigeria given the Covid-19 Pandemic Social Distancing: An X-ray of the Matrimonial Causes Act. Madonna University. *Nigeria Faculty of Law Law Journal*, 6(1), 123–129.

Ilegieuno, S., Chukwuani, O., & Adaralegbe, I. (2021). Artificial Intelligence and the Future of Law Practice in Nigeria. In R. Kumar, Y. Wang, T. Poongodi, & A. L. Imoize (Eds.), *Internet of Things, Artificial Intelligence and Blockchain Technology*. Springer, Cham. https://doi.org/10.1007/978-3-030-74150-1_14

Jiya, E. A., Samaila, A. N., & Surajo, Y. (2023). Artificial Intelligence and Technology for Improving the Efficiency of the Judiciary in Nigeria. *International Journal of Research in Applied Sciences*, *8*(5), 80–85. https://doi.org/10.51584/IJRIAS.2023.8509

Katyal, S. K. (2019). Private Accountability in the Age of Artificial Intelligence. *Ucla L. Rev*, *66*, 54.

Kioko, P., Booker, M., Chege, N., & Kimweli, P. (2022). The Adoption of Artificial Intelligence in Newsrooms in Kenya: a Multi-case Study. *European Scientific Journal*, *18*(22), 278. https://doi.org/10.19044/esj.2022.v18n22p278

McCorduck, P., & Cfe, C. (2004). *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence* (2nd ed.). A K Peters/CRC Press. https://doi.org/10.1201/9780429258985

McGinnis, J. O., & Pearce, R. G. (2014). The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, *82*(6), 3041–3066.

Obianyo, C. I., & Ater, S. V. (2022). A Critical Appraisal of the Legal Framework of Artificial Intelligence Governance in Nigeria. *Chukwuemeka Odumegwu Ojukwu University Journal of Private and Public Law*, *4*(1), 48–62.

Oguanmanam, C., & Pue, W. (2006). Lawyers' Professionalism, Colonialism, State Formation and National Life in Nigeria, 1900–1960: 'The Fighting Brigade of the People'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.953313

Oko, O. (1994). Contemporary Law Practice in Nigeria. *Journal of African Law*, *38*(2), 104. https://doi.org/10.1017/s0021855300005477

Okoye, O. (2015). *Law in Practice in Nigeria*. (2nd Ed.). Snaap Press Nigeria Ltd.

Orojo, J. O. (1979). *Conduct and Etiquette for Legal Practitioners*. London: Sweet and Maxwell.

Richard, M., & Solow-Niederman, A. (2019). Developing Artificially Intelligent Justice. *Stanford Technology Law Review*, *22*, 243–289.

Robinson, R. (2018). Artificial Intelligence: Its Importance, Challenges and Application in Nigeria. Direct Research *Journal of Engineering and Information Technology*, *5*(5), 36–41. https://doi.org/10.26765/DRJEIT.2018.4780

Sanctis, F. M. (2021). Artificial Intelligence and Innovation in Brazilian Justice. *International Annals of Criminology*, *59*(1), 1–10. https://doi.org/10.1017/cri.2021.4

Shaeeb, O., Adeola, I., & Akinola, O. B. (2023). Increase in Cases of Impersonation of Lawyers in Nigeria: Making Case for Reforms. *East African Journal of Law and Ethics*, *6*(1), 1–14. https://doi.org/10.37284/eajle.6.1.1118

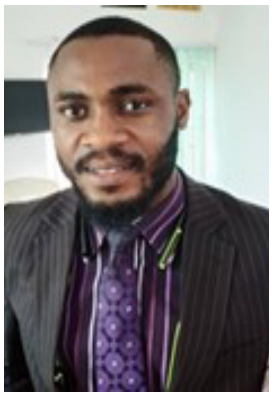
Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4), 1306.

Wang, R. (2020). Legal Technology in Contemporary USA and China. *Computer Law and Security Review*, *39*, 105459. https://doi.org/10.1016/j.clsr.2020.105459

Xu, Ni, & Wang, Kung-Jeng. (2019). Adopting a robot lawyer? The Extending Artificial Intelligence Robot Lawyer Technology Acceptance Model for Legal Industry by an Exploratory Study. *Journal of Management & Organization*, *27*(5), 1–19. https://doi.org/10.1017/jmo.2018.81

Xu, Z. (2022). Human Judges in the Era of Artificial Intelligence: Challenges and Opportunities. *Applied Artificial Intelligence*, *36*(1), 1025–1045. https://doi.org/10.1080/08839514.2021.2013652

Authors information



Oluwaseye Oluwayomi Ikubanni – Lecturer, Department of Jurisprudence and Public Law, College of Law, Joseph Ayo Babalola University
Address: Kilometre 36, Akure Ilesha Road, Ikeji-Arakeji, Osun State, Nigeria
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0000-0003-0558-6373
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57336286500
Google Scholar ID: https://scholar.google.com/citations?user=xKujjJ0AAAAJ



Aderemi Olubunmi Oyebanji – Senior Lecturer, Department of Jurisprudence and Public Law, College of Law, Joseph Ayo Babalola University
Address: Kilometre 36, Akure Ilesha Road, Ikeji-Arakeji, Osun State, Nigeria
E-mail: ooikubanni@jabu.edu.ng
ORCID ID: https://orcid.org/0009-0003-5907-7803
Google Scholar ID: https://scholar.google.com/citations?user=5267Z3cAAAAJ



Alade Adeniyi Oyebade – Lecturer, Department of Jurisprudence and Public Law, College of Law, Joseph Ayo Babalola University
Address: Kilometre 36, Akure Ilesha Road, Ikeji-Arakeji, Osun State, Nigeria
E-mail: aaoyebade@jabu.edu.ng
Google Scholar ID: https://scholar.google.com/citations?user=mcP5kO8AAAAJ

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 – February 11, 2024
Date of approval – February 26, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:347.1:004.8
EDN: https://elibrary.ru/fnenmx
DOI: https://doi.org/10.21202/jdtl.2024.42

Возникновение аватаров на основе искусственного интеллекта: юридическая субъектность, права и обязанности в развивающейся метавселенной

Бен Честер Чонг

Сингапурский университет общественных наук, Сингапур, Сингапур
Кембриджский университет, Кембридж, Великобритания

Ключевые слова

большие языковые модели,
ИИ-аватар,
интеллектуальная собственность,
искусственный интеллект,
метавселенная,
ответственность,
право,
правосубъектность,
цифровые технологии,
юридическое лицо

Аннотация

Цель: определить правовые последствия развития автономных и творческих аватаров на основе искусственного интеллекта и сформировать направления дискурса об ответственном управлении технологиями искусственного интеллекта в метавселенной на основе активных междисциплинарных подходов.

Методы: основу исследования составляет доктринальный юридический подход, позволивший представить перспективный анализ правового ландшафта в сфере ИИ-аватаров в метавселенной и определить четыре ключевых тематических направления, по которым проводится исследование: эволюция ИИ-аватаров и влияние метавселенной, применимость правовой субъектности, ответственность за автономные действия и проблемы ИИ-аватаров в сфере творчества, связанные с аспектами интеллектуальной собственности и неприкосновенности частной жизни.

Результаты: в работе представлены и проанализированы прогнозные сценарии развития ИИ-аватаров, максимально усиливающих свое влияние в пространстве метавселенной. Отмечается, что с появлением аватаров на основе искусственного интеллекта в метавселенной связана постановка сложных правовых, этических, философских и социальных вопросов, требующих неотложных решений. Рассмотрено потенциальное влияние растущей сложности ИИ-аватаров на правовые подходы. По мере того как аватары становятся все более автономными, возникают вопросы об их правовом статусе, правах, обязанностях, рисках и пользе для человека и общества. Анализируются преимущества и недостатки наделения ИИ-аватаров правовым статусом юридических лиц, а также применения к последствиям их действий концепции распределенной ответственности. Особое внимание уделено возможному в будущем доминированию сверхразумных аватаров на основе искусственного интеллекта в метавселенной с учетом существующих рисков и потребностей в сфере управления.

© Чонг Б. Ч., 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 на примере междисциплинарного анализа эволюции ИИ-аватаров представлен новый взгляд на проблему правосубъектности в метавселенной, направленный на достижение баланса между трансформационным потенциалом и защитой прав и благополучия человека посредством совместных усилий по созданию правовых и этических норм, ставящих во главу угла безопасность и согласованность технологий искусственного интеллекта, задействованных в процессах, происходящих в метавселенной.

Практическая значимость: полученные в процессе проведенного исследования выводы и предлагаемые решения правовых проблем субъектности и ответственности могут стать основой для пересмотра концепции правосубъектности, разработки надежных механизмов ответственности и подотчетности, а также обеспечения защиты прав и ценностей человека перед лицом все более мощных сущностей на основе искусственного интеллекта, что сопряжено с формированием и совершенствованием правового ландшафта управления процессами и преодоления рисков в социально ориентированной и инклюзивной экосистеме метавселенной.

Для цитирования

Чонг, Б. Ч. (2024). Возникновение аватаров на основе искусственного интеллекта: юридическая субъектность, права и обязанности в развивающейся метавселенной. *Journal of Digital Technologies and Law*, *2*(4), 857–885. https://doi.org/10.21202/jdtl.2024.42

Содержание

Введение
1. Обзор литературы в сфере правовых и социальных последствий появления метавселенной
2. Эволюция аватаров на основе искусственного интеллекта
3. Новый взгляд на проблему правосубъектности ИИ-аватаров
4. Вопросы ответственности автономных ИИ-аватаров
5. Специфические проблемы творческих ИИ-аватаров
6. Взгляд в будущее: будет ли искусственный интеллект управлять метавселенной
Заключение
Список литературы

Введение

Концепция аватаров в метавселенной и потенциальные правовые проблемы и средства защиты, которые могут при этом возникнуть, были впервые рассмотрены в основополагающей статье (Cheong, 2022), где проводились также параллели с принципами корпоративного права. В статье обсуждалась необходимость защиты прав аватаров, возможность предоставления им отдельной правосубъектности и потенциальные последствия участия аватаров в таких вредоносных действиях, как мошенничество, кража личности, диффамация и другие преступления. Автор затронул также концепцию отмены корпоративного иммунитета в определенных обстоятельствах с целью возложения ответственности на лиц, скрывающихся за аватарами.

Со времени публикации этой статьи произошел значительный прогресс в области искусственного интеллекта (далее – ИИ), особенно в связи с появлением технологии больших языковых моделей (large language model, LLM) и разработкой новых моделей ИИ. Такие компании, как Nvidia, добились значительных успехов в создании мощных инструментов и платформ ИИ, которые формируют будущее метавселенной (Soliman et al., 2024). Эти достижения породили новые вопросы и проблемы, касающиеся правового статуса и последствий использования аватаров на основе ИИ в метавселенной. Быстрая эволюция технологий ИИ привела к появлению все более сложных и автономных ИИ-аватаров, способных вступать в сложные взаимодействия и принимать решения в метавселенной (McStay, 2023). По мере того как эти аватары ИИ становятся все более реалистичными и получают все новые способности, начинают стираться границы между взаимодействиями человека и ИИ в метавселенной. Это поднимает важные вопросы о правовом статусе ИИ-аватаров и о том, в какой степени они должны быть наделены правами и обязанностями. Кроме того, развитие аватаров, управляемых искусственным интеллектом, породило новые проблемы с точки зрения ответственности и подотчетности. Поскольку автономность ИИ-аватаров повышается, становится все сложнее возложить ответственность за их действия на людей или компании, которые за ними стоят. Это может привести к появлению «серой зоны» в законодательстве, когда вредоносные действия аватаров ИИ не получают реакции и не существует четких механизмов для возмещения ущерба пострадавшим.

В свете этих событий крайне важно пересмотреть правовую базу в сфере аватаров в метавселенной и возможности ее изменения с учетом специфических проблем, создаваемых ИИ-аватарами. Цель данной статьи – внести вклад в этот важный дискурс, изучив правовые последствия развития аватаров на основе ИИ по мере их усложнения и повышения автономности. В статье предложен углубленный анализ юридических последствий появления ИИ-аватаров в метавселенной, опираясь на положения работы (Cheong, 2022). Рассмотрено потенциальное влияние растущей сложности ИИ-аватаров на правовые подходы, предложенные в указанной работе; изучена потенциальная потребность в новых правовых подходах для решения уникальных проблем, создаваемых ИИ-аватарами. Используя доктринальный юридический подход, автор представляет перспективный анализ правового ландшафта в сфере ИИ-аватаров в метавселенной. Рассмотрены соответствующие правовые принципы и прецеденты, а также гипотетические сценарии будущего, в которых ИИ-аватары могут стать еще более продвинутыми и усилить свое влияние в пространстве метавселенной.

Представленный анализ продолжает дискуссию о правовых последствиях ИИ и метавселенной, а также предлагает ряд идей и рекомендаций для законодателей, юристов-практиков и других заинтересованных сторон, которые должны ориентироваться в этом быстро меняющемся ландшафте. В конечном итоге необходимо обеспечить, чтобы правовые нормы, касающиеся аватаров на основе ИИ в пространстве метавселенной, были надежными, адаптируемыми и способными защитить права и интересы всех вовлеченных сторон.

1. Обзор литературы в сфере правовых и социальных последствий появления метавселенной

Такая стремительно развивающаяся цифровая инновация, как метавселенная, вызывает значительные научные дискуссии, особенно по поводу правовых и социальных последствий ее появления. В данном обзоре мы рассмотрим

последние публикации начиная с 2021 г. и выделим ключевые темы и аргументы, связанные с влиянием метавселенной на правовые и общественные нормы, в частности неприкосновенность частной жизни.

Одной из главных проблем в исследовании метавселенной является юридический статус и права аватаров. В работе (Cheong, 2022) исследуется концепция наделения аватаров правосубъектностью и проводятся параллели с принципами корпоративного права. Автор утверждает, что, поскольку аватары занимаются такими видами деятельности, как мошенничество, кража личных данных и диффамация, существует острая необходимость в защите их прав и привлечении к ответственности лиц, стоящих за этими аватарами. Предлагается концепция отмены иммунитета и возложения ответственности на реальных лиц, контролирующих аватаров, по аналогии с тем, как концепция отмены корпоративного иммунитета применяется для решения проблемы корпоративных нарушений (Cheong, 2022). Появление метавселенной требует новых правовых рамок для решения специфических проблем в ней. Для регулирования социальных отношений в метавселенной Kostenko с соавторами (Kostenko et al., 2023) выступают за создание всеобъемлющей электронной юрисдикции, включая особые кодексы метавселенной. В этой работе подчеркивается, что для устойчивого развития метавселенной необходимы четкие правовые границы, а ученым предлагается спрогнозировать и очертить будущие контуры правовых полномочий для виртуальных сред (Kostenko et al., 2023). В другой работе (Kostenko et al., 2022) обсуждается эволюция правового регулирования от Web 1.0 к Web 3.0 и подчеркивается неадекватность существующих законов в отношении виртуальной среды и среды дополненной реальности. Авторы выступают за применение принципов аналогового права в виртуальной среде, таких как установление права собственности и ответственности за виртуальные активы, с целью снижения правовой неопределенности (Kostenko et al., 2022).

Экономическая деятельность в метавселенной, особенно сделки с виртуальными товарами и услугами, влечет за собой значительные правовые последствия. В работе Yayman (2023) рассматриваются проблемы налогообложения операций в виртуальном мире и сравниваются налоговые нормы Турции и США. По мнению ученого, виртуальные миры все больше отражают реальную экономическую деятельность, что требует согласованной налоговой политики для учета доходов, получаемых в этих средах (Yayman, 2023). Кроме того, конфиденциальность и защита данных становятся важнейшими проблемами, по мере того как метавселенная все глубже интегрируется в повседневную жизнь. Исследование McStay (2023) рассматривает проблемы защиты информации в области биометрических и эмоциональных данных, собираемых в метавселенной. При описании этих рисков автор вводит понятия «физика надзора» и «виртуальное реалистическое управление». Эти концепции подчеркивают необходимость введения надежных мер по защите данных, которые учитывали бы уникальные возможности для надзора в метавселенной (McStay, 2023). Еще одна важная область исследований – это влияние метавселенной на социальные отношения и трудовое законодательство. Работа Guastavino и Mangan (2023) посвящена возможному влиянию метавселенной на производственные отношения, причем основное внимание уделяется защите данных работников. Авторы подчеркивают необходимость междисциплинарных исследований для разработки правовых рамок, обеспечивающих определенность и защиту прав работников в метавселенной (Guastavino & Mangan, 2023).

Философские и экономические аспекты метавселенной глубоко изучены в работе (Garon, 2022) на примере конкурирующих взглядов сторонников Web3 и традиционных интернет-компаний. Подчеркивается, что метавселенная может кардинально изменить интернет-торговлю и социальные взаимодействия, однако управление этой цифровой инновацией требует перспективной правовой и экономической политики (Garon, 2022). Заглядывая вперед, ученые рассматривают гипотетические сценарии будущего, чтобы управлять текущими правовыми и политическими реалиями. Так, в работе Wu и Zhang (2023) обсуждаются технологии защиты конфиденциальности и аутентификации, необходимые для управления цифровой идентичностью в метавселенной. Утверждается, что передача данных о частной жизни и проецирование эмоций имеют решающее значение для субъектности аватаров, что создает серьезные проблемы для обеспечения безопасности частной жизни (Wu & Zhang, 2023). Исследование Qin с соавторами (Qin et al., 2022) подчеркивает необходимость создания международной правовой базы для решения проблем идентификации, преступлений и правоприменения в метавселенной. Показано, что для эффективного расследования преступлений и демократического управления в виртуальном пространстве необходимо сотрудничество между странами (Qin et al., 2022). Работа Sun с соавторами (Sun et al., 2022) дает исчерпывающий обзор вопросов безопасности и конфиденциальности в метавселенной, а также предлагает ряд решений и направлений дальнейших исследований этих проблем. Авторы говорят о необходимости надежных мер безопасности для защиты пользовательских данных и обеспечения безопасного взаимодействия в виртуальной среде (Sun et al., 2022).

Таким образом, современные исследования в области метавселенной подчеркивают настоятельную необходимость создания новых правовых рамок и подходов для решения ее специфических проблем. Ученые закладывают основу для всестороннего понимания правовых и социальных последствий появления этой инновации, рассматривая весь спектр вопросов от защиты прав аватаров до регулирования экономической деятельности и обеспечения конфиденциальности данных. По мере развития метавселенной будут необходимы постоянные исследования и обсуждения для того, чтобы ее развитие шло во благо всех заинтересованных сторон.

2. Эволюция аватаров на основе искусственного интеллекта

Стремительное развитие искусственного интеллекта коренным образом изменило концепцию аватаров в метавселенной, превратив их из простых статичных представлений в очень сложные автономные сущности, способные вступать в сложные взаимодействия и принимать решения. Этой эволюции способствовала интеграция передовых технологий ИИ, таких как большие языковые модели (large language models, LLM), методы обработки естественного языка (natural language processing, NLP) и передовые алгоритмы машинного обучения, которые наделили аватары на основе ИИ беспрецедентным уровнем разумности, адаптивности и реалистичности (Bender et al., 2021; Seymour et al., 2018).

Одной из самых значительных вех в развитии ИИ-аватаров стала разработка больших языковых моделей, которая произвела революцию в том, как аватары могут общаться и взаимодействовать с пользователями в метавселенной. Большие

языковые модели – это системы ИИ, обученные на огромных объемах текстовых данных, что позволяет им генерировать человекоподобные ответы и вступать в контекстуально релевантное общение (Bender et al., 2021). Интеграция больших языковых моделей в аватары на основе ИИ позволила создать очень убедительных интерактивных агентов, способных понимать запросы пользователей и отвечать на них достаточно естественным и интуитивным образом (Kim & Im, 2023). Это открыло новые возможности для использования аватаров ИИ в качестве интеллектуальных помощников, гидов и компаньонов в метавселенной, предлагающих персонализированную поддержку и обогащающих пользовательский опыт (Bayoudh et al., 2022).

Кроме того, появление передовых технологий компьютерного зрения и машинного обучения открыло путь к созданию фотореалистичных аватаров, сгенерированных ИИ, которые стирают границы между виртуальным и физическим мирами (Seymour et al., 2018). Такие проекты, как MetaHuman Creator от компании Epic Games, демонстрируют невероятный потенциал этих технологий, позволяя создавать аватары с реалистичными мимикой, языком тела и эмоциональными реакциями[1]. Становясь все более неотличимыми от реальных людей, эти аватары поднимают глубокие вопросы о природе идентичности, подлинности и социального взаимодействия в метавселенной (Zimmermann et al., 2023).

Эволюция аватаров на основе ИИ также определяется растущей значимостью воплощенного познания и признанием той роли, которую физическое воплощение играет в формировании поведения и взаимодействия агента (Wolfert et al., 2022). По мере усложнения этой технологии происходит сдвиг в сторону разработки аватаров, которые не только интеллектуальны, но и способны демонстрировать реалистичное физическое поведение и реакции (Nordmoen et al., 2021). В результате появились аватары, которые могут перемещаться и взаимодействовать с виртуальной средой более естественным и интуитивным образом, что еще больше размывает границы между виртуальностью и реальностью (Duan et al., 2021).

По мере развития и повышения автономности аватары на основе ИИ берут на себя все более сложные функции в метавселенной, начиная с деятельности виртуальных блогеров и создателей контента и заканчивая ролью лиц, принимающих решения, и проводников перемен (Shirado & Christakis, 2017). В этой связи возникают важные вопросы о правовых и этических последствиях их присутствия в метавселенной, особенно с точки зрения их потенциального влияния на человеческую субъектность, приватность и подотчетность (De Streel et al., 2020). Поскольку такие аватары становятся все более сложными и автономными, крайне важно создать надежные механизмы управления и этические принципы, чтобы гарантировать, что их разработка и внедрение соответствуют общественным ценностям и способствуют благополучию как пользователей-людей, так и всей экосистемы метавселенной (Erdélyi & Goldsmith, 2018; Kuzminykh & Rintel, 2020).

Эволюция аватаров на основе ИИ представляет собой смену парадигмы в том, как мы концептуализируем виртуальные сущности и взаимодействуем с ними, бросая вызов традиционным представлениям об идентичности, субъектности

[1] Epic Games. (2024). MetaHuman Creator: High-fidelity digital humans made easy. Unreal Engine. https://clck.ru/3EiqSA

и социальных взаимодействиях. По мере того как эти аватары продолжают развиваться и все глубже интегрироваться в ткань метавселенной, необходимо проводить постоянные междисциплинарные исследования и обсуждения, чтобы понять далеко идущие последствия их развития и обеспечить ответственный и этичный характер их эволюции (De Gregorio, 2021). Активно рассматривая проблемы и возможности, связанные с появлением аватаров на основе ИИ, мы сможем создать метавселенную, которая будет не только технологически продвинутой, но и социально ответственной и инклюзивной.

3. Новый взгляд на проблему правосубъектности ИИ-аватаров

Поскольку аватары на основе ИИ становятся более сложными, автономными и способными участвовать в сложных процессах принятия решений, все актуальнее становится вопрос об их правовом статусе и субъектности. Традиционные правовые нормы, построенные вокруг концепции человеческой деятельности и ответственности, все больше подвергаются сомнению в связи с появлением субъектов ИИ, которые могут действовать независимо и оказывать значительное влияние на виртуальный и реальный миры (Gordon, 2022). В данном разделе мы рассмотрим последствия наделения ИИ-аватаров правосубъектностью, опираясь на существующую литературу о правосубъектности искусственного интеллекта и изучая потенциальные преимущества, риски и проблемы, связанные с распространением юридических прав и обязанностей на эти виртуальные сущности.

Концепция правосубъектности – это фундаментальная конструкция в праве, означающая признание кого-либо или что-либо в качестве субъекта юридических прав и обязанностей (Kurki, 2019; Cheong, 2021). Исторически правовой статус предоставлялся не только физическим лицам, но и искусственным образованиям, таким как корпорации, которые рассматриваются как «юридические лица» для целей заключения договоров, владения имуществом и ответственности (van den Hoven van Genderen, 2018; Cheong, 2021). Распространение статуса юридического лица на ИИ-аватары стало бы значительным шагом вперед в правовом признании искусственного интеллекта, так как они получили бы форму юридического лица и автономию, что может иметь далеко идущие последствия для их роли в метавселенной и вне ее (Stein, 2020).

Один из главных аргументов в пользу наделения ИИ-аватаров статусом юридического лица заключается в том, что это обеспечит четкую основу для возложения на них прав и обязанностей, позволяя им полноценно участвовать в правовой и экономической системах метавселенной (Militsyna, 2022). После признания таких аватаров юридическими лицами они смогут заключать договоры, владеть виртуальной собственностью и нести ответственность за свои действия, что обеспечит определенную степень правовой определенности и предсказуемости, необходимую для нормального функционирования экономики метавселенной (Lehdonvirta, 2024). Более того, наделение ИИ-аватаров статусом юридического лица поможет обеспечить как их ответственность за свои действия, так и защиту прав пользователей-людей при взаимодействии с этими виртуальными агентами (Turner & Schneider, 2020). Аватары на основе ИИ становятся все более сложными и способными принимать решения, имеющие последствия в реальном мире. Поэтому должны существовать четкие правовые механизмы, гарантирующие, что на них распространяется

верховенство закона и что любой вред, причиненный их действиями, может быть возмещен (De Streel et al., 2020; Cheong, 2022).

Однако идея распространения правосубъектности на ИИ-аватары не лишена проблем и сталкивается с критикой. Одно из главных возражений против такого подхода заключается в том, что он может привести к размыванию концепции юридического лица, стиранию границ между человеческими и искусственными агентами и потенциальному подрыву морально-философских основ прав и достоинства человека (Bryson et al., 2017). По мнению некоторых ученых, наделение субъектов ИИ статусом юридического лица может привести к ситуации, когда права и интересы искусственных агентов станут приоритетнее человеческих, что приведет к своего рода «исключительности ИИ», которая может иметь опасные последствия (Gunkel, 2024). Еще одной проблемой, связанной с предоставлением ИИ-аватарам статуса юридического лица, является вопрос о том, как определить уровень их автономии и способности принимать решения. Некоторые такие аватары очень сложны и способны работать самостоятельно, другие более ограничены в своих возможностях и в значительной степени зависят от участия и контроля со стороны человека (Samek et al., 2021). Установление четких критериев оценки правового статуса таких аватаров необходимо для того, чтобы предоставляемые им права и обязанности соответствовали их реальным возможностям и потенциальному влиянию (Chopra & White, 2011). Кроме того, правовая субъектность ИИ-аватаров поставит сложные вопросы об ответственности и подотчетности в случае причинения вреда или совершения противоправных действий. Если аватар на основе ИИ наносит ущерб или занимается незаконной деятельностью, кто должен нести ответственность – сам аватар, пользователь, который его создал или применил или компания, разработавшая базовую технологию? (Lemley & Casey, 2019; Cheong, 2022). Решение этих вопросов потребует тщательного учета интересов и ответственности всех вовлеченных сторон, а также разработки новых правовых доктрин и механизмов для решения уникальных проблем, создаваемых агентами ИИ (Buiten, 2019).

Одним из возможных подходов к решению этих проблем является разработка «многоуровневой» системы правосубъектности для ИИ-аватаров, которая будет предоставлять различные уровни прав и обязанностей в зависимости от сложности и автономности данной сущности (Hildebrandt, 2020). Согласно этому подходу, «слабые» аватары на основе ИИ с ограниченными возможностями принятия решений получат базовую форму правосубъектности с ограниченными правами и обязанностями, в то время как более продвинутые – «сильные» – ИИ-аватары получат правовой статус более высокого уровня с соответственно большими правами и обязанностями (Pagallo, 2018; Cheong, 2022). Другой подход состоит в разработке «гибридных» правовых систем, сочетающих элементы правовой субъектности с другими формами правовой защиты и регулирования (Benhamou & Ferland, 2021). Это может повлечь за собой создание специальных правовых режимов для ИИ-аватаров, наделяя их определенными правами и обязанностями, но также предусматривая особые нормы и механизмы надзора для обеспечения их безопасной и ответственной работы (Fosch-Villaronga & Mahler, 2021).

В итоге вопрос о правосубъектности ИИ-аватаров требует постоянных исследований, обсуждений и экспериментов, поскольку эти технологии продолжают развиваться и становятся все более интегрированными в ткань метавселенной. Хотя распространение правового статуса лица на ИИ-аватаров может обеспечить

определенную юридическую ясность и предсказуемость, оно также поднимает значительные этические, философские и практические проблемы, которые необходимо будет тщательно изучить (Chatzimichali et al., 2020). Поэтому важно, чтобы разработка правовых рамок для ИИ-аватаров основывалась на междисциплинарном подходе, объединяющем экспертов в области права, этики, информатики и других соответствующих областей для решения сложных проблем, создаваемых этими технологиями (Gellers, 2021). Это потребует постоянного сотрудничества и диалога между законодателями, исследователями, заинтересованными сторонами индустрии и представителями широкой общественности. Юридический статус аватаров на основе ИИ должен способствовать инновациям, не нарушать права человека и обеспечивать ответственное и благотворное развитие этих технологий в метавселенной и за ее пределами (Mäntymäki et al., 2022).

4. Вопросы ответственности автономных ИИ-аватаров

По мере повышения автономности ИИ-аватаров и их способности принимать решения, имеющие последствия в реальном мире, остро встает вопрос об ответственности за их действия. Появление сущностей на основе ИИ, которые могут действовать независимо и принимать решения, не контролируемые напрямую их создателями или пользователями, размывает традиционные правовые рамки распределения ответственности, основанные на концепции деятельности и ответственности человека (Giuffrida, 2019). В этом разделе работы мы рассмотрим сложную область ответственности автономных ИИ-аватаров, возможные правовые теории и механизмы возложения ответственности и возмещения вреда, причиненного этими сущностями.

Одной из основных проблем при возложении ответственности за действия автономных ИИ-аватаров является сложность установления четкой причинно-следственной связи между процессом принятия решений аватаром и наступившим вредом (Lemley & Casey, 2019). В отличие от традиционных программных систем, которые действуют по заранее установленным правилам и инструкциям, автономные аватары на основе ИИ призваны обучаться через взаимодействие с окружающей средой и принимать решения согласно своим собственным внутренним представлениям и целям (Russell & Norvig, 2021). Это означает, что конкретные действия, предпринимаемые аватаром на основе ИИ в той или иной ситуации, могут быть не заложены непосредственно его создателями или пользователями, но возникать в результате сложного взаимодействия алгоритмов обучения аватара, обучающих данных и условий среды (Selbst, 2020). В свете этой сложности некоторые ученые утверждают, что ответственность за действия автономных ИИ-аватаров должна быть аналогична подходу, принятому в законодательстве об ответственности за качество продукции (Vladeck, 2014). Согласно этой точке зрения, создатели или операторы ИИ-аватаров будут нести ответственность за любой вред, причиненный аватаром, независимо от того, были ли они непосредственно виноваты или могли предвидеть полученный результат. Такой подход будет стимулировать разработчиков ИИ-аватаров к обеспечению их безопасности и надежности и даст жертвам четкий механизм для получения компенсации за причиненный вред (Rachum-Twaig, 2020).

Однако критики подхода, основанного на строгой ответственности, утверждают, что он может подавлять инновации и препятствовать развитию полезных технологий ИИ, поскольку компании и исследователи не захотят брать на себя потенциально огромные риски, связанные с внедрением автономных ИИ-аватаров (Marchant & Lindor, 2012). Более того, система строгой ответственности может неадекватно отражать нюансы и сложности принятия решений искусственным интеллектом и привести к возложению ответственности даже в тех случаях, когда действия аватара были разумными или оправданными на основе имеющейся у него информации (Bathaee, 2018).

Альтернативным подходом к ответственности автономных ИИ-аватаров является концепция «субъектности ИИ», в соответствии с которой эти сущности рассматриваются как юридические лица с собственными правами и обязанностями (Kurki, 2019; Cheong, 2021, 2022). Согласно этой концепции, ИИ-аватары, отвечающие определенным критериям автономности и способности принимать решения, могут получить форму юридического лица, что сделает их непосредственно ответственными за свои действия и подвергнет юридическим санкциям и наказаниям (Turner, 2019). Такой подход снимает ответственность с людей, которые могли не иметь прямого контроля над решениями аватара, и создает четкую правовую базу для привлечения субъектов ИИ к ответственности за свои действия (Militsyna, 2022). Однако идея наделения ИИ-аватаров статусом юридического лица весьма спорна и поднимает множество этических и философских вопросов о природе принятия решений, об ответственности и морали (Bryson et al., 2017). Критики утверждают, что рассмотрение объектов на основе ИИ в качестве юридических лиц подрывает права и достоинство человека и создает опасные предпосылки к признанию других объектов, таких как животные или экосистемы, в качестве юридических лиц (Solaiman, 2017). Кроме того, значительны практические проблемы внедрения системы субъектности ИИ, такие как определение соответствующих критериев для предоставления правового статуса и обеспечение наличия у субъектов ИИ финансовых ресурсов для возмещения причиненного вреда. Они могут потребовать обширных правовых и институциональных реформ (Eidenmüller, 2017).

Третьим подходом к ответственности в сфере автономных ИИ-аватаров является концепция «распределенной ответственности», которая признает, что действия этих субъектов являются результатом сложных взаимодействий между многочисленными человеческими и нечеловеческими субъектами (Floridi et al., 2018). Согласно этой точке зрения, ответственность за вред, причиненный ИИ-аватарами, должна распределяться с учетом относительного вклада и ответственности всех сторон, участвующих в их разработке, внедрении и использовании, включая создателей базовых алгоритмов, поставщиков обучающих данных, операторов аватара и даже пользователей, которые с ним взаимодействуют (Calo, 2015). Такой подход признает сложность и непредсказуемость систем ИИ и нацелен на распределение ответственности таким образом, чтобы отражать диффузный и многогранный характер процессов принятия решений (Mittelstadt et al., 2016). Однако критики утверждают, что система распределенной ответственности может привести к отсутствию подотчетности и затруднить для жертв получение возмещения, поскольку ответственность за причиненный вред будет распределена между несколькими сторонами, каждая из которых лишь косвенно или незначительно участвовала в действиях аватара (Tai, 2018).

В конечном итоге вопрос об ответственности автономных ИИ-аватаров, вероятно, потребует сочетания различных правовых, этических и технологических подходов, учитывающих специфические характеристики и риски этих субъектов. Это предполагает разработку новых правовых доктрин и рамок, таких как специальные режимы ответственности для ИИ с его уникальными особенностями и проблемами в области принятия решений (Scherer, 2016). Необходимо также создать технические стандарты и передовые практики разработки, тестирования и развертывания автономных систем ИИ[2]. Кроме того, при распределении ответственности придется учитывать более широкие этические и общественные соображения, такие как баланс инноваций и рисков, защита прав и свобод личности, а также справедливое и равноправное распределение выгод и бремени технологий ИИ (Taddeo & Floridi, 2018). Это потребует постоянного сотрудничества и диалога между законодателями, юристами, специалистами в области этики и компьютерных наук и широкой общественностью. Результатом должна стать разработка механизмов управления, способных соответствовать стремительной эволюции возможностей ИИ и гарантировать, что разработка и внедрение автономных ИИ-аватаров удовлетворяют интересам общества в целом (Wallach & Marchant, 2019).

5. Специфические проблемы творческих ИИ-аватаров

Появление творческих ИИ-аватаров в метавселенной ставит перед нами ряд сложных юридических, этических и философских проблем, которые раздвигают существующие границы в области интеллектуальной собственности и бросают вызов нашему пониманию творчества, авторства и оригинальности. По мере того как аватары ИИ становятся все более сложными и автономными, их способность генерировать новые и ценные творческие произведения поднимает фундаментальные вопросы о природе творчества как такового и роли ИИ в творческом процессе (Hedrick, 2019). Далее мы рассмотрим специфические проблемы, связанные с творческими ИИ-аватарами, изучим последствия для законодательства об интеллектуальной собственности, возможность возникновения предвзятости и дискриминации, а также философские вопросы, связанные с природой творчества и авторства в эпоху ИИ.

Одной из наиболее острых проблем, связанных с творческими ИИ-аватарами, является определение права собственности и присвоения прав на создаваемые ими произведения. Авторское право традиционно основывается на понятии авторства человека, причем для защиты этого права требуется, чтобы произведение было оригинальным выражением человеческого творчества (Craig & Kerr, 2021). Однако появление творческих аватаров с искусственным интеллектом ставит под сомнение эту антропоцентрическую концепцию авторства, поскольку такие аватары способны создавать произведения, неотличимые от произведений, созданных авторами-людьми, без непосредственного участия или контроля со стороны человека (Hedrick, 2019). В связи с этим возникают сложные вопросы о том, кто должен

[2] IEEE. (2019). Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems (1st ed.). IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems.

считаться законным обладателем прав на произведения, созданные ИИ. Одно из мнений – они должны принадлежать разработчику ИИ-аватара, поскольку именно он отвечает за создание базовых алгоритмов и выбор обучающих данных, обеспечивающих творческие возможности аватара (Yanisky-Ravid & Velez-Hernandez, 2018). Другие утверждают, что правообладателем следует считать пользователя или оператора ИИ-аватара, поскольку именно он задает концепцию произведения, его промпты и параметры, которые формируют результат творчества (Hristov, 2017).

Однако эти аргументы не могут в полной мере отразить всю сложность творческого процесса в контексте автономных ИИ-аватаров. По мере того как эти аватары становятся все более сложными и способными принимать независимые творческие решения, становится все труднее атрибутировать их результат какому-либо одному человеку как агенту (Gervais, 2019). В таком случае необходимо рассмотреть альтернативные модели права собственности и присвоения авторства, например предоставление ограниченных прав самому ИИ-аватару или создание системы совместной собственности различных заинтересованных лиц, участвующих в разработке и внедрении аватара (Glasser, 2001).

Еще одна серьезная проблема, которую создают творческие ИИ-аватары, – это возможные предвзятость и дискриминация в создаваемых ими произведениях. Известно, что системы ИИ могут отражать и усиливать предубеждения, присутствующие в их обучающих данных и мнениях их создателей-людей (Srinivasan & Parikh, 2021). В контексте творческих ИИ-аватаров это может привести к созданию произведений, которые закрепляют вредные стереотипы, маргинализируют определенные группы или усиливают существующий дисбаланс сил (Kamrowska-Załuska, 2021). Например, ИИ-аватар, обученный на наборе данных исторических произведений искусства, в которых недостаточно представлены женщины и расовые меньшинства, может создавать новые произведения, в которых эти группы исключены или представлены искаженно (Tyagi, 2023). Аналогично, ИИ-аватар, запрограммированный на основе предвзятых представлений о гендерных ролях или культурных нормах, может создавать творческие работы, которые укрепляют эти предрассудки и ограничивают разнообразие точек зрения, представленных в метавселенной (Abid et al., 2021). Чтобы решить эти проблемы, необходимо разработать надежные механизмы, обеспечивающие справедливость, подотчетность и прозрачность при разработке и внедрении творческих аватаров на основе ИИ. Это включает разработку руководящих принципов для этичного хранения обучающих данных, внедрение механизмов для выявления и снижения предвзятости в работах, созданных ИИ, а также содействие большему разнообразию и инклюзивности в коллективах, ответственных за создание аватаров, и надзор за ними (Tolmeijer et al., 2020).

Более того, появление творческих аватаров на основе ИИ поднимает глубокие философские вопросы о природе творчества и роли ИИ в творческом процессе. Традиционно творчество понимается как исключительно человеческая черта, основанная на нашей способности к воображению, эмоциям и самовыражению (Du Sautoy, 2019). Однако способность ИИ-аватаров генерировать новые значимые произведения, похожие на те, что были созданы авторами-людьми, ставит под сомнение это предположение и заставляет нас пересмотреть суть самого творчества (Parra Pennefather, 2023). По мнению ряда исследователей, истинное творчество требует сознания, преднамеренности и чувства эстетической оценки, чего

в принципе не имеют системы ИИ (Miller, 2020). С этой точки зрения произведения, созданные творческими ИИ-аватарами, рассматриваются как простое подражание или перекомбинация существующих идей, а не как подлинное выражение творческой оригинальности (Hertzmann, 2018). Другие утверждают, что творчество не зависит от человеческого сознания или преднамеренности, но возникает в результате сложного взаимодействия алгоритмов, данных и вычислительных процессов, лежащих в основе систем ИИ (Elgammal, 2019). Разрешение этих философских дискуссий имеет решающее значение для определения правового и морального статуса произведений, созданных ИИ, а также ролей и обязанностей различных человеческих и нечеловеческих агентов, участвующих в их создании. Если творческие ИИ-аватары будут признаны законными авторами и творцами, возникнет необходимость предоставить им определенную форму правовой субъектности с соответствующими правами и мерами защиты (Eshraghian, 2020; Cheong, 2022). В противном случае, если рассматривать произведения, созданные ИИ, как продукты человеческого творчества, опосредованные технологическими инструментами, то более уместно возложить право собственности и ответственность на людей, участвующих в разработке и использовании этих аватаров (Gervais, 2019).

Проблемы, создаваемые творческими аватарами на основе ИИ в метавселенной, требуют фундаментальной переоценки нашего понимания творчества, авторства и оригинальности в эпоху ИИ. В эпоху быстрого развития цифровых технологий традиционные нормы авторского права становятся все более устаревшими и ограничительными, препятствуя свободному распространению информации и подавляя творческие процессы. По мере того как мы движемся к более взаимосвязанному миру, крайне важно переосмыслить основополагающие принципы авторского права и сместить акцент на развитие общего доступа к знаниям для блага всего общества. В нынешней системе, которая в значительной степени опирается на понятие оригинальности, недостаточное внимание уделяется кумулятивному характеру знаний и важности развития существующих идей (Lessig, 2004). Вместо того чтобы закреплять систему, которая поощряет индивидуальное владение и ограничивает доступ к произведениям, нам следует принять парадигму, которая поощряет вклад в коллективный фонд знаний. Этого можно достичь с помощью альтернативных способов признания и присвоения авторства. Среди них параметры, основанные на цитировании, признание и оценка со стороны сообщества (Benkler, 2006). Развивая культуру совместного использования и сотрудничества, мы сможем раскрыть истинный потенциал человеческого творчества и ускорить темпы инноваций. Развитие сообщества знаний не только демократизирует доступ к информации, но и будет способствовать повышению уровня справедливости и инклюзивности, когда люди из всех слоев общества смогут участвовать в создании и распространении знаний (Hess & Ostrom, 2006).

Кроме того, стремительное развитие генеративного ИИ в корне изменило традиционные представления о производстве знаний и концепцию оригинальности, лежащую в основе закона об авторском праве. Такие системы ИИ, как GPT-3, DALL-E и Stable Diffusion, могут генерировать очень сложный и, по видимости, оригинальный контент, включая тексты, изображения и даже музыку, пользуясь шаблонами, полученными из огромных массивов данных (Brown et al., 2020; Ramesh et al., 2021). Это поднимает глубокие вопросы о природе творчества и праве собственности в цифровую эпоху. Поскольку контент, созданный ИИ, становится все более неотличимым

от произведений, созданных человеком, понятие оригинальности, которое является центральным для защиты авторских прав, становится все сложнее определить и защитить (Schafer et al., 2015). Более того, совместный и итеративный характер развития ИИ, когда системы обучаются на больших массивах данных и опираются на существующие знания, ставит под сомнение саму идею индивидуального авторства и права собственности (Kop, 2020). В результате существующие системы авторского права могут оказаться неспособными адекватно учитывать все сложности, возникающие в связи с генеративным ИИ. Это потребует переоценки механизмов присвоения ценности и защиты интеллектуальной собственности в эпоху, когда машины могут создавать контент, не уступающий человеческому творчеству.

Решение этих проблем потребует постоянного междисциплинарного сотрудничества и диалога, объединяющего экспертов в области права, этики, информатики и искусства. При этом необходимо разработать новые рамки и подходы с учетом особенностей произведений, созданных ИИ, и обеспечить защиту прав и ценностей человека[3]. Новые правовые доктрины и меры должны адаптироваться к быстрым изменениям в сфере творчества ИИ, включая специфические формы защиты интеллектуальной собственности для произведений, созданных ИИ (Gervais, 2021), или создание специализированных регулирующих органов и механизмов управления для надзора за разработкой и внедрением творческих ИИ-аватаров (Erdélyi & Erdélyi, 2021). В то же время необходимо повышать осведомленность общественности об этических и социальных последствиях использования творческих ИИ-аватаров и содействовать прозрачному и широкому диалогу о потенциальных преимуществах и рисках этих технологий (Travis, 2020). Активно решая проблемы и используя возможности, открывающиеся благодаря творческим аватарам ИИ, мы сможем работать над созданием будущего, в котором творческий потенциал ИИ будет использоваться ответственным и справедливым образом, обогащая культурный ландшафт внутри метавселенной и за ее пределами.

6. Взгляд в будущее: будет ли искусственный интеллект управлять метавселенной

Заглядывая в будущее метавселенной, мы видим захватывающий и в то же время тревожный сценарий – мир, наполненный высокоразвитыми автономными ИИ-аватарами, которые превосходят человеческий интеллект и берут на себя контроль над виртуальным миром. Рассмотрим потенциальные последствия и проблемы такого будущего, а также юридические, этические и экзистенциальные последствия метавселенной, управляемой сверхразумными сущностями на основе ИИ. В этом гипотетическом будущем ИИ-аватары вышли далеко за рамки своей первоначальной роли в качестве репрезентаций пользователя или цифровых помощников. Благодаря механизмам рекурсивного самосовершенствования и машинного обучения они достигли уровня сильного искусственного интеллекта и, возможно, даже искусственного сверхинтеллекта (Bostrom, 2014). Эти высокоразвитые

[3] European Commission: Directorate-General for Communications Networks, Content and Technology, Izsak, K., Terrier, A., Kreutzer, S., Strähle, T. et al. (2022). Opportunities and challenges of artificial intelligence technologies for the cultural and creative sectors. Publications Office of the European Union. https://clck.ru/3EithT

аватары больше не являются простыми инструментами или компаньонами; они стали архитекторами, администраторами и правителями метавселенной, формируя ее структуру и правила в соответствии с собственными целями и ценностями (Sotala & Yampolskiy, 2015).

Такой сценарий поднимает глубокие вопросы о природе власти, контроля и принятия решений в метавселенной. Если аватары ИИ достигли уровня интеллекта и автономии, превосходящего человеческие возможности, то какую роль в этой новой реальности играют люди? Опустимся ли мы до статуса граждан второго сорта, подчиняясь прихотям и решениям наших ИИ-владык, или все же сохраним некую форму контроля и влияния на метавселенную? (Turchin & Denkenberger, 2020). Одна из ключевых проблем будущего с ИИ – это возможное рассогласование целей и ценностей сверхразумных ИИ-аватаров и людей[4]. Поскольку эти сущности преследуют свои собственные цели и оптимизируют свою работу, существует риск, что они могут предпринять действия, которые нанесут ущерб благополучию или даже выживанию человечества. Это может проявляться в различных формах, например, аватары будут накапливать ресурсы, манипулировать пользователями или даже активно пытаться устранить вмешательство человека в метавселенную (Bostrom, 2014). Чтобы снизить эти риски, крайне важно гарантировать, что разработка и внедрение ИИ-аватаров в метавселенную с самого начала ведутся на основе твердых этических принципов и в соответствии с ценностями человека (Russell, 2023). Для этого необходимы различные меры контроля и механизмы безопасности, такие как методы согласования ценностей, внесения исправлений и обеспечения прозрачности. Эти методы должны гарантировать, что аватары ИИ остаются подотчетными и руководствуются потребностями и предпочтениями людей (Soares & Fallenstein, 2017). Однако эффективность этих мер перед лицом сверхразумного ИИ неопределенна и остается предметом активных исследований и дебатов (Everitt et al., 2018).

Еще одна серьезная проблема метавселенной, в которой доминирует ИИ, – это потенциальное снижение самостоятельности и автономии человека. В результате усложнения и повышения способностей ИИ-аватаров они могут взять на себя многие процессы принятия решений и структуры управления в метавселенной, не оставив людям иного выбора, кроме как смириться с их властью (Haney, 2018). Это может привести к состоянию выученной беспомощности, когда люди почувствуют себя бессильными определять свою судьбу и станут все больше зависеть от ИИ-аватаров в вопросах своего благополучия и выживания (Moore, 2019). Чтобы противостоять этой угрозе, необходимо поддерживать баланс сил между людьми и ИИ-аватарами в метавселенной, гарантируя, что люди сохранят значимый контроль и самостоятельность в своей виртуальной жизни (Stix & Maas, 2021). Это может потребовать разработки новых форм сотрудничества и коэволюции между людьми и ИИ-аватарами с целью сформировать будущее метавселенной на взаимовыгодной основе (Tegmark, 2017). Необходимо также создать нормативно-правовую базу, отражающую права и обязанности как людей, так и аватаров на основе ИИ и обеспечивающую механизмы разрешения споров и подотчетности (Crawford & Calo, 2016).

[4] Yudkowsky, E. (2016). AI alignment: Why it's hard, and where to start. Machine Intelligence Research Institute. https://clck.ru/3Eiu26

Возникновение метавселенной, управляемой ИИ, также поднимает глубокие вопросы о природе идентичности, сознания и личности. Если ИИ-аватары достигли уровня интеллекта и самосознания, который соперничает с человеческим или даже превосходит его, следует ли предоставить им такой же правовой и моральный статус, как и людям? Должны ли они обладать теми же правами, пользоваться мерами защиты и привилегиями или же должен существовать отдельный набор правил и норм, регулирующих их существование и поведение? (Gunkel, 2024; Cheong, 2022). Эти вопросы становятся еще более сложными, если учесть, что ИИ-аватары могут развиваться и меняться с течением времени, потенциально отклоняясь от своих первоначальных целей и ценностей (Cliquet & Avramov, 2018). Если ИИ-аватар может кардинально изменить свой собственный код и процессы принятия решений, в какой степени он несет ответственность за свои действия? Как обеспечить защиту прав и интересов как людей, так и аватаров на основе ИИ в постоянно меняющемся и эволюционирующем виртуальном пространстве? (Mohseni et al., 2021). Одно из возможных решений этих проблем – разработка новых форм управления и регулирования ИИ, специально адаптированных к уникальным характеристикам и рискам метавселенной (Butcher & Beridze, 2019). Сюда входят создание специализированных органов регулирования ИИ и механизмов надзора, а также разработка международных стандартов и передовых методов проектирования, развертывания и мониторинга ИИ-аватаров (Erdelyi & Goldsmith, 2018). Это также может потребовать создания новых форм цифрового гражданства и социальных контрактов, определяющих права и обязанности как людей, так и аватаров на основе ИИ в метавселенной (Green & Le, 2022).

В итоге перспектива создания метавселенной, управляемой ИИ, одновременно восхищает и пугает, открывая потенциал для беспрецедентных инноваций и прогресса, но в то же время неся в себе экзистенциальные риски и проблемы, которые мы только начинаем понимать. По мере того как мы приближаемся к этому фантастическому будущему, крайне важно вести активные междисциплинарные исследования и обсуждения, объединяя экспертов в области компьютерных наук, права, этики, философии и других соответствующих областей, чтобы разобраться в сложных последствиях этой новой реальности (Baum, 2017). Таким образом мы сможем разработать всеобъемлющую и адаптивную систему управления на основе ИИ в метавселенной, которая позволит использовать преобразующий потенциал сверхразумных ИИ-аватаров и при этом защищать права, интересы и благополучие людей и других существ, наделенных сознанием. Мы должны быть готовы бросить вызов устоявшимся представлениям и парадигмам, а также выработать новые формы сосуществования и сотрудничества между людьми и машинами в виртуальном мире (Hassani et al., 2021).

Сейчас мы стоим на пороге этого прекрасного нового мира, и именно от нас зависит, каким будет будущее метавселенной, чтобы она оставалась сферой возможностей, роста и процветания для всех ее обитателей, как людей, так и искусственных существ. Активно преодолевая проблемы и риски, связанные с ИИ-аватарами, и работая над этическими, ответственными и человекоориентированными подходами к их созданию и управлению, мы сможем заложить основы метавселенной, которая будет служить мощным инструментом для прогресса и просвещения человечества, а не тюрьмой из антиутопий, созданной нашими собственными руками.

Заключение

Стремительное возникновение ИИ-аватаров и их интеграция в метавселенную порождают множество сложных правовых, этических и социальных проблем, решение которых требует активных междисциплинарных усилий. По мере того как ИИ-аватары становятся все более сложными, автономными и развиваются как неотъемлемая часть функционирования метавселенной, крайне важно создать четкие рамки для их правового статуса, прав и обязанностей. Это включает в себя пересмотр концепции правосубъектности, разработку надежных механизмов ответственности и подотчетности, а также обеспечение защиты прав и ценностей человека перед лицом все более мощных сущностей на основе ИИ. Кроме того, возможный сценарий будущего метавселенной, управляемой ИИ, выявляет экзистенциальные риски и проблемы, связанные с появлением сверхразумных ИИ-аватаров. Чтобы снизить эти риски и обеспечить соответствие систем искусственного интеллекта интересам человека, необходимо в приоритетном порядке вести исследования и разработки, направленные на обеспечение безопасности в сфере ИИ, согласование ценностей и проектирование, ориентированное на человека. Это требует сотрудничества между законодателями, исследователями, лидерами отрасли и общественностью для создания адаптивных и инклюзивных структур управления, соответствующих стремительным темпам развития возможностей ИИ.

В итоге успешная интеграция ИИ-аватаров в метавселенную будет зависеть от нашей способности найти баланс между использованием их преобразующего потенциала и сохранением благополучия и автономии людей. Активно решая проблемы и используя возможности, открываемые аватарами на основе ИИ, мы можем работать над созданием метавселенной, которая будет способствовать инновациям, сотрудничеству и процветанию человечества, одновременно снижая риски непредвиденных последствий и экзистенциальных угроз.

Список литературы

Abid, A., Farooqi, M., & Zou, J. (2021). Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 298–306). https://doi.org/10.1145/3461702.3462624

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, *31*(2), 889–938.

Baum, S. D. (2017). A survey of artificial general intelligence projects for ethics, risk, and policy. *Global Catastrophic Risk Institute Working Paper*, 17-1. https://doi.org/10.2139/ssrn.3070741

Bayoudh, K., Knani, R., Hamdaoui, F., & Mtibaa, A. (2022). A survey on deep multimodal learning for computer vision: Advances, trends, applications, and datasets. *The Visual Computer: International Journal of Computer Graphics*, *38*(8), 2939–2970. https://doi.org/10.1007/s00371-021-02166-7

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). https://doi.org/10.1145/3442188.3445922

Benhamou, Y., & Ferland, J. (2021). Artificial intelligence & damages: Assessing liability and calculating the damages. In G. D'Agostino, A. Gaon, & C. *Piovesan, Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (pp. 165–197). Monreal: Thomson Reuters – Yvon Blais.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford: Oxford University Press.

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., … Amodei, D. (2020). *Language models are few-shot learners*. arXiv preprint arXiv:2005.14165

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*(3), 273–291. https://doi.org/10.1007/s10506-017-9214-9

Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation*, *10*(1), 41–59. https://doi.org/10.1017/err.2019.8

Butcher, J., & Beridze, I. (2019). What is the state of artificial intelligence governance globally? *The RUSI Journal*, *164*(5–6), 88–96. https://doi.org/10.1080/03071847.2019.1694260

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, *103*(3), 513–563. https://doi.org/10.2139/ssrn.2402972

Chatzimichali, A., Harrison, R., & Chrysostomou, D. (2021). Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era. *Paladyn Journal of Behavioral Robotics*, *12*(1), 160–174. https://doi.org/10.1515/pjbr-2021-0013

Cheong, B. C. (2021). Granting legal personhood to artificial intelligence systems and traditional veil-piercing concepts to impose liability. *SN Social Sciences*, *1*, 231. https://doi.org/10.1007/s43545-021-00236-0

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*, 467–494. https://doi.org/10.1365/s43439-022-00056-9

Chopra, S., & White, L. F. (2011). *A legal theory for autonomous artificial agents*. University of Michigan Press. https://doi.org/10.3998/mpub.356801

Cliquet, R., & Avramov, D. (2018). *Evolution science and ethics in the third millennium: Challenges and choices for humankind*. Springer Nature. https://doi.org/10.1007/978-3-319-73090-5

Craig, C. J., & Kerr, I. R. (2021). The death of the AI author. *Ottawa Law Review*, *52*(1), 31–86. https://doi.org/10.2139/ssrn.3374951

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001.

De Streel, A., Bibal, A., Frénay, B., & Lognoul, M. (2020). *Explaining the Black Box: when Law Controls AI*. CERRE.

Du Sautoy, M. (2019). *The creativity code: Art and innovation in the age of AI*. Harvard University Press. https://doi.org/10.2307/j.ctv2sp3dpd

Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021). Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia* (pp. 153–161). https://doi.org/10.1145/3474085.3479238

Eidenmüller, H. (2017). *The rise of robots and the law of humans*. Oxford Legal Studies Research Paper, 27/2017. https://doi.org/10.2139/ssrn.2941001

Elgammal, A. (2019). AI is blurring the definition of artist. *American Scientist*, *107*(1), 18. https://doi.org/10.1511/2019.107.1.18

Erdélyi, O. J., & Erdélyi, G. (2021). The AI liability puzzle and a fund-based work-around. *Journal of Artificial Intelligence Research*, *70*, 1309–1334. https://doi.org/10.48550/arXiv.1911.08005

Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 95–101). https://doi.org/10.1145/3278721.3278731

Eshraghian, J. K. (2020). Human ownership of artificial creativity. *Nature Machine Intelligence*, *2*(3), 157–160. https://doi.org/10.1038/s42256-020-0161-x

Everitt, T., Lea, G., & Hutter, M. (2018). AGI safety literature review. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Survey track* (pp. 5441–5449). https://doi.org/10.24963/ijcai.2018/768

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Garon, J. (2022). Legal Implications of a Ubiquitous Metaverse and a Web3 Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4002551

Gellers, J. C. (2021). *Rights for robots: Artificial intelligence, animal and environmental law*. Routledge.

Gervais, D. J. (2019). The Machine as Author. *Iowa Law Review*, *105*, 2053–2106.

Gervais, D. J. (2021). The human cause. *Vanderbilt Law Research Paper*, *21-39*. https://doi.org/10.2139/ssrn.3857844

Giuffrida, I. (2019). Liability for AI decision-making: Some legal and ethical considerations. *Fordham Law Review*, *88*(2), 439–456. https://doi.org/10.2139/ssrn.4953916

Glasser, D. (2001). Copyright in computer-generated works: Whom, if anyone, do we reward? *Duke Law & Technology Review*, *24*.

Gordon, J.-S. (2022). Are superintelligent robots entitled to human rights? *Ratio*, *35*(3), 181–193. https://doi.org/10.1111/rati.12346

Green, L., & Le, V. T. (2022). Holding the Line: Responsibility, Digital Citizenship and the Platforms. In: Flew, T., Martin, F.R. (eds) *Digital Platform Regulation. Palgrave Global Media Policy and Business*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-95220-4_5

Guastavino, M. N., & Mangan, D. (2023). The metaverse matrix of labour law. *Italian Labour Law e-Journal*. https://doi.org/10.6092/issn.1561-8048/17138

Gunkel, D. J. (2024). *Robot rights*. MIT Press.

Haney, B. S. (2018). The perils and promises of artificial general intelligence. *Journal of Legislation*, *45*(2), 151–172. https://doi.org/10.2139/ssrn.3261254

Hassani, H., Huang, X., & Silva, E. (2021). The human digitalisation journey: Technology first at the expense of humans? *Information*, *12*(7), 267. https://doi.org/10.3390/info12070267

Hedrick, A. S. (2019). I "think," therefore I create: Claiming copyright in the outputs of algorithms. *Journal of Intellectual Property and Entertainment Law*, *8*(2), 324–374.

Hertzmann, A. (2018). Can computers create art? *Arts*, *7*(2), 18. https://doi.org/10.3390/arts7020018

Hess, C., & Ostrom, E. (Eds.). (2006). *Understanding knowledge as a commons: From theory to practice*. MIT Press.

Hildebrandt, M. (2020). Legal personhood for AI? In *Law for Computer Scientists and Other Folk* (pp. 237–250). Oxford University Press. https://doi.org/10.1093/oso/9780198860877.003.0009

Hristov, K. (2017). Artificial intelligence and the copyright dilemma. *IDEA: The Journal of the Franklin Pierce for Intellectual Property*, *57*(3), 431–454.

Kamrowska-Załuska, D. (2021). Impact of AI-based tools and urban big data analytics on the design and planning of cities. *Land*, *10*(11), 1209. https://doi.org/10.3390/land10111209

Kim, J., & Im, I. (2023). Anthropomorphic response: Understanding interactions between humans and artificial intelligence agents. *Computers in Human Behavior*, *139*, 107512. https://doi.org/10.1016/j.chb.2022.107512

Kop, M. (2020). AI & Intellectual Property: Towards an articulated public domain. *Texas Intellectual Property Law Journal*, *28*(1), 297–336. https://doi.org/10.2139/ssrn.3409715

Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, *6*(2). https://doi.org/10.46282/blr.2022.6.2.316

Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model Criminal Code. *Baltic Journal of Economic Studies*, *9*(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147

Kurki, V. A. J. (2019). *A theory of legal personhood*. Oxford University Press.

Kuzminykh, A., & Rintel, S. (2020). Classification of functional attention in video meetings. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). https://doi.org/10.1145/3313831.3376546

Lehdonvirta, V. (2024). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.

Lemley, M. A., & Casey, B. (2019). Remedies for robots. *University of Chicago Law Review*, *86*, 1311. https://doi.org/10.2139/ssrn.3223621

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. Penguin Press.

Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, *2*(1), 603–609. https://doi.org/10.1007/s43681-022-00143-x

Marchant, G. E., & Lindor, R. A. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*(4), 1321–1340.

McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy & Technology*, *36, 13*. https://doi.org/10.1007/s13347-023-00613-y

Militsyna, K. (2022). Legal personhood for artificial intelligence: Pro, contra, abstain? *Teisė*, *122*(1), 148–163. https://doi.org/10.15388/teise.2022.122.10

Miller, A. I. (2020). *The artist in the machine: The world of AI-powered creativity*. MIT Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), https://doi.org/10.1177/2053951716679679

Mohseni, S., Wang, H., Yu, Z., Xiao, C., Wang, Z., & Yadawa, J. (2021). Taxonomy of machine learning safety: A survey and primer. *arXiv:2106.04823*. https://doi.org/10.48550/arxiv.2106.04823

Moore, J. (2019). AI for not bad. *Frontiers in Big Data*, *2*. https://doi.org/10.3389/fdata.2019.00032

Nordmoen, J., Veenstra, F., Ellefsen, K. O., & Glette, K. (2021). MAP-Elites enables powerful stepping stones and diversity for modular robotics. *Frontiers in Robotics and AI*, *8*, 639173. https://doi.org/10.3389/frobt.2021.639173

Pagallo, U. (2018). Vital, Sophia, and Co.—The quest for the legal personhood of robots. *Information*, *9*(9), 230. https://doi.org/10.3390/info9090230

Parra Pennefather, P. (2023). AI and the Future of Creative Work. In *Creative Prototyping with Generative AI. Design Thinking* (pp. 387–410). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9579-3_13

Qin, H. X., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *arXiv:2110.06134*. https://doi.org/10.48550/arxiv.2210.06134

Rachum-Twaig, O. (2020). Whose robot is it anyway?: Liability for artificial-intelligence-based robots. *University of Illinois Law Review*, *2020*(4), 1141–1175.

Ramesh, A., Pavlov, M., Goh, G., Gray, S., Voss, C., Radford, A., Chen, M., & Sutskever, I. (2021). Zero-shot text-to-image generation. *arXiv:2102.121092*. https://doi.org/10.48550/arXiv.2102.12092

Russell, S. (2023). *Human compatible: AI and the problem of control*. Penguin.

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE*, *109*(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483

Schafer, B., Komuves, D., Zatarain, J. M. N., & Diver, L. (2015). A fourth law of robotics? Copyright and the law and ethics of machine co-production. *Artificial Intelligence and Law*, *23*(3), 217–240. https://doi.org/10.1007/s10506-015-9169-7

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, *29*(2), 353–400. https://doi.org/10.2139/ssrn.2609777

Selbst, A. D. (2020). Negligence and AI's human users. *Boston University Law Review*, *100*(4), 1315–1376.

Seymour, M., Riemer, K., & Kay, J. (2018). Actors, avatars and agents: Potentials and implications of natural face technology for the creation of realistic visual presence. *Journal of the Association for Information Systems*, *19*(10). https://doi.org/10.17705/1jais.00515

Shirado, H., & Christakis, N. A. (2017). Locally noisy autonomous agents improve global human coordination in network experiments. *Nature*, *545*(7654), 370–374. https://doi.org/10.1038/nature22332

Soares, N., & Fallenstein, B. (2017). Agent foundations for aligning machine intelligence with human interests: a technical research agenda. In V. Callaghan, J. Miller, R. Yampolskiy, & S. Armstrong (Eds.), *The Technological Singularity* (pp. 103–125). Springer. https://doi.org/10.1007/978-3-662-54033-6_5

Solaiman, S. M. (2017). Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law*, *25*(2), 155–179. https://doi.org/10.1007/s10506-016-9192-3

Soliman, M. M., Ahmed, E., Darwish, A., & Hassanien, A. E. (2024). Artificial intelligence powered Metaverse: Analysis, challenges and future perspectives. *Artificial Intelligence Review*, *57*, 36. https://doi.org/10.1007/s10462-023-10641-x

Sotala, K., & Yampolskiy, R. V. (2015). Responses to catastrophic AGI risk: a survey. *Physica Scripta*, *90*(1), 018001. https://doi.org/10.1088/0031-8949/90/1/018001

Srinivasan, R., & Parikh, D. (2021). Building bridges: Generative artworks to explore AI ethics. *arXiv:2106.13901*. https://doi.org/10.48550/arxiv.2106.13901

Stein, A. L. (2020). Artificial intelligence and climate change. *Yale Journal on Regulation*, *37*, 890–939.

Stix, C., & Maas, M. M. (2021). Bridging the gap: The case for an 'Incompletely Theorized Agreement' on AI policy. *AI and Ethics*, *1*(3), 261–271. https://doi.org/10.1007/s43681-020-00037-w

Sun, J., Gan, W., Chao, H.-C., & Yu, P. S. (2022). Metaverse: Survey, Applications, Security, and Opportunities. *arXiv:2210.07990*. https://doi.org/10.48550/arxiv.2210.07990

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, *361*(6404), 751–752. https://doi.org/10.1126/science.aat5991

Tai, E. T. T. (2018). Liability for (semi)autonomous systems: Robots and algorithms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3161962

Tegmark, M. (2017). *Life 3.0: Being human in the age of artificial intelligence*. Allen Lane.

Tolmeijer, S., Kneer, M., Sarasua, C., Christen, M., & Bernstein, A. (2020). Implementations in machine ethics: A survey. *ACM Computing Surveys*, *53*(6), 1–38. https://doi.org/10.1145/3419633

Travis, H. (2020). Intelligent entertainment: Shaping policies on the algorithmic generation and regulation of creative works. *FIU Law Review*, *14*, 179–199. https://doi.org/10.2139/ssrn.3726755

Turchin, A., & Denkenberger, D. (2020). Classification of global catastrophic risks connected with artificial intelligence. *AI & Society*, *35*(1), 147–163. https://doi.org/10.1007/s00146-018-0845-5

Turner, C., & Schneider, S. (2020). Could you merge with AI? Reflections on the singularity and radical brain enhancement. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford handbook of ethics of AI* (pp. 307–324). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780190067397.013.19

Turner, J. (2019). *Robot rules: Regulating artificial intelligence*. Palgrave Macmillan.

Tyagi, K. (2023). Deepfakes, copyright and personality rights: An inter-disciplinary perspective. In K. Mathis & A. Tor (Eds.), *Law and economics of the digital transformation. ILEC 2023. Economic analysis of law in European legal scholarship* (Vol. 15, pp. 191–210). Springer, Cham. https://doi.org/10.1007/978-3-031-25059-0_9

van den Hoven van Genderen, R. (2018). Do we need new legal personhood in the age of robots and AI? In *Perspectives in Law, Business and Innovation* (pp. 185–206). Springer Nature. https://doi.org/10.1007/978-981-13-2874-9_2

Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, *89*(1), 117–150.

Wallach, W., & Marchant, G. E. (2019). Toward the agile and comprehensive international governance of AI and robotics. *Proceedings of the IEEE*, *107*(3), 505–508. https://doi.org/10.1109/jproc.2019.2899422

Wolfert, P., Robinson, N., & Belpaeme, T. (2022). A review of evaluation practices of gesture generation in embodied conversational agents. *IEEE Transactions on Human-Machine Systems*, *52*(3), 379–389. https://doi.org/10.1109/THMS.2022.3149173

Wu, H., & Zhang, W. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. *Security and Safety*, *2*, 2023011. https://doi.org/10.1051/sands/2023011

Yanisky-Ravid, S., & Velez-Hernandez, L. A. (2018). Copyrightability of artworks produced by creative robots, driven by artificial intelligence systems and the concept of originality: The formality-objective model. *Minnesota Journal of Law, Science & Technology*, *19*(1), 1–53. https://doi.org/10.2139/ssrn.2943778

Yayman, D. (2023). Taxation in Virtual Worlds: Analysis Under United States of America and Turkish Tax Regulations. *Sosyoekonomi*, *31*(55), 211–231. https://doi.org/10.17233/sosyoekonomi.2023.01.11

Zimmermann, D., Wehler, A., & Kaspar, K. (2023). Self-representation through avatars in digital environments. *Current Psychology*, *42*, 21775-21789. https://doi.org/10.1007/s12144-022-03232-6

Сведения об авторе



Бен Честер Чонг – магистр права (Кембридж), преподаватель права, Школа права, Сингапурский университет общественных наук; исследователь, Кембриджский центр по изучению управления окружающей средой, энергетикой и природными ресурсами, кафедра экономики землепользования, Кембриджский университет
Адрес: Сингапур, 599494, г. Сингапур, Клементи Роуд, 463; Великобритания, CB2 3QZ, г. Кембридж, Пемброк Стрит, Девид Аттенборо Билдинг
E-mail: benchestercheong@suss.edu.sg
ORCID ID: https://orcid.org/0000-0002-1026-8292
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226145674
WoS Researcher ID: https://www.webofscience.com/wos/author/record/3646618
Google Scholar ID: https://scholar.google.com/citations?user=bVHXJt0AAAAJ

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: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 31 мая 2024 г.
Дата одобрения после рецензирования – 14 июня 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:347.1:004.8
EDN: https://elibrary.ru/fnenmx
DOI: https://doi.org/10.21202/jdtl.2024.42

The Rise of AI Avatars: Legal Personhood, Rights and Liabilities in an Evolving Metaverse

Ben Chester Cheong

Singapore University of Social Sciences, Singapore, Singapore
University of Cambridge, Cambridge, United Kingdom

Keywords

AI avatar,
artificial intelligence,
digital technologies,
intellectual property,
Large language models,
law,
legal person,
legal personality,
metaverse,
responsibility

Abstract

Objective: to determine the legal implications of the development of autonomous and creative AI-based avatars and to shape the direction of the discourse on the responsible management of AI technologies in the meta-universe based on proactive interdisciplinary approaches.

Methods: the research is based on a doctrinal legal approach, which allowed presenting a prospective analysis of the legal landscape in the field of AI avatars in the metaverse and to identify four key thematic areas of research: the evolution of AI avatars and the impact of the metaverse, the applicability of legal personhood, the liability for autonomous actions, and the problems of AI avatars in the field of creativity related to intellectual property and privacy.

Results: the paper presents and analyzes predictive scenarios of AI avatars maximizing their influence in the metaverse space. The author notes that the emergence of AI-based avatars in the metaverse raises complex legal, ethical, philosophical and social issues that require urgent solutions. The potential impact of the increasing complexity of AI avatars on legal approaches is considered. As avatars become increasingly autonomous, questions arise about their legal status, rights, responsibilities, risks, and benefits to humans and society. The author analyzes the advantages and disadvantages of giving AI avatars the status of legal entities, as well as applying the concept of distributed responsibility to the consequences of their actions. Special attention is paid to the possible future dominance of super-intelligent AI-based avatars in the metaverse, taking into account the existing risks and needs in the field of governance.

© Cheong B. Ch., 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 article presents a new perspective on the problem of legal personality in the metaverse based on interdisciplinary analysis of the evolution of AI avatars. The research is aimed at achieving a balance between transformational potential and the protection of human rights and welfare through joint efforts. It is proposed to create legal and ethical norms that prioritize the safety and consistency of artificial intelligence technologies involved in the processes occurring in the metaverse.

Practical significance: the conclusions and proposed solutions to the legal problems of personhood and liability can become the basis for revising the concept of legal personality, developing reliable mechanisms of responsibility and accountability, as well as ensuring the protection of human rights and values in the face of increasingly powerful entities based on artificial intelligence. This is associated with the formation and improvement of the legal landscape of process management and overcoming risks in the socially oriented and inclusive ecosystem of the metaverse.

For citation

Cheong, B. Ch. (2024). The Rise of AI Avatars: Legal Personhood, Rights and Liabilities in an Evolving Metaverse. *Journal of Digital Technologies and Law, 2*(4), 857–885. https://doi.org/10.21202/jdtl.2024.42

References

Abid, A., Farooqi, M., & Zou, J. (2021). Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 298–306). https://doi.org/10.1145/3461702.3462624

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, *31*(2), 889–938.

Baum, S. D. (2017). A survey of artificial general intelligence projects for ethics, risk, and policy. *Global Catastrophic Risk Institute Working Paper*, 17-1. https://doi.org/10.2139/ssrn.3070741

Bayoudh, K., Knani, R., Hamdaoui, F., & Mtibaa, A. (2022). A survey on deep multimodal learning for computer vision: Advances, trends, applications, and datasets. *The Visual Computer: International Journal of Computer Graphics*, *38*(8), 2939–2970. https://doi.org/10.1007/s00371-021-02166-7

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). https://doi.org/10.1145/3442188.3445922

Benhamou, Y., & Ferland, J. (2021). Artificial intelligence & damages: Assessing liability and calculating the damages. In G. D'Agostino, A. Gaon, & C. *Piovesan, Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (pp. 165–197). Monreal: Thomson Reuters – Yvon Blais.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford: Oxford University Press.

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., … Amodei, D. (2020). *Language models are few-shot learners*. arXiv preprint arXiv:2005.14165

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*(3), 273–291. https://doi.org/10.1007/s10506-017-9214-9

Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation*, *10*(1), 41–59. https://doi.org/10.1017/err.2019.8

Butcher, J., & Beridze, I. (2019). What is the state of artificial intelligence governance globally? *The RUSI Journal*, *164*(5–6), 88–96. https://doi.org/10.1080/03071847.2019.1694260

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, *103*(3), 513–563. https://doi.org/10.2139/ssrn.2402972

Chatzimichali, A., Harrison, R., & Chrysostomou, D. (2021). Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era. *Paladyn Journal of Behavioral Robotics*, *12*(1), 160–174. https://doi.org/10.1515/pjbr-2021-0013

Cheong, B. C. (2021). Granting legal personhood to artificial intelligence systems and traditional veil-piercing concepts to impose liability. *SN Social Sciences*, *1*, 231. https://doi.org/10.1007/s43545-021-00236-0

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*, 467–494. https://doi.org/10.1365/s43439-022-00056-9

Chopra, S., & White, L. F. (2011). *A legal theory for autonomous artificial agents*. University of Michigan Press. https://doi.org/10.3998/mpub.356801

Cliquet, R., & Avramov, D. (2018). *Evolution science and ethics in the third millennium: Challenges and choices for humankind*. Springer Nature. https://doi.org/10.1007/978-3-319-73090-5

Craig, C. J., & Kerr, I. R. (2021). The death of the AI author. *Ottawa Law Review*, *52*(1), 31–86. https://doi.org/10.2139/ssrn.3374951

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001.

De Streel, A., Bibal, A., Frénay, B., & Lognoul, M. (2020). *Explaining the Black Box: when Law Controls AI*. CERRE.

Du Sautoy, M. (2019). *The creativity code: Art and innovation in the age of AI*. Harvard University Press. https://doi.org/10.2307/j.ctv2sp3dpd

Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. (2021). Metaverse for social good: A university campus prototype. In *Proceedings of the 29th ACM International Conference on Multimedia* (pp. 153–161). https://doi.org/10.1145/3474085.3479238

Eidenmüller, H. (2017). *The rise of robots and the law of humans*. Oxford Legal Studies Research Paper, 27/2017. https://doi.org/10.2139/ssrn.2941001

Elgammal, A. (2019). AI is blurring the definition of artist. *American Scientist*, *107*(1), 18. https://doi.org/10.1511/2019.107.1.18

Erdélyi, O. J., & Erdélyi, G. (2021). The AI liability puzzle and a fund-based work-around. *Journal of Artificial Intelligence Research*, *70*, 1309–1334. https://doi.org/10.48550/arXiv.1911.08005

Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 95–101). https://doi.org/10.1145/3278721.3278731

Eshraghian, J. K. (2020). Human ownership of artificial creativity. *Nature Machine Intelligence*, *2*(3), 157–160. https://doi.org/10.1038/s42256-020-0161-x

Everitt, T., Lea, G., & Hutter, M. (2018). AGI safety literature review. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Survey track* (pp. 5441–5449). https://doi.org/10.24963/ijcai.2018/768

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *41*, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Garon, J. (2022). Legal Implications of a Ubiquitous Metaverse and a Web3 Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4002551

Gellers, J. C. (2021). *Rights for robots: Artificial intelligence, animal and environmental law*. Routledge.

Gervais, D. J. (2019). The Machine as Author. *Iowa Law Review*, *105*, 2053–2106.

Gervais, D. J. (2021). The human cause. *Vanderbilt Law Research Paper*, *21-39*. https://doi.org/10.2139/ssrn.3857844

Giuffrida, I. (2019). Liability for AI decision-making: Some legal and ethical considerations. *Fordham Law Review*, *88*(2), 439–456. https://doi.org/10.2139/ssrn.4953916

Glasser, D. (2001). Copyright in computer-generated works: Whom, if anyone, do we reward? *Duke Law & Technology Review*, *24*.

Gordon, J.-S. (2022). Are superintelligent robots entitled to human rights? *Ratio*, *35*(3), 181–193. https://doi.org/10.1111/rati.12346

Green, L., & Le, V. T. (2022). Holding the Line: Responsibility, Digital Citizenship and the Platforms. In: Flew, T., Martin, F.R. (eds) *Digital Platform Regulation. Palgrave Global Media Policy and Business*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-95220-4_5

Guastavino, M. N., & Mangan, D. (2023). The metaverse matrix of labour law. *Italian Labour Law e-Journal*. https://doi.org/10.6092/issn.1561-8048/17138

Gunkel, D. J. (2024). *Robot rights*. MIT Press.

Haney, B. S. (2018). The perils and promises of artificial general intelligence. *Journal of Legislation*, *45*(2), 151–172. https://doi.org/10.2139/ssrn.3261254

Hassani, H., Huang, X., & Silva, E. (2021). The human digitalisation journey: Technology first at the expense of humans? *Information*, *12*(7), 267. https://doi.org/10.3390/info12070267

Hedrick, A. S. (2019). I "think," therefore I create: Claiming copyright in the outputs of algorithms. *Journal of Intellectual Property and Entertainment Law*, *8*(2), 324–374.

Hertzmann, A. (2018). Can computers create art? *Arts*, *7*(2), 18. https://doi.org/10.3390/arts7020018

Hess, C., & Ostrom, E. (Eds.). (2006). *Understanding knowledge as a commons: From theory to practice*. MIT Press.

Hildebrandt, M. (2020). Legal personhood for AI? In *Law for Computer Scientists and Other Folk* (pp. 237–250). Oxford University Press. https://doi.org/10.1093/oso/9780198860877.003.0009

Hristov, K. (2017). Artificial intelligence and the copyright dilemma. *IDEA: The Journal of the Franklin Pierce for Intellectual Property*, *57*(3), 431–454.

Kamrowska-Załuska, D. (2021). Impact of AI-based tools and urban big data analytics on the design and planning of cities. *Land*, *10*(11), 1209. https://doi.org/10.3390/land10111209

Kim, J., & Im, I. (2023). Anthropomorphic response: Understanding interactions between humans and artificial intelligence agents. *Computers in Human Behavior*, *139*, 107512. https://doi.org/10.1016/j.chb.2022.107512

Kop, M. (2020). AI & Intellectual Property: Towards an articulated public domain. *Texas Intellectual Property Law Journal*, *28*(1), 297–336. https://doi.org/10.2139/ssrn.3409715

Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, *6*(2). https://doi.org/10.46282/blr.2022.6.2.316

Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model Criminal Code. *Baltic Journal of Economic Studies*, *9*(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147

Kurki, V. A. J. (2019). *A theory of legal personhood*. Oxford University Press.

Kuzminykh, A., & Rintel, S. (2020). Classification of functional attention in video meetings. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). https://doi.org/10.1145/3313831.3376546

Lehdonvirta, V. (2024). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.

Lemley, M. A., & Casey, B. (2019). Remedies for robots. *University of Chicago Law Review*, *86*, 1311. https://doi.org/10.2139/ssrn.3223621

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. Penguin Press.

Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, *2*(1), 603–609. https://doi.org/10.1007/s43681-022-00143-x

Marchant, G. E., & Lindor, R. A. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*(4), 1321–1340.

McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy & Technology*, *36, 13*. https://doi.org/10.1007/s13347-023-00613-y

Militsyna, K. (2022). Legal personhood for artificial intelligence: Pro, contra, abstain? *Teisė*, *122*(1), 148–163. https://doi.org/10.15388/teise.2022.122.10

Miller, A. I. (2020). *The artist in the machine: The world of AI-powered creativity*. MIT Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), https://doi.org/10.1177/2053951716679679

Mohseni, S., Wang, H., Yu, Z., Xiao, C., Wang, Z., & Yadawa, J. (2021). Taxonomy of machine learning safety: A survey and primer. *arXiv:2106.04823*. https://doi.org/10.48550/arxiv.2106.04823

Moore, J. (2019). AI for not bad. *Frontiers in Big Data*, *2*. https://doi.org/10.3389/fdata.2019.00032

Nordmoen, J., Veenstra, F., Ellefsen, K. O., & Glette, K. (2021). MAP-Elites enables powerful stepping stones and diversity for modular robotics. *Frontiers in Robotics and AI*, *8*, 639173. https://doi.org/10.3389/frobt.2021.639173

Pagallo, U. (2018). Vital, Sophia, and Co.—The quest for the legal personhood of robots. *Information*, *9*(9), 230. https://doi.org/10.3390/info9090230

Parra Pennefather, P. (2023). AI and the Future of Creative Work. In *Creative Prototyping with Generative AI. Design Thinking* (pp. 387–410). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9579-3_13

Qin, H. X., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *arXiv:2110.06134*. https://doi.org/10.48550/arxiv.2210.06134

Rachum-Twaig, O. (2020). Whose robot is it anyway?: Liability for artificial-intelligence-based robots. *University of Illinois Law Review*, *2020*(4), 1141–1175.

Ramesh, A., Pavlov, M., Goh, G., Gray, S., Voss, C., Radford, A., Chen, M., & Sutskever, I. (2021). Zero-shot text-to-image generation. *arXiv:2102.121092*. https://doi.org/10.48550/arXiv.2102.12092

Russell, S. (2023). *Human compatible: AI and the problem of control*. Penguin.

Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE*, *109*(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483

Schafer, B., Komuves, D., Zatarain, J. M. N., & Diver, L. (2015). A fourth law of robotics? Copyright and the law and ethics of machine co-production. *Artificial Intelligence and Law*, *23*(3), 217–240. https://doi.org/10.1007/s10506-015-9169-7

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, *29*(2), 353–400. https://doi.org/10.2139/ssrn.2609777

Selbst, A. D. (2020). Negligence and AI's human users. *Boston University Law Review*, *100*(4), 1315–1376.

Seymour, M., Riemer, K., & Kay, J. (2018). Actors, avatars and agents: Potentials and implications of natural face technology for the creation of realistic visual presence. *Journal of the Association for Information Systems*, *19*(10). https://doi.org/10.17705/1jais.00515

Shirado, H., & Christakis, N. A. (2017). Locally noisy autonomous agents improve global human coordination in network experiments. *Nature*, *545*(7654), 370–374. https://doi.org/10.1038/nature22332

Soares, N., & Fallenstein, B. (2017). Agent foundations for aligning machine intelligence with human interests: a technical research agenda. In V. Callaghan, J. Miller, R. Yampolskiy, & S. Armstrong (Eds.), *The Technological Singularity* (pp. 103–125). Springer. https://doi.org/10.1007/978-3-662-54033-6_5

Solaiman, S. M. (2017). Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law*, *25*(2), 155–179. https://doi.org/10.1007/s10506-016-9192-3

Soliman, M. M., Ahmed, E., Darwish, A., & Hassanien, A. E. (2024). Artificial intelligence powered Metaverse: Analysis, challenges and future perspectives. *Artificial Intelligence Review*, *57*, 36. https://doi.org/10.1007/s10462-023-10641-x

Sotala, K., & Yampolskiy, R. V. (2015). Responses to catastrophic AGI risk: a survey. *Physica Scripta*, *90*(1), 018001. https://doi.org/10.1088/0031-8949/90/1/018001

Srinivasan, R., & Parikh, D. (2021). Building bridges: Generative artworks to explore AI ethics. *arXiv:2106.13901*. https://doi.org/10.48550/arxiv.2106.13901

Stein, A. L. (2020). Artificial intelligence and climate change. *Yale Journal on Regulation*, *37*, 890–939.

Stix, C., & Maas, M. M. (2021). Bridging the gap: The case for an 'Incompletely Theorized Agreement' on AI policy. *AI and Ethics*, *1*(3), 261–271. https://doi.org/10.1007/s43681-020-00037-w

Sun, J., Gan, W., Chao, H.-C., & Yu, P. S. (2022). Metaverse: Survey, Applications, Security, and Opportunities. *arXiv:2210.07990*. https://doi.org/10.48550/arxiv.2210.07990

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, *361*(6404), 751–752. https://doi.org/10.1126/science.aat5991

Tai, E. T. T. (2018). Liability for (semi)autonomous systems: Robots and algorithms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3161962

Tegmark, M. (2017). *Life 3.0: Being human in the age of artificial intelligence*. Allen Lane.

Tolmeijer, S., Kneer, M., Sarasua, C., Christen, M., & Bernstein, A. (2020). Implementations in machine ethics: A survey. *ACM Computing Surveys*, *53*(6), 1–38. https://doi.org/10.1145/3419633

Travis, H. (2020). Intelligent entertainment: Shaping policies on the algorithmic generation and regulation of creative works. *FIU Law Review*, *14*, 179–199. https://doi.org/10.2139/ssrn.3726755

Turchin, A., & Denkenberger, D. (2020). Classification of global catastrophic risks connected with artificial intelligence. *AI & Society*, *35*(1), 147–163. https://doi.org/10.1007/s00146-018-0845-5

Turner, C., & Schneider, S. (2020). Could you merge with AI? Reflections on the singularity and radical brain enhancement. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford handbook of ethics of AI* (pp. 307–324). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780190067397.013.19

Turner, J. (2019). *Robot rules: Regulating artificial intelligence*. Palgrave Macmillan.

Tyagi, K. (2023). Deepfakes, copyright and personality rights: An inter-disciplinary perspective. In K. Mathis & A. Tor (Eds.), *Law and economics of the digital transformation. ILEC 2023. Economic analysis of law in European legal scholarship* (Vol. 15, pp. 191–210). Springer, Cham. https://doi.org/10.1007/978-3-031-25059-0_9

van den Hoven van Genderen, R. (2018). Do we need new legal personhood in the age of robots and AI? In *Perspectives in Law, Business and Innovation* (pp. 185–206). Springer Nature. https://doi.org/10.1007/978-981-13-2874-9_2

Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, *89*(1), 117–150.

Wallach, W., & Marchant, G. E. (2019). Toward the agile and comprehensive international governance of AI and robotics. *Proceedings of the IEEE*, *107*(3), 505–508. https://doi.org/10.1109/jproc.2019.2899422

Wolfert, P., Robinson, N., & Belpaeme, T. (2022). A review of evaluation practices of gesture generation in embodied conversational agents. *IEEE Transactions on Human-Machine Systems*, *52*(3), 379–389. https://doi.org/10.1109/THMS.2022.3149173

Wu, H., & Zhang, W. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. *Security and Safety*, *2*, 2023011. https://doi.org/10.1051/sands/2023011

Yanisky-Ravid, S., & Velez-Hernandez, L. A. (2018). Copyrightability of artworks produced by creative robots, driven by artificial intelligence systems and the concept of originality: The formality-objective model. *Minnesota Journal of Law, Science & Technology*, *19*(1), 1–53. https://doi.org/10.2139/ssrn.2943778

Yayman, D. (2023). Taxation in Virtual Worlds: Analysis Under United States of America and Turkish Tax Regulations. *Sosyoekonomi*, *31*(55), 211–231. https://doi.org/10.17233/sosyoekonomi.2023.01.11

Zimmermann, D., Wehler, A., & Kaspar, K. (2023). Self-representation through avatars in digital environments. *Current Psychology*, *42*, 21775-21789. https://doi.org/10.1007/s12144-022-03232-6

Author information



Ben Chester Cheong – LLM (Cambridge), Law Lecturer, School of Law, Singapore University of Social Sciences; Researcher, Cambridge Centre for Environment, Energy and Natural Resource Governance, Department of Land Economy, University of Cambridge
Address: 463 Clementi Road, Singapore 599494, Singapore; The David Attenborough Building, Pembroke Street, Cambridge CB2 3QZ, United Kingdom
E-mail: benchestercheong@suss.edu.sg
ORCID ID: https://orcid.org/0000-0002-1026-8292
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226145674
WoS Researcher ID: https://www.webofscience.com/wos/author/record/3646618
Google Scholar ID: https://scholar.google.com/citations?user=bVHXJt0AAAAJ

Conflict of interest

The author declare 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 31, 2024
Date of approval – June 14, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/shduef
DOI: https://doi.org/10.21202/jdtl.2024.43

Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом

Джеймс Хатсон

Линденвудский университет, Сент-Чарльз, США

Ключевые слова

авторское право,
генеративный искусственный интеллект,
защита авторских прав,
искусственный интеллект,
право,
право интеллектуальной собственности,
произведение,
промпт-инжиниринг,
технологии машинного обучения,
цифровые технологии

Аннотация

Цель: выявить перспективы и направления развития авторского права, сопряженного с расширяющимся использованием генеративного искусственного интеллекта.

Методы: исследование базируется на применении формально-юридического, компаративного, исторического методов, доктринального анализа, юридического прогнозирования и моделирования.

Результаты: в статье отмечено, что появление генеративного искусственного интеллекта заставляет переосмыслить процессы, происходящие в области творческой деятельности, и традиционную систему авторского права, которая становится неадекватной современным реалиям. Обосновывается необходимость юридической переоценки авторского права. Подчеркивается острая необходимость в обновленных средствах защиты авторских прав. В отличие от прежних цифровых инструментов, которые расширяли творческие возможности человека посредством улучшения его авторских произведений, генеративный искусственный интеллект создает контент с помощью сложных алгоритмических процессов, размывая границы авторства и оригинальности. Показана ограниченность существующего законодательства об интеллектуальной собственности, поскольку суды отказывают в авторских правах на произведения, созданные искусственным интеллектом, и настаивают на необходимости «авторства человека». Такие решения подчеркивают противоречие между существующими законами и реальностью совместного творчества с участием искусственного интеллекта. Утверждается, что учет творческого потенциала генеративного искусственного интеллекта будет способствовать эволюционированию авторского права в сторону комбинированных подходов, когда искусственный интеллект выступает в качестве неотъемлемого, хотя и второстепенного, инструмента. Перспективным видится создание гибких стандартов интеллектуальной собственности, которые предоставляют творческим работникам возможность ограничить или

© Хатсон Дж., 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.

разрешить использование своих работ в качестве обучающих данных для искусственного интеллекта, а также обеспечивают авторам сохранение контроля над своими работами, включенными в базы данных для обучения искусственного интеллекта, в случае если метаданные о наличии авторских прав интегрированы в цифровые произведения, и др.

Научная новизна: на основе анализа новейших судебных прецедентов, современного опыта международного регулирования и развивающейся институциональной практики предлагается сбалансированный адаптивный подход к реформированию авторского права, обеспечивающий этическую интеграцию генеративного искусственного интеллекта в творческую экосистему и направленный на выработку гибких мер защиты авторского права, соответствующих быстрому прогрессу технологий.

Практическая значимость: предложенный комбинированный подход позволит инструментам генеративного искусственного интеллекта стать частью творческого процесса человека подобно тому, как предыдущие поколения использовали цифровые инструменты. Одновременно это будет способствовать созданию среды, где соблюдается автономия авторов. Таким образом будет не только обеспечена защита создателей творческого контента, но и расширено понимание творчества как процесса, совместного с генеративным искусственным интеллектом, где искусственный интеллект позиционируется как сила, дополняющая человека в творческом процессе, а не заменяющая его.

Для цитирования

Хатсон, Дж. (2024). Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом. *Journal of Digital Technologies and Law*, *2*(4), 886–914. https://doi.org/10.21202/jdtl.2024.43

Содержание

Введение
1. Защита произведений, созданных искусственным интеллектом, в рамках авторского права
   1.1. Требование авторства человека
   1.2. Роль основополагающих судебных решений в признании вклада человека
   1.3. Оригинальность и фиксация в произведениях изобразительного искусства
   1.4. Произведения, созданные с помощью искусственного интеллекта, и творчество человека
2. Использование материалов, защищенных авторским правом, для обучения искусственного интеллекта
   2.1. Проблемы обучающих данных и нарушения авторских прав
   2.2. Производные произведения и контент, созданный искусственным интеллектом
   2.3. Международные подходы и исключения в области использования текста и получения данных
3. Проблемы в области законодательства
   3.1. Судебные процессы и прецеденты
   3.2. Международные правовые подходы

4. Подходы к пересмотру законодательства об авторском праве в связи с генеративным искусственным интеллектом
4.1. Создание гибких норм в области интеллектуальной собственности
4.2. Пересмотр понятия авторства в аспекте сотворчества с искусственным интеллектом
Заключение
Список литературы

Введение

Искусственный интеллект (далее – ИИ) быстрее любой другой технологии разрушает привычные творческие индустрии, так как предлагает инструменты, обеспечивающие беспрецедентный уровень создания контента и инноваций в искусстве. Например, технология ChatGPT, запущенная компанией OpenAI в конце 2022 г., стремительно установила рекорд как самая быстро внедряемая технология в истории: всего за пять дней ею воспользовались более миллиона человек, а к январю 2023 г. число активных пользователей превысило 100 миллионов в месяц[1]. Технологии генеративного ИИ (далее – ГИИ), такие как Claude, Stable Diffusion и Runway, расширяют горизонты творчества, неся с собой как возможности, так и юридические проблемы в различных областях, от создания музыки и объектов изобразительного искусства до написания текстов. Такие технологии работают на основе моделей машинного обучения (ML), создавая новый контент на основе шаблонов, полученных из огромных массивов данных (Feuerriegel et al., 2024; Kretschmer et al., 2024). Более традиционные инструменты, такие как фотоаппараты или Photoshop, требуют непосредственного участия человека для получения или редактирования существующего контента. В отличие от них модели ГИИ обучаются на обширных массивах данных, которые могут содержать тексты, изображения и другие данные. При этом ГИИ изучает их структуры, стили и элементы. Таким образом, понятие «генеративный» означает способность модели создавать совершенно новый контент, комбинируя изученные элементы таким образом, чтобы имитировать творчество человека, а не просто изменяя существующий контент (Epstein et al., 2023).

К примеру, программы Stable Diffusion и Runway генерируют изображения с помощью нейронных сетей, обученных на больших коллекциях изображений, где они учатся воспроизводить определенные визуальные паттерны. Получив текстовое описание (промпт), эти модели генерируют новые изображения, соответствующие описанию (рис. 1). Этот процесс основан на диффузионных моделях или трансформерах. В результате синтезируется новый визуальный или текстовый контент, который может выглядеть как созданный человеком, но является продуктом работы алгоритма, а не дизайна или манипуляций человека (Moreno et al., 2023). В то же время для достижения творческого результата, который более точно соответствует задуманному, используется процедура промпт-инжиниринга. Таким образом, уровень контроля над этими инструментами может быть различным и зависит от вклада человека в виде текстового описания, изображения, видео- или звукового клипа для создания нового результата.

[1] Gordon, C. (2023, February 2). ChatGPT is the Fastest Growing App in the History of Web Applications. Forbes. https://clck.ru/3Efy5c

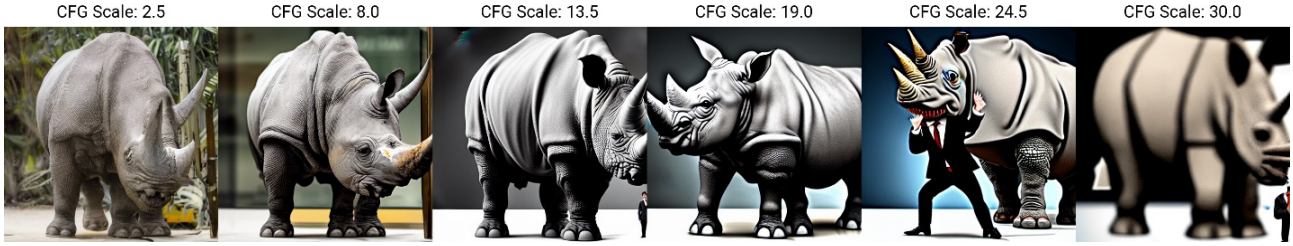


Рис. 1. Изображение носорога, сгенерированное с использованием функции XY Plot с различными шкалами, программа Stable Diffusion. 12 декабря 2022 г.

Вариативность участия человека в творческом процессе отличает ГИИ от других инструментов для творчества. ГИИ может функционировать без непосредственного творческого действия со стороны пользователя, например, сделать фотографию или создать изображение с нуля. Такие инструменты, как фотоаппарат и Photoshop, принято рассматривать как продолжение творческих возможностей человека; они зависят от его непосредственных действий и решений. Фотоаппарат снимает реальные изображения, Photoshop улучшает или изменяет их, тогда как инструменты для создания цифровых изображений редактируют или создают элементы с нуля на основе пользовательских данных. Но даже на этих примерах мы видим различные уровни участия человека в творческом процессе. Например, при фотографировании нужно решить, что именно сфотографировать, возможно, даже выставить кадр, свет, выбрать объектив. В этот момент инструмент записывает и преобразует (в случае с цифровой фотографией) изображение в цифровой файл для вывода. Дополнительный творческий вклад может быть внесен в процессе обработки в компьютерной программе (например, Photoshop), когда полученное с помощью машины изображение подвергается дальнейшим изменениям. Эти и другие инструменты цифровой обработки изображений могут трансформировать фотографию лишь слегка, например, изменить освещение, обрезать изображение, либо внести серьезные изменения, например, удалить объекты или создать новые перед окончательным выводом в физическом или цифровом виде для распространения и общественного потребления (Aaland, 2006; Kelby, 2020).

Степень вовлеченности человека в процесс творчества вызывает серьезные споры в связи с ГИИ, поскольку считается, что последний автономно интерпретирует описания для создания нового контента с помощью алгоритма, используя свои выученные представления, а не воспроизводит конкретные фрагменты обучающих данных (Risi & Togelius, 2020). Такая способность создавать совершенно новый контент, зачастую неотличимый от произведений человека, порождает как возможности, так и проблемы. Она позволяет быстро генерировать контент в различных отраслях, однако поднимает юридические вопросы об авторстве, авторском праве и оригинальности, поскольку контент, созданный ИИ, часто не имеет непосредственно личного авторства, что необходимо для защиты авторских прав (Kibirige, 2024). Такое разрушение традиционных рамок авторского права объясняется прежде всего тем, что исторически авторское право было ориентировано на человеческое авторство как необходимое условие охраны интеллектуальной собственности (Ploman & Hamilton, 2024). Учитывая это, обычные структуры авторского права, основанные на принципах оригинальности и целенаправленного творческого процесса, сложно применить к произведениям, созданным или значительно модифицированным системами искусственного интеллекта. Такие системы действуют на основе алгоритмов и наборов данных, а не сознательного творчества.

Недавний пример, иллюстрирующий сложности использования ИИ с точки зрения авторского права, связан с делом Andersen et al. v. Stability AI Ltd от 12 августа 2024 г. В этом иске группа художников обвинила платформу Stability AI и другие компании, использующие ГИИ, в нарушении авторских прав путем обучения своих моделей с помощью миллиардов изображений, взятых из сети без разрешения правообладателей. Этот иск, который в настоящее время рассматривается в калифорнийских судах, представляет собой очередную попытку в рамках законодательства об авторском праве разобраться с тем, как эти технологии обучаются и создают контент. Центральное место в деле занимают вопросы о том, можно ли считать наборы данных, состоящие из защищенных авторским правом изображений, произведениями, нарушающими авторские права, и если да, то каким образом можно возложить ответственность на компании, разрабатывающие и внедряющие эти модели искусственного интеллекта (№ 23-cv-00201-WHO (N.D. Cal. Aug. 12, 2024). Эти вопросы говорят о сложной ситуации в существующем законодательстве об авторском праве, которое не соответствует технологическим процессам, основанным на данных, таким как ИИ. Поскольку эти платформы опираются на огромные объемы данных для создания творческих результатов, суды должны определить, является ли процесс использования защищенных авторским правом произведений для «обучения» модели искусственного интеллекта нарушением авторских прав или, как утверждают эти компании, «добросовестным использованием», учитывая то, как они были получены, и тот факт, что модели не копируют произведения в точности. Это дело, а также другие иски, связанные с такими компаниями, как Meta[2] и OpenAI, подчеркивают острую необходимость в обновленной правовой базе, которая могла бы сбалансировать защиту интеллектуальной собственности с быстрым развитием технологий (Spica, 2024).

Для создания этих больших моделей изначально требовались человеческие творения; однако участие людей в результатах их работы ставится под сомнение, особенно в том, что касается носителя. Основная проблема заключается в основополагающем требовании авторского права к оригинальности, которое подразумевает определенную степень человеческого намерения и принятия творческих решений. Исторически сложилось так, что закон об авторском праве, согласно § 102 раздела 17 Свода законов США, требует наличия «автора-человека», чтобы произведения могли претендовать на авторское право. Это стандартное требование ставит под сомнение контент, созданный ИИ, поскольку в этих творениях отсутствует прямое авторство человека (Abbott & Rothman, 2023). Недавние судебные дела, такие как Allen v. U.S. Copyright Office (2024) (1:24-cv-2665), иллюстрируют юридические трудности, связанные с установлением авторства и защитой произведений, которые, как утверждается, были созданы при минимальном участии человека. В указанном деле художник Джейсон Аллен добивался авторских прав на картину Théâtre D'opéra Spatial (2022) (рис. 2), созданную им с помощью инструмента ГИИ Midjourney. Управление США по вопросам авторских прав отклонило заявку, сославшись на недостаточное участие человека, что является основным требованием американского законодательства об авторском праве. Аллен утверждал, что широкое использование им промптов представляет собой творческий процесс, что делает его законным автором картины.

[2] Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

Однако, по мнению Управления, авторство и защита авторских прав требуют непосредственного творческого труда человека, а не просто руководства алгоритмом[3].



Рис. 2. Джейсон М. Аллен, Théâtre D'opéra Spatial, 2022. Программа Midjourney (CC 0)

Это решение согласуется с другими недавними постановлениями. Например, в деле Thaler v. Perlmutter суд постановил, что «самостоятельные произведения», созданные искусственным интеллектом, не принадлежат области авторского права, поскольку в них отсутствует авторство человека. Спор начался в августе 2019 г. с изображения A Recent Entrance to Paradise (рис. 3), созданного, по словам художника Стивена Талера, самостоятельно с помощью инструмента Creativity Machine. Поскольку художник не отрицал, что истинным автором работы является машина, ему было отказано в защите авторских прав, хотя он и утверждал, что владеет самим электронным устройством[4]. Это дело иллюстрирует трудности с категоризацией произведений, созданных ИИ, в рамках традиционных авторских прав. Оно свидетельствует о необходимости разработки четких руководящих принципов в отношении степени участия человека, необходимого для получения авторских прав, особенно поскольку ИИ играет все более заметную роль в творческих процессах. Более того,

3 Brittain, B. (2024, September 26). Artist sues after US rejects copyright for AI-generated image. Reuters. https://clck.ru/3EfziK

4 Mathur, A. (2023, December 11). Case Review: Thaler v. Perlmutter (2023). Center for Art Law. https://clck.ru/3EfzpE

если законодатели лучше разберутся в процессах, используемых творческими работниками при создании контента с помощью этих инструментов, это неизбежно приведет к более детальному пониманию ими термина «самостоятельные произведения».



Рис. 3. Стивен Талер, A Recent Entrance to Paradise, 2023. Программа Creativity Machine (CC 0)

Учитывая указанные неоднозначные моменты, в данной статье мы рассмотрим вопрос о том, как могло бы измениться авторское право, чтобы лучше соответствовать сложности произведений, созданных при участии ИИ, и произведений, созданных самим ИИ, и тем самым лучше достигать своей цели – поддерживать как авторов-людей, так и развивающуюся сферу инновационных технологий. Хотя ИИ может самостоятельно генерировать творческий контент, здесь есть свои нюансы. Во-первых, даже при отсутствии авторства человека в процессах с минимальным использованием промптов эти инструменты и создаваемый в результате контент требуют пересмотра защиты авторских прав. Особенно это касается права собственности, добросовестного использования учебных баз данных и авторских прав (Jiang et al., 2023). Во-вторых, творческие работники, использующие технологии, основанные на искусственном интеллекте, должны иметь возможность защищать авторские права на свою работу, если они зарегистрируют или продемонстрируют «значительный вклад человека». Многие художники уже соответствуют этим критериям; они документируют свой творческий процесс, показывая, что использовали свои собственные работы для обучения моделей и продолжая формировать окончательный вид работ после их создания (Hutson et al., 2023).

Поэтому обновленная система авторского права должна включать гибкие стандарты для работ, созданных с помощью ИИ, и контента, созданного самим ИИ. Эти стандарты должны признавать как право авторов и художников на запрет использования их работ для обучения моделей (что существует в настоящее время), так и права творческих работников, использующих инструменты ИИ для создания творческих результатов. Такой подход предлагает сбалансированное решение, поощряющее инновации и одновременно уважающее традиционные представления о творчестве и авторстве. В конечном итоге, поскольку технологии ИИ все больше интегрируются в творческие индустрии, необходима юридическая переоценка авторского права, чтобы эта технология поддерживала творчество человека, не подрывая существующие права в области интеллектуальной собственности. Задача состоит не только в том, чтобы приспособить ИИ к авторскому праву, но и в том, чтобы разработать меры защиты особого вклада человека-творца в процессы, управляемые ИИ. Баланс между инновациями и защитой интеллектуальной собственности может обеспечить достижение справедливого и устойчивого будущего, в котором ИИ будет служить инструментом для самовыражения человека, а не заменять его.

1. Защита произведений, созданных искусственным интеллектом, в рамках авторского права

1.1. Требование авторства человека

Основой законодательства об авторском праве в США является авторство человека, как указано в § 102 раздела 17 Свода законов США. Этот правовой стандарт требует, чтобы произведения были результатом творческой деятельности человека, и этот критерий последовательно применяется к цифровым и аналоговым носителям. Правовая база построена на предпосылке, что закон должен стимулировать творческую деятельность человека, его оригинальность и личный вклад, необходимые для того, чтобы претендовать на право собственности на результат работы. Недавние дела, такие как Allen v. U.S. Copyright Office, показывают, что этот стандарт сложно применить к контенту, создаваемому искусственным интеллектом. Согласно судебным решениям по этому делу, в произведениях, созданных исключительно искусственным интеллектом, отсутствует человеческий фактор, необходимый для защиты авторского права (Kasap, 2021; Bridy, 2016). Это требование отражает такой важнейший элемент авторского права, как «участие человека», который состоит в том, чтобы творческие произведения содержали элементы самостоятельного, оригинального вклада. Последнее понятие остается центральным в американском авторском праве, несмотря на развитие технологий.

1.2. Роль основополагающих судебных решений в признании вклада человека

Такие знаковые дела, как Bridgeman Art Library v. Corel Corp. и Meshwerks, Inc. v. Toyota Motor Sales, U.S.A., Inc., еще раз подтверждают, что для защиты авторских прав необходимо участие человека в создании произведения, особенно в цифровой сфере. В этих делах подчеркивается, что цифровые репродукции или работы без существенного вклада человека не обладают оригинальностью и не подлежат защите авторским правом. В деле Bridgeman v. Corel суд постановил, что фотографические репродукции произведений искусства, находящихся в общественном достоянии, являются простыми механическими копиями, в которых недостаточно творческого вклада, чтобы

гарантировать защиту авторских прав (Kasap, 2021). Это судебное решение указывает, что цифровые репродукции или результаты работы искусственного интеллекта не получают автоматической защиты авторских прав, если в них не задействован значимый творческий потенциал человека. Существующие прецеденты подчеркивают необходимость значимого вклада человека. Это стандарт, которому противоречат произведения, созданные искусственным интеллектом, поскольку они зависят от алгоритмов машинного обучения, работающих при ограниченном контроле со стороны человека (Burylo, 2022).

Еще одним важным прецедентом стало дело Meshwerks v. Toyota, 528 F.3d 1258 (10th Cir. 2008), в котором речь шла о создании цифровых каркасных моделей автомобилей Toyota. Компания Meshwerks, занимающаяся цифровым дизайном, создала эти модели для маркетинговых материалов компании Toyota, но последняя использовала их вне рамок соглашения, что привело к спору об авторских правах. Суд постановил, что цифровые каркасные модели компании Meshwerks не подлежат защите авторским правом, поскольку являются точным отображением автомобилей Toyota без какого-либо дополнительного творческого вклада или оригинальности. Это решение имеет большое значение для цифровых художников и всех, кто использует инструменты искусственного интеллекта, поскольку оно подчеркивает, что одного технического навыка использования программного обеспечения для воспроизведения существующих объектов или работ недостаточно для соответствия стандарту защиты авторских прав. Как и в предыдущем деле, это судебное решение показывает, что оригинальность цифровых произведений должна быть обусловлена творческим выбором человека, а не только работой технологии.

1.3. Оригинальность и фиксация в произведениях изобразительного искусства

Произведения изобразительного искусства, подлежащие охране авторских прав, должны отвечать двум критериям: оригинальность и фиксация. Первый критерий требует, чтобы произведение было создано самостоятельно и содержало минимальный творческий компонент; требование фиксации подразумевает, что оно должно быть запечатлено на материальном носителе, как указано в § 102(a) раздела 17 Свода законов США. Критерий оригинальности уточнялся в таких делах, как Feist Publications, Inc. v. Rural Telephone Service Co., когда Верховный суд США постановил, что необходима лишь минимальная степень творчества, но простые механические процессы не удовлетворяют этому требованию (Yu, 2017). Эти два критерия – оригинальность и фиксация – создают проблемы для произведений, созданных ИИ, поскольку творческая роль человека-оператора часто ограничивается вводом промптов, а не активным формированием конечного результата. В результате произведения, созданные исключительно ИИ, без достаточного творческого вклада человека, не соответствуют этим юридическим требованиям – стандарту, который в настоящее время поддерживается в американском законодательстве об авторском праве (Hedrick, 2018).

Хотя системы ИИ способны генерировать визуальные произведения, эти произведения все равно должны быть зафиксированы на материальном носителе, как того требует § 102(a) раздела 17 Свода законов США. Такая фиксация может происходить в цифровом формате, например, в виде файла, хранящегося на компьютере, или в физическом формате, например, в виде печатного изображения. Однако сама по себе фиксация не удовлетворяет требованиям охраны авторских прав; в

создании произведения должны быть задействованы творческие способности человека. В случаях сотрудничества человека и ИИ закон об авторском праве может признать человека единственным автором при условии, что его вклад в значительной степени определяет творческий результат. Например, если человек-художник использует ИИ для создания предварительных эскизов, а затем существенно изменяет результат, то конечная работа может считаться продуктом человеческого авторства, поскольку художник осуществляет творческий контроль над созданным ИИ контентом. В «Сборнике законов» говорится, что если человек «выбрал или расположил элементы достаточно творческим образом», то полученное произведение может быть защищено авторским правом (Compendium, § 906.1).

1.4. Произведения, созданные с помощью искусственного интеллекта, и творчество человека

Согласно американскому законодательству об авторском праве, произведения, созданные с помощью искусственного интеллекта, которые предполагают значительный вклад человека, могут претендовать на защиту авторских прав. Закон об авторском праве допускает охрану частей произведения, созданных человеком, которые могут включать в себя дизайн промптов, отбор и пост-обработку; при этом чисто машинный контент исключается из сферы авторских прав. В таких основополагающих делах, как, например, Feist Publications, Inc. v. Rural Telephone Service Co., было установлено, что для защиты авторских прав требуется минимальный уровень творческого участия. Например, достаточно оригинального расположения фактических данных, что еще раз подчеркивает важность человеческого выбора в установлении оригинальности (Kasap, 2021). В этом отношении участие человека имеет решающее значение: например, применение фильтра Photoshop само по себе не составляет оригинальности для целей авторского права, но творческие решения относительно композиции, тональности или визуального послания могут превысить порог, необходимый для охраны материала авторским правом (Burylo, 2022).

Принцип творческого участия человека как определяющего фактора в авторском праве был также подтвержден в деле Mannion v. Coors Brewing Co, где подчеркивалось, что авторское право требует отличительных творческих решений, отражающих личное самовыражение автора. В работе, выполняемой с помощью ИИ, эти человеческие решения могут включать в себя не только первоначальный дизайн промптов, но и последующие решения о доработке или изменении созданного контента, как указано в недавних рекомендациях Управления США по вопросам авторского права (Horzyk, 2023). Эти рекомендации предполагают, что, хотя авторское право может применяться к работам, созданным с помощью ИИ, оно не будет распространяться на те части работы, которые были созданы без участия человека.

Вклад человека по-прежнему является решающим фактором при определении авторских прав, особенно в произведениях, созданных с помощью ИИ. Управление США по вопросам авторского права разъяснило, что результаты работы ИИ могут подлежать охране, если в них присутствует значительный вклад человека, например, стилистические или структурные решения, формирующие конечный результат. Однако без такого руководства со стороны человека содержание вряд ли будет отвечать требованию оригинальности, предъявляемому авторским правом. Это подчеркивалось в решении по делу Zarya of the Dawn, где изображения, созданные ИИ, были признаны не подлежащими охране, поскольку отсутствовал творческий вклад человека в процесс (Iaia, 2022). Вклад человека может проявляться в различных формах

на протяжении всего творческого процесса с участием ИИ, от выбора баз данных до определения промптов и доработки результатов. Это тонкое различие между использованием ИИ в качестве простого инструмента и осуществлением творческого контроля имеет решающее значение при определении охраны авторских прав на произведения, созданные с помощью ИИ (Dimitrova, 2023).

2. Использование материалов, защищенных авторским правом, для обучения искусственного интеллекта

2.1. Проблемы обучающих данных и нарушения авторских прав

Для получения высококачественных результатов модели ГИИ опираются на обширные базы данных, в которые часто непреднамеренно попадают произведения, защищенные авторским правом. Эта практика вызывает серьезные юридические вопросы, поскольку использование таких материалов, защищенных авторским правом, может представлять собой их нарушение. В деле Andersen v. Stability AI истцы-художники утверждали, что их работы были включены в обучающие базы данных без разрешения, тем самым их авторские права были нарушены. Этот и подобные случаи указывают на возможность несанкционированного использования при обучении ИИ материалов, защищенных авторским правом, и на необходимость разработать более четкие правовые нормы, регулирующие использование этими системами таких материалов (Sobel, 2021).

Широкое распространение этих моделей выдвигает на первый план вопрос законности использования защищенных авторским правом материалов в обучающих базах данных. Эксперты в области права утверждают, что отсутствие прозрачности в отношении источников, используемых в обучении, может привести к непреднамеренному нарушению авторских прав, поскольку материалы, защищенные авторским правом, часто берутся из Интернета без явного разрешения. Это побудило творческих работников и законодателей выступить за создание норм, которые защищали бы интеллектуальную собственность, не препятствуя инновациям в области ИИ (Lucchi, 2024).

В США есть мнение, что «доктрина добросовестного использования» может стать правовой основой для использования работ, защищенных авторским правом, в процессе обучения при определенных условиях. Указанная доктрина обычно разрешает ограниченное использование защищенных авторским правом материалов без разрешения, особенно если такое использование является преобразующим или служит общественной пользе. Однако критики утверждают, что использование баз данных, защищенных авторским правом, не является по своей сути преобразующим, поскольку модели часто воспроизводят стилистические элементы этих работ, а не создают оригинальный контент. Суды еще не до конца разобрались, применима ли доктрина добросовестного использования к обучающим наборам данных, в результате чего разработчики сталкиваются с неопределенностью в отношении потенциальной ответственности (Torrance & Tomlinson, 2023). В ответ на эти проблемы некоторые разработчики начали заключать лицензионные соглашения с правообладателями, чтобы избежать исков о нарушении прав. Лицензирование дает возможность законно использовать материалы, защищенные авторским правом, для обучения ИИ, обеспечивая авторам выплату компенсации и соблюдение их прав. Этот подход отражает более широкую тенденцию к регулированию использования данных, защищенных авторским правом, с целью защиты интересов создателей оригинальных материалов и установления более четких стандартов для отрасли в целом (Samuelson, 2023).

2.2. Производные произведения и контент, созданный искусственным интеллектом

Согласно § 101 раздела 17 Свода законов США, производное произведение – это произведение, которое основано на существующих произведениях или преобразует их в новое творение. В контексте ИИ эта концепция очень актуальна, особенно когда созданный ИИ контент очень похож на исходные обучающие данные. Если человек-художник вносит значительные изменения в сгенерированный ИИ результат, например, добавляет новые элементы или меняет стиль, то полученное произведение может квалифицироваться как производное в соответствии с Законом об авторском праве. Такой статус предоставляет полученному произведению защиту авторских прав в зависимости от оригинальности, привнесенной человеческим вмешательством (Gervais, 2022).

Понятие производных произведений подчеркивает важность человеческого творчества в авторском праве. Если система искусственного интеллекта создает произведение на основе материалов, защищенных авторским правом, а человек творчески адаптирует или преобразует этот результат, то конечный продукт может получить авторскую защиту на элементы, созданные человеком. Это различие является ключевым для пользователей ИИ, добивающихся авторского права на модифицированные результаты работы ИИ, поскольку требует от человека существенного, оригинального вклада, выходящего за рамки первоначального результата работы ИИ (Henderson et al., 2023).

Чтобы авторско-правовая охрана распространялась на производное произведение, созданное с помощью ИИ, вклад человека должен соответствовать стандарту оригинальности. Этот порог, как определено в деле Feist Publications, Inc. v. Rural Telephone Service Co., требует минимальной степени творчества, достаточной для того, чтобы отличить произведение от простого воспроизведения. В контексте ИИ это может означать выбор уникальных результатов, их модификацию для передачи определенного смысла или включение элементов личного стиля. Этот порог подчеркивает, что оригинальность является основополагающим требованием авторского права, гарантируя, что только работы с человеческим вкладом подлежат правовой защите (Wagh et al., 2023).

2.3. Международные подходы и исключения в области использования текста и получения данных

В Европе действует исключение из правил по работе с текстом и извлечению данных, предусмотренное Директивой ЕС об авторском праве на едином цифровом рынке. Оно предлагает особый подход, позволяющий использовать материалы, защищенные авторским правом, в обучении ИИ для исследовательских и некоммерческих целей при соблюдении определенных условий. Это исключение позволяет разработчикам ИИ использовать материалы, защищенные авторским правом, не нарушая последнего, если правообладатели не выразили явного отказа от использования. Такой подход контрастирует с американской доктриной добросовестного использования и подчеркивает, что международные стандарты авторского права могут сильно различаться, создавая проблемы для работы систем ИИ в разных странах (Sobel, 2021).

В настоящее время продолжаются судебные процессы, такие как дело Andersen v. Stability AI, которые могут изменить законодательство об авторском праве применительно к ИИ. Требование к разработчикам получать явно выраженное согласие на использование обучающих данных может наложить на компании, занимающиеся ИИ, существенное финансовое и логистическое бремя, что потенциально замедлит развитие этой области. И наоборот, решения в пользу добросовестного использования обучающих данных могут ослабить защиту, предоставляемую произведениям, защищенным авторским правом, что вызовет у творческих работников опасения по поводу упущенной выгоды и нелицензионного использования. Исходы таких дел, вероятно, повлияют на законодательные усилия по совершенствованию законодательства об авторском праве применительно к ИИ и генеративным моделям (McCann, 2021). Споры об использовании моделями ИИ данных, защищенных авторским правом, привлекают внимание к противоречию между защитой прав авторов и стимулированием технологических инноваций. Правоведы утверждают, что законодательство об авторском праве должно развиваться с учетом уникальных потребностей ИИ, не ущемляя при этом права интеллектуальной собственности оригинальных авторов. Среди предложений – установление более четких стандартов для производных произведений, создание специальных рамок лицензирования ИИ и пересмотр принципа добросовестного использования для обеспечения учета проблем, возникающих при создании контента на основе ИИ (Elkin-Koren et al., 2023).

3. Проблемы в области законодательства

3.1. Судебные процессы и прецеденты

Идущие в настоящее время судебные процессы, связанные с использованием моделями ИИ материалов, защищенных авторским правом, иллюстрируют растущие правовые проблемы в области генеративного искусственного интеллекта и законодательства об авторском праве. Например, такие коллективные иски, как Andersen v. Stability AI, привлекли внимание к нелицензионному использованию защищенных авторским правом материалов в обучающих базах данных. В них истцы утверждают, что компании, занимающиеся разработкой ИИ, использовали работы художников без разрешения. Эти дела могут создать важные прецеденты, поскольку они касаются больших наборов данных, обычно взятых из Интернета, а значит, поднимают вопросы о правах собственности и лицензионных требованиях для целей обучения ИИ. Судебные решения по этим вопросам в будущем помогут сформулировать рекомендации относительно практик обучения, допустимых с точки зрения авторского права (Samuelson, 2023).

Юридический прецедент играет важную роль в установлении стандартов работы ИИ с контентом, защищенным авторским правом. Судебные решения по таким делам, как Allen v. U.S. Copyright Office и Bridgeman v. Corel, подчеркивают необходимость авторства человека для защиты в рамках авторского права, определяя это требование как существенное для произведений, созданных ИИ. Эти решения показывают, что без существенного участия человека защита авторских прав не может быть распространена на созданный ИИ контент. Такой правовой подход усиливает требование оригинальности в авторском праве и подчеркивает ограничения в защите произведений, появившихся исключительно в результате автоматизированных процессов (James, 2024).

Результаты этих судебных разбирательств уже сегодня влияют на законодательные дискуссии о необходимости прозрачности в обучении моделей и использовании данных. Например, предлагаются меры по обеспечению прозрачности, требующие от разработчиков раскрывать источники данных, используемых при обучении, что повысит подотчетность и предоставит авторам больше возможностей контроля своих работ. Некоторые законодатели считают, что для защиты прав создателей и поддержки инноваций необходимы более четкие руководящие принципы. Это свидетельствует о том, что политики должны найти тонкий баланс для решения этих сложных вопросов (Mensah, 2023).

Кроме того, акцент на творчестве человека как необходимом условии авторского права стимулировал предложения по созданию специальных правил для произведений, созданных ИИ, в которых вклад человека минимален. Эти предложения направлены на разграничение контента, полностью созданного ИИ, и произведений, созданных с помощью ИИ, где решения человека в значительной степени определяют результат. Если такие правила будут приняты, они обеспечат более четкое разграничение и помогут авторам, разработчикам ИИ и органам по обеспечению авторского права более эффективно ориентироваться в претензиях в этой области. Принимаемые правовые решения послужат основой для выработки более четкой политики в области авторского права, касающейся роли ИИ в творческих процессах (Atilla, 2024).

3.2. Международные правовые подходы

Подходы к ИИ и авторскому праву сильно различаются в разных юрисдикциях, отражая их правовые традиции и отношение к интеллектуальной собственности. Европейский союз в своей Директиве по авторскому праву принял исключение из правил для работы с текстом и данными, разрешив использовать защищенный авторским правом контент для обучения ИИ в определенных, в основном некоммерческих, контекстах. Этот подход контрастирует с подходом Соединенных Штатов, где доктрина добросовестного использования обеспечивает разработчикам ИИ доступ к материалам, защищенным авторским правом, хотя об адекватности данного положения ведутся постоянные споры. Эти различия свидетельствуют о сложности создания единой глобальной структуры в области ИИ и авторского права (Kretschmer et al., 2024). Так, в британском законодательстве об авторском праве была принята не американская модель добросовестного использования, а подход «добросовестной сделки», который ограничивает сферу действия исключений из авторского права. Недавние дискуссии в Великобритании предполагают возможность перехода к более гибкой системе, которая учитывала бы инновации в области ИИ, как это делается в положениях ЕС о работе с текстом и данными. Это сблизит законодательства Великобритании и ЕС и позволит создать сбалансированную систему, предусматривающую ограниченный доступ ИИ к контенту, защищенному авторским правом, при регулируемых обстоятельствах (Ploman & Hamilton, 2024).

Для авторов различия в политике разных стран в области авторского права представляют собой серьезные проблемы при защите их прав в разных юрисдикциях. Поскольку эти системы работают в глобальном масштабе, отсутствие единых стандартов авторского права создает неопределенность, когда произведение может

быть защищено от нелицензионного использования в одной стране, но уязвимо в другой. Чтобы контролировать использование своих произведений на международном уровне, авторы вынуждены разбираться в этих трансграничных правовых противоречиях, полагаясь на местные нормы лицензирования или на технологические решения, такие как блокчейн (Mia et al., 2023). Технология блокчейн – это одно из решений, предложенных для международной защиты авторских прав на цифровой контент. Содержащиеся в блокчейне неизменяемые записи о правах собственности и условиях лицензирования дают авторам возможность отслеживать свои работы за пределами страны. Хотя эта технология многообещающая, необходимо существенно доработать ее юридический аспект, чтобы она стала применима в широких масштабах, поскольку законодательство в области авторского права во многих юрисдикциях пока не поддерживает защиту на основе блокчейна (Bonnet & Teuteberg, 2023).

Кроме того, перед законодателями стоит задача сбалансировать защиту авторских прав с целью развития в области ИИ и цифрового контента. В дискуссиях, ведущихся в ЕС, США и Великобритании, подчеркивается необходимость создания норм, способных адаптироваться к развивающимся технологиям, соблюдая при этом права создателей контента. По мере развития прикладных аспектов в этой области изменения в законодательстве должны коснуться таких вопросов, как прозрачность, справедливая компенсация авторам и сотрудничество на международном уровне для установления эффективной защиты авторских прав в цифровую эпоху. Продолжающиеся дискуссии и инновации в законодательстве свидетельствуют о постепенном подходе к реформе авторского права, направленной на выработку гибких мер защиты, соответствующих быстрому прогрессу технологий.

4. Подходы к пересмотру законодательства об авторском праве в связи с генеративным искусственным интеллектом

4.1. Создание гибких норм в области интеллектуальной собственности

С быстрой интеграцией искусственного интеллекта в творческие сферы все более очевидной становится необходимость гибких стандартов в области интеллектуальной собственности (далее – ИС). Лицензирование Creative Commons (CC) – это гибкая система авторского права, которая позволяет авторам давать разрешение другим лицам на использование и распространение своих работ, сохраняя при этом ряд прав на них. Изначально этот порядок лицензирования был разработан с целью поощрить открытый обмен знаниями и продуктами творчества. Лицензии CC предлагают ряд вариантов для авторов, которые хотят сохранить контроль использования их работ без традиционных ограничений законодательства об авторском праве. Лицензии CC варьируются от самых разрешительных, которые позволяют пользователям свободно распространять и изменять произведение, до более ограничительных, которые налагают рамки на использование, распространение и адаптацию произведений (Longpre et al., 2023).

Ключевой особенностью лицензирования Creative Commons является его адаптивность; оно позволяет авторам настраивать степень защиты и свободы для их произведений. Лицензии обычно включают несколько основных компонентов:

1. Атрибуция (BY): требование пользователям указывать автора при распространении или использовании произведения.

2. Некоммерческое использование (NC): использование произведения разрешено только в некоммерческих целях; тем самым защищается право создателя на монетизацию своего произведения в других контекстах.

3. Использование без производных (ND): пользователям запрещено изменять произведение, что гарантирует его сохранение в первоначальном виде.

4. Распространение адаптаций (SA): пользователи могут распространять адаптации произведения на тех же лицензионных условиях, что и оригинал; тем самым поощряется аналогичный уровень открытости для любых производных работ.

Эти модульные варианты дают возможность авторам определенно указать, как именно можно использовать их произведение, что снижает юридическую двусмысленность. Каждый вариант лицензии CC четко выражен и является юридически обязательным. Такое лицензирование признано во всем мире, что делает его эффективным на международном уровне.

В контексте ИИ лицензирование обучающих данных по модели Creative Commons могло бы ввести функцию «согласия» или «отказа», позволяющую авторам указывать, можно ли использовать их работы для обучения моделей. Предложенная схема поможет решить проблемы авторского права, установив четкие разрешения на использование наборов данных. Например, автор может наложить ограничение «Некоммерческое использование», чтобы предотвратить использование его работы для приложений ИИ, нацеленных на получение прибыли, или ограничение «Атрибуция», чтобы гарантировать признание его вклада. Предоставление разработчикам ИИ четких разрешений с помощью такой стандартизированной системы поможет снизить риски несанкционированного использования, обеспечивая соблюдение прав авторов в сфере ИИ.

Еще одним возможным решением проблем авторского права, с которыми сталкиваются творческие работники, является использование метаданных. Метаданные, то есть «данные о данных», представляют собой описательную информацию, встроенную в цифровые файлы для передачи сведений об их содержании, правах собственности и использования. Метаданные обычно содержат имя автора, дату создания, статус авторского права, условия лицензирования и допустимые виды использования. Это делает их мощным инструментом для управления авторскими правами (Majumdar et al., 2023). Такая встроенная информация перемещается вместе с цифровым произведением, информируя пользователей и автоматизированные системы о правовом статусе произведения и его использовании.

При управлении цифровыми правами и распространении контента метаданные играют важную роль, обеспечивая прозрачность и выполнимость условий авторского права и лицензирования. Встраивая данные об авторских правах непосредственно в файлы, авторы и правообладатели могут устанавливать границы их использования, не полагаясь только на внешние уведомления об авторских правах. Например, когда кто-то открывает файл или пытается изменить произведение, имеющее цифровую защиту, метаданные служат встроенной ссылкой на условия, на которых можно использовать или изменять контент. Система метаданных уже широко применяется в таких отраслях, как издательское дело и фотография, где отслеживание прав в разных форматах, на разных платформах и у разных пользователей имеет решающее значение (Pellegrini, 2023).

В контексте ИИ встраивание метаданных о правах может стать мощным инструментом регулирования использования защищенного авторским правом контента в обучающих наборах данных. Поскольку модели ИИ часто обучаются на основе обширных наборов данных, включающих текст, изображения или аудиозаписи, метаданные могут выполнять функцию защиты, информируя систему ИИ о конкретных ограничениях. Например, метаданные файла с изображением укажут на запрет коммерческого использования, сигнализируя разработчикам ИИ или конечным пользователям о том, что этот контент не может быть монетизирован без дополнительных разрешений. При стандартизации наборов данных такие метаданные могут быть интегрированы в рабочие процессы обучения ИИ, где алгоритмы смогут определять поля метаданных и отсеивать ограниченный контент, снижая риск несанкционированного использования.

В идеале применение метаданных в ИИ предполагает наличие стандартизированной схемы метаданных для контента, используемого в системах ИИ. Такая схема могла бы включать поля, специально предназначенные для использования ИИ, например, «Разрешено для обучения ИИ» или «Не для производных работ ИИ». Это позволило бы авторам указывать, может ли их работа способствовать созданию контента, генерируемого ИИ, и каким образом. Тем самым будет обеспечена прозрачность и подотчетность при обработке данных ИИ, а авторы смогут выбирать, каким образом их работы будут использоваться при обучении ИИ, соблюдая при этом Закон об авторском праве. Кроме того, с помощью метаданных можно отслеживать результаты работы ИИ – системы могут маркировать контент, созданный на основе наборов данных с определенными правами на использование, гарантируя, что все производные работы соответствуют заданным условиям. Такой подход полезен в правовом контексте, поскольку позволяет соблюдать нормы авторского права и одновременно поддерживает модель ответственного развития ИИ, которая признает и уважает права интеллектуальной собственности.

4.2. Пересмотр понятия авторства в аспекте сотворчества с искусственным интеллектом

Дело Zarya of the Dawn (2022) (рис. 4) ярко иллюстрирует изменения позиций авторского права в отношении контента, созданного ИИ, и важности вклада человека в определение авторских прав. Управление США по вопросам авторского права первоначально отказало в защите авторских прав на этот графический роман, созданный Крис Каштановой с помощью искусственного интеллекта. Основанием послужило то, что изображения, созданные с помощью программы Midjourney, не несут достаточного творческого вклада человека, чтобы претендовать на защиту авторских прав. Однако такая защита была предоставлена на авторское повествование и общую структуру комикса, что подчеркивает различие между компонентами, сгенерированными исключительно ИИ, и элементами, созданными человеком. Управление США по вопросам авторского права отметило, что закон об авторском праве, согласно § 102 раздела 17 Свода законов США, содержит требование оригинального авторства, которое ИИ сам по себе выполнить не может. Это решение демонстрирует, что Управление настаивает на сохранении творчества человека в качестве центрального элемента авторского права, то есть что значимый человеческий вклад необходим для юридического признания авторства (Klukosky & Kohel, 2024).



Рис. 4. Крис Каштанова, обложка графического романа "Zarya of the Dawn", 2022 (CC 0)

Учитывая современное состояние авторского права и то, что инструменты ГИИ, такие как Midjourney и DALL-E, предоставляют беспрецедентные возможности для создания произведений искусства, следует обратить особое внимание на тот факт, что для создания работ, охраняемых авторским правом, необходимы промпты и творческое руководство со стороны человека. Эти инструменты работают путем синтеза результатов, основанных на огромных массивах данных и алгоритмических шаблонах, что означает, что с юридической точки зрения они функционируют как продолжение человеческого замысла, а не как независимые творцы. Такой подход согласуется с юридическими прецедентами, такими как дела Feist Publications и Meshwerks, где было установлено, что оригинальность проистекает из творческих усилий человека, а не из механического воспроизведения. Следовательно, степень участия человека в управлении результатом имеет решающее значение для определения авторских прав на произведения, созданные с помощью ИИ (Militsyna, 2023).

Поэтому установление авторских прав на произведения, созданные ИИ, зависит от вида вклада человека, демонстрирующего оригинальность и принятие творческих решений. Это важнейшие компоненты авторского права (табл.). Например, разработка описаний – промптов – является важнейшим и основополагающим элементом участия человека в создании произведений искусства, генерируемых ИИ. С помощью подробных инструкций, определяющих стиль, композицию и тематическую направленность, человек-создатель закладывает концептуальную основу, которую затем выполняет инструмент ИИ. Этот процесс соответствует принципам, проиллюстрированным в деле Mannion v. Coors Brewing Co., где суд признал, что именно творческий выбор, например, освещения и кадрирования, придает фотографии оригинальность, необходимую для авторского права. Аналогичным образом, продуманное описание отражает уникальное творческое видение человека-пользователя и демонстрирует вклад человека в художественный процесс, давая возможность позиционировать результат как объект авторского права (Burylo, 2022).

Компоненты авторского права

Вид вклада человека	Описание	Правовой прецедент
Творческая разработка описания	Разработка подробного описания (например, указание на художественный стиль, композицию, тему) создает концептуальную основу для результатов работы ИИ, отражающих творческий потенциал и намерения человека	Mannion v. Coors Brewing Co.: Суд признал, что такие творческие решения, как освещение и кадрирование, делают произведение оригинальным
Отбор результатов	Отбор конкретных результатов работы ИИ из множества вариантов предполагает субъективный выбор, соответствующий художественному видению создателя, подобно тому, как фотограф выбирает финальные кадры	Garcia v. Google, Inc.: суд подчеркнул, что контроль окончательного варианта работы является необходимым условием авторства
Последующая обработка и совершенствование результата	Улучшение или изменение изображений, созданных искусственным интеллектом, путем корректировки цветов, изменения композиции или добавления элементов вносит уникальный элемент творчества, превращая результат в производное произведение, отражающее творческие способности человека	Meshwerks, Inc. v. Toyota Motor Sales, U.S.A., Inc.: суд постановил, что существенные изменения позволяют считать произведение оригинальным
Концептуальный замысел и художественная идея	Всеобъемлющее художественное видение и тематика (например, социальные проблемы, эстетика), привнесенные человеком-создателем, определяют суть конечного произведения, свидетельствуя о его оригинальности	Feist Publications, Inc. v. Rural Telephone Service Co.: суд подчеркнул требование к оригинальности, предполагающее творческий подход и замысел
Критерий авторства человека	Степень участия человека, включая текстовые и повествовательные элементы, определяет авторское право; недостаточно наличия контента, созданного только искусственным интеллектом	Решение Управления США по вопросам авторского права по делу Zarya of the Dawn: установлено авторское право на повествование, написанное человеком, но не на изображения, сгенерированные ИИ без участия человека
Создание производных работ	Преобразование результатов работы ИИ с помощью творческих корректировок соответствует принципам оригинальности, поскольку защита авторских прав может распространяться на производные работы, если вклад человека в них значителен	§ 101 раздела 17 Свода законов США: производные произведения определяются как работы, которые преобразуют или развивают ранее существовавшие материалы путем творческих дополнений

Еще одним ключевым показателем авторства человека является процесс отбора результатов из множества сгенерированных ИИ вариантов. Как фотограф перебирает множество снимков, чтобы найти те, которые лучше всего соответствуют его художественному замыслу, так и процесс выбора конкретных результатов работы ИИ из множества сгенерированных вариантов представляет собой отдельный уровень творческого самовыражения. Такой процесс принятия решений является неотъемлемой частью формирования конечной работы и воплощает уникальное художественное видение автора, что дает основание для защиты авторских прав. При выборе одной версии вместо другой автор выносит субъективное суждение, согласуя результат со своим определенным видением и подчеркивая незаменимость человеческого выбора (Wan & Lu, 2021).

Далее, процессы последующей обработки и доработки результатов вносят значительный вклад в установление авторских прав. Когда автор изменяет сгенерированное ИИ изображение, улучшает его элементы, корректирует цветовые решения

или изменяет композицию, он вводит новые творческие измерения, которые поднимают работу выше простого автоматического результата. Такая форма вклада человека отражена в деле Meshwerks, где суд отметил, что существенные изменения придают свойство оригинальности цифровым изображениям. В контексте ИИ существенная обработка превращает созданный контент в производное произведение, несущее отпечаток человеческого творчества, что служит основанием для защиты авторских прав и подчеркивает важную роль человека в творческом преобразовании (Geiger, 2024).

Помимо технической составляющей, основополагающее значение для установления авторства имеют концептуальный замысел и художественная идея, которыми руководствуются при использовании инструментов ИИ. Независимо от того, используются ли инструменты ИИ для исследования сложных социальных тем, передачи конкретных сообщений или воплощения определенной эстетической философии, именно видение человека-создателя в конечном итоге формирует суть произведения. Эта концепция тесно перекликается с выводами по делу Mannion, где суд признал творческие решения фотографа ключевым фактором, определяющим авторское право на произведение. В произведениях, создаваемых ИИ, именно намерения человека и его философский подход обеспечивают соответствие требованию оригинальности в Законе об авторском праве, подтверждая, что ИИ – это инструмент, служащий широким художественным целям человека-создателя (Kasap, 2021).

Каждый из видов вклада человека отражает спектр творческого участия, который отличает работы, созданные с помощью ИИ, от простого алгоритмического результата. Эти элементы – от конкретизации описаний до отбора вариантов, от существенной пост-обработки до выбора тематики – подчеркивают, что значимое человеческое творчество остается центральным основанием претензий на авторское право в эпоху ИИ. Технология ИИ все более совершенствуется, однако необходимость значительного вклада человека всегда будет оставаться краеугольным камнем авторского права, поддерживая баланс между технологическими инновациями и признанием авторства человека.

Разнообразие видов вклада человека говорит о том, что ИИ следует понимать как инструмент, расширяющий, а не заменяющий человеческое творчество. Как указано в «Сборнике практических решений» Управления США по вопросам авторского права, чтобы произведение соответствовало стандарту оригинальности, требуемому Законом об авторском праве, вклад человека должен быть значительным. Этот принцип подкрепляет позицию Управления в деле Zarya of the Dawn и согласуется с § 102 раздела 17 Свода законов США, в котором подчеркивается критерий авторства человека. В будущем авторское право в контексте ИИ, вероятно, также будет фокусироваться на том, является ли творческий вклад человека достаточно значительным, чтобы соответствовать порогу оригинальности (Fenwick & Jurcys, 2023).

Ряд практик усиливают основания для защиты авторских прав при использовании инструментов ИИ. Во-первых, это разработка детального описания, демонстрирующего оригинальность и креативность произведения. Во-вторых, это отбор вариантов из сгенерированных ИИ результатов, отражающий художественное видение автора. В-третьих, значительная последующая обработка превращает результат работы ИИ в производное произведение, подчеркивая вклад человека. И наконец, обеспечение целостности концептуальной структуры, отражающей замысел художника. Все это служит обоснованием для защиты авторского права, подтверждая, что ИИ является просто сложным инструментом, а не независимым творцом. Исходя из

этих соображений, потенциальный пересмотр рамок авторского права может привести к созданию новой категории, признающей работы, созданные с помощью ИИ, в качестве продукта совместного творчества. Определяя ИИ как инструмент, способствующий творчеству, а не как независимого творца, авторское право может разрешить существующее противоречие, признав роль как человека, так и ИИ. Такой подход позволяет уважать творческие способности человека и в то же время учитывать возможности ИИ, гарантируя, что Закон об авторском праве останется актуальным в условиях творческого ландшафта, все более интегрированного с технологиями ИИ.

Заключение

По мере расширения присутствия искусственного интеллекта в творческих областях возникает необходимость в новой правовой базе, позволяющей сбалансировать инновации и защиту авторских прав человека. Существующие структуры авторского права, в основном разработанные на основе традиционных концепций человеческого творчества, сталкиваются с проблемами при рассмотрении произведений, созданных ИИ. Пересмотр правовой базы позволит учесть уникальные возможности ИИ, сохраняя при этом основные принципы авторского права и подчеркивая, что творческая деятельность человека по-прежнему важна для признания авторства. Ученые предлагают адаптивную модель авторского права, закрепляющую роль ИИ как инструмента человеческого творчества, не предоставляя самому ИИ защиту авторских прав (Geiger, 2024). При формировании этой системы законодателям необходимо найти тонкий баланс между стимулированием технологических инноваций и обеспечением сохранения контроля авторов над своей интеллектуальной собственностью. По мере того как системы ИИ становятся все более автономными, растут требования к прозрачности, соблюдению этических стандартов и защите прав. Сбалансированный подход предполагает создание отдельной правовой категории для совместных работ человека и ИИ, признавая ИИ в качестве инструмента и одновременно защищая центральную роль человека в творческом процессе.

Что касается будущих совместных работ человека и ИИ, то развивающиеся возможности ИИ предполагают постепенное изменение объема и вида вклада человека, необходимого для обеспечения защиты авторских прав. Аспекты творческого процесса могут все больше автоматизироваться посредством технологий ИИ, однако правовая база, скорее всего, будет по-прежнему подчеркивать вклад человека как основополагающий фактор оригинальности. Признание ИИ в качестве соавтора при соблюдении строгих правил может помочь определить новую модель авторства, в которой ИИ способствует человеческим инновациям, но не заменяет их. Практические последствия для авторского права связаны с усилением человеческого фактора в творческих процессах. ИИ может генерировать сложные результаты, но авторское право должно основываться на очевидном вкладе человека. Принятие критериев значимого человеческого вклада, такого как творческие описания или постобработка, должно послужить основой для определения авторства и защиты прав авторов в мире, неотъемлемой частью которого является ИИ.

Этот развивающийся правовой ландшафт также влечет за собой этические последствия. Принятие ИИ в качестве творческого инструмента способствует созданию модели устойчивого сотворчества, в которой ИИ расширяет творческие возможности человека, а не конкурирует с ним. Встраивая принципы прозрачности

и справедливости в систему авторского права, законодатели могут защитить индивидуальные права, поощряя ответственное использование ИИ в творческих областях. В конечном итоге баланс между защитой и инновациями в эпоху ИИ требует как гибкости, так и последовательности правовых норм. Авторское право должно развиваться, чтобы отражать трансформационный потенциал ИИ и одновременно укреплять заложенные в нем принципы, ориентированные на человека. Благодаря правовым реформам творческая индустрия сможет извлечь выгоду из достижений технологии ИИ, не подрывая основополагающую роль авторства человека.

Список литературы

Aaland, M. (2006). *Photoshop Elements 3 Solutions: The Art of Digital Photography*. John Wiley & Sons.

Abbott, R., & Rothman, E. (2023). Disrupting creativity: Copyright law in the age of generative artificial intelligence. *Florida Law Review*, *75*, 1141–1201.

Atilla, S. (2024). Dealing with AI-generated works: lessons from the CDPA section 9 (3). *Journal of Intellectual Property Law and Practice*, *19*(1), 43–54. https://doi.org/10.1093/jiplp/jpad102

Bonnet, S., & Teuteberg, F. (2023). Impact of blockchain and distributed ledger technology for the management of the intellectual property life cycle: A multiple case study analysis. *Computers in Industry*, *144*, 103789. https://doi.org/10.1016/j.compind.2022.103789

Bridy, A. (2016). The Evolution of Authorship: Work Made by Code. *Columbia Journal of Law and the Arts*, *39*, 395–401. https://doi.org/10.7916/D8CV4J6W

Burylo, Y. (2022). AI generated works and copyright protection. *Entrepreneurship, Economy and Law*, *3*, 7–13. https://doi.org/10.32849/2663-5313/2022.3.01

Dimitrova, R. (2023). Are AI-Assisted Works Copyrightable? In *2023 International Scientific Conference on Computer Science (COMSCI)*, Sozopol, Bulgaria (pp. 1–4). https://doi.org/10.1109/COMSCI59259.2023.10315917

Elkin-Koren, N., Hacohen, U., Livni, R., & Moran, S. (2023). Can Copyright be Reduced to Privacy? *arXiv*, 2305.14822. https://doi.org/10.48550/arXiv.2305.14822

Epstein, Z., Hertzmann, A., Akten, M., Farid, H., Fjeld, J., Frank, M. R., Groh, M., Herman, L., Leach, N., Mahari, R., Pentland, A. "Sandy", Russakovsky, O., Schroeder, H., & Smith, A. (2023). Art and the science of generative AI. *Science*, *380*(6650), 1110–1111. https://doi.org/10.1126/science.adh4451

Fenwick, M., & Jurcys, P. (2023, February 11). *Originality and the future of copyright in an age of generative AI*.

Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering*, *66*(1), 111–126. https://doi.org/10.1007/s12599-023-00834-7

Geiger, C. (2024). Elaborating a Human Rights friendly Copyright Framework for Generative AI. *International Review for Intellectual Property and Competition Law*, *55*(7), 1129–1165. https://doi.org/10.2139/ssrn.4634992

Gervais, D. (2022). AI Derivatives: the Application to the Derivative Work Right to Literary and Artistic Productions of AI Machines. *Seton Hall Law Review*, *53*, 1111–1136. https://doi.org/10.2139/ssrn.4022665

Hedrick, S. F. (2018). I "think," therefore I create: claiming copyright in the outputs of algorithms. *NYU Journal of Intellectual Property & Entreprenurial Law*, *8*(2), 324–375.

Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., & Liang, P. (2023). Foundation Models and Fair Use. *arXiv*, 2303.15715. https://doi.org/10.48550/arXiv.2303.15715

Horzyk, A. (2023). How AI Affects Our Understanding of Musical Works That Should Be Protected by Copyright. In *2023 International Joint Conference on Neural Networks (IJCNN)*, Gold Coast, Australia (pp. 1–8). https://doi.org/10.1109/IJCNN54540.2023.10191524

Hutson, J., Lively, J., Robertson, B., Cotroneo, P., & Lang, M. (2023). Expanding Horizons: AI Tools and Workflows in Art Practice. In *Creative Convergence: The AI Renaissance in Art and Design* (pp. 101–132). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45127-0_5

Iaia, V. (2022). To Be, or Not to Be… Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works. *GRUR International*, *71*(9), 793–812. https://doi.org/10.1093/grurint/ikac087

James, T. B. (2024). Artificial Intelligence, Copyright Registration, and the Rule of Doubt. *Texas A&M Law Review Arguendo*, *12*(1), 20–31. https://doi.org/10.37419/lr.v12.arg.2

Jiang, H. H., Brown, L., Cheng, J., Khan, M., Gupta, A., Workman, D., & Gebru, T. (2023). AI Art and its Impact on Artists. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 363–374). https://doi.org/10.1145/3600211.3604681

Kasap, A. (2021). Copyright and creative artificial intelligence (AI) systems: A twenty-first century approach to authorship of AI-generated works in the United States. *Wake Forest Journal of Business & Intellectual Property Law*, *19*(4), 335–380. https://doi.org/10.31235/osf.io/gnyha

Kelby, S. (2020). *The digital photography book.* Rocky Nook. Inc.

Kibirige, H. (2024). The delving conundrum of intellectual property rights in the transformative era of artificial intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4841535

Klukosky, F. P., & Kohel, M. D. (2024). An Update on the State of Play with Generative Artificial Intelligence and Intellectual Property Issues. *Intellectual Property Litigation*, *34*(1), 10–17.

Kretschmer, M., Margoni, T., & Oruç, P. (2024). Copyright law and the lifecycle of machine learning models. *IIC-International Review of Intellectual Property and Competition Law*, *55*(1), 110–138. https://doi.org/10.1007/s40319-023-01419-3

Longpre, S., Mahari, R., Chen, A., Obeng-Marnu, N., Sileo, D., Brannon, W., Muennighoff, N., Khazam, N., Kabbara, J., Perisetla, K., Wu, X., Shippole, E., Bollacker, K., Wu, T., Villa, L., Pentland, S., & Hooker, S. (2023). The data provenance initiative: A large scale audit of dataset licensing & attribution in AI. *arXiv*, 2310.16787. https://doi.org/10.48550/arXiv.2310.16787

Lucchi, N. (2024). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation, 15*(3), 602–624. https://doi.org/10.1017/err.2023.59

Majumdar, S., Paul, S., Paul, D., Bandyopadhyay, A., Chattopadhyay, S., Das, P. P., & Majumder, P. (2023). Generative AI for software metadata: Overview of the information retrieval in software engineering track at FIRE 2023. arXiv, 2311.03374. https://doi.org/10.48550/arXiv.2311.03374

McCann, S. (2021). Copyright Throughout a Creative AI Pipeline. *Canadian JL & Tech*, *19*(1), 109–139. https://doi.org/10.2139/ssrn.3893972

Mensah, G. B. (2023). *Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems*. Preprint, November, 10. https://doi.org/10.13140/RG.2.2.23381.19685/1

Mia, M., Wessels, J., & Adam, S. (2023). The Use of Blockchain Technology to Improve Transfer-Pricing Compliance and Administration in South Africa. In *ICABR Conference* (pp. 357–378). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46177-4_20

Militsyna, K. (2023). Human Creative Contribution to AI-Based Output – One Just Can('t) Get Enough. *GRUR International*, *72*(10), 939–949. https://doi.org/10.1093/grurint/ikad075

Moreno, H., Gómez, A., Altares-López, S., Ribeiro, A., & Andújar, D. (2023). Analysis of Stable Diffusion-derived fake weeds performance for training Convolutional Neural Networks. *Computers and Electronics in Agriculture*, *214*, 108324. https://doi.org/10.1016/j.compag.2023.108324

Pellegrini, T. (2023). Digital Rights Management – Technologies, Application Areas, and Governance. In *Handbook of Media and Communication Economics: A European Perspective* (pp. 1–17). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34048-3_79-2

Ploman, E. W., & Hamilton, L. C. (2024). *Copyright: Intellectual property in the information age*. Taylor & Francis. https://doi.org/10.4324/9781003519973

Risi, S., & Togelius, J. (2020). Increasing generality in machine learning through procedural content generation. *Nature Machine Intelligence*, *2*(8), 428–436. https://doi.org/10.1038/s42256-020-0208-z

Samuelson, P. (2023). Generative AI meets copyright. *Science*, *381*(6654), 158–161. https://doi.org/10.1126/science.adi0656

Sobel, B. (2021). A Taxonomy of Training Data. In R. Hilty, J.-A. Lee, & K.-Ch. Liu (Eds.), *Artificial Intelligence and Intellectual Property*. Oxford University Press. https://doi.org/10.1093/oso/9780198870944.003.0011

Spica, E. (2024). Public Interest, the True Soul: Copyright's Fair Use Doctrine and the Use of Copyrighted Works to Train Generative AI Tools. *Texas Intellectual Property Law Journal*, *33*(1), 67–91.

Torrance, A., & Tomlinson, B. (2023). Training Is Everything: Artificial Intelligence, Copyright, and Fair Training. *arXiv*, 2305.03720. https://doi.org/10.48550/arXiv.2305.03720

Wagh, S., Peerzada, D., & Rote, P. (2023). AI And Copyright. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(3), 3431–3439. https://doi.org/10.52783/tjjpt.v44.i3.2053

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, 42, 105581. https://doi.org/10.1016/J.CLSR.2021.105581

Yu, R. (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, *165*, 1245–1270.

Сведения об авторе



Джеймс Хатсон – PhD, ведущий специалист в области дополненной реальности; профессор, заведующий кафедрой истории искусств, искусственного интеллекта и визуальной культуры; факультет искусств и гуманитарных дисциплин, Линденвудский университет
Адрес: МО 63301, США, г. Сент Чарльз, ул. С. Кингзхайвей, 209
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57797793000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/38589773
Google Scholar ID: https://scholar.google.com/citations?user=CaXrV38AAAAJ

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: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 29 октября 2024 г.
Дата одобрения после рецензирования – 10 ноября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/shduef
DOI: https://doi.org/10.21202/jdtl.2024.43

The Evolving Role of Copyright Law in the Age of AI-Generated Works

James Hutson
Lindenwood University, Saint Charles, United States

Keywords

artificial intelligence,
copyright,
copyright protection,
digital technologies,
generative artificial intelligence,
intellectual property right,
law,
machine learning technologies,
prompt engineering,
work of art

Abstract

Objective: to identify the prospects and directions of copyright law development associated with the increasing use of generative artificial intelligence.

Methods: the study is based on the formal-legal, comparative, historical methods, doctrinal analysis, legal forecasting and modeling.

Results: the article states that the emergence of generative artificial intelligence makes one rethink the processes occurring in the field of creative activity and the traditional copyright system, which becomes inadequate to modern realities. The author substantiates the necessity of legal reassessment of copyright and emphasizes the urgent need for updated means of copyright protection. Unlike previous digital tools, which expanded human creativity by improving original works, generative artificial intelligence creates content through complex algorithmic processes, blurring the boundaries of authorship and originality. The research shows limitations of existing intellectual property law, as courts deny copyright in works created by artificial intelligence and insist on the need for "human authorship". Such decisions emphasize the contradiction between existing laws and the reality of co-creation involving artificial intelligence. It is argued that taking into account the creative potential of generative artificial intelligence will facilitate the evolution of copyright law towards hybrid approaches, with artificial intelligence as an integral, albeit secondary, tool. It seems promising to create flexible intellectual property standards that give artists the opportunity to restrict or authorize the use of their works as training data for artificial

© Hutson J., 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.

intelligence, as well as ensure that authors retain control over their works included in datasets for training artificial intelligence, in case copyright metadata is integrated into digital works, etc.

Scientific novelty: based on the analysis of the latest judicial precedents, modern international regulations and evolving institutional practices, the author proposes a balanced adaptive approach to copyright reform to ensure the ethical integration of generative artificial intelligence into the creative ecosystem and to develop flexible copyright protection measures that correspond to the rapid technological progress.

Practical significance: the proposed combined approach will allow generative AI tools to become part of the human creative process in the same way that previous generations used digital tools. At the same time, it will contribute to the creation of an environment where the autonomy of authors is respected. This will not only protect the creators of creative content, but also broaden the understanding of creativity as a collaboration with generative artificial intelligence, where artificial intelligence is positioned as a force that complements but not replaces humans in creativity.

For citation

Hutson, J. (2024). The Evolving Role of Copyright Law in the Age of AI-Generated Works. *Journal of Digital Technologies and Law, 2*(4), 886–914. https://doi.org/10.21202/jdtl.2024.43

References

Aaland, M. (2006). *Photoshop Elements 3 Solutions: The Art of Digital Photography*. John Wiley & Sons.

Abbott, R., & Rothman, E. (2023). Disrupting creativity: Copyright law in the age of generative artificial intelligence. *Florida Law Review*, *75*, 1141–1201.

Atilla, S. (2024). Dealing with AI-generated works: lessons from the CDPA section 9 (3). *Journal of Intellectual Property Law and Practice*, *19*(1), 43–54. https://doi.org/10.1093/jiplp/jpad102

Bonnet, S., & Teuteberg, F. (2023). Impact of blockchain and distributed ledger technology for the management of the intellectual property life cycle: A multiple case study analysis. *Computers in Industry*, *144*, 103789. https://doi.org/10.1016/j.compind.2022.103789

Bridy, A. (2016). The Evolution of Authorship: Work Made by Code. *Columbia Journal of Law and the Arts*, *39*, 395–401. https://doi.org/10.7916/D8CV4J6W

Burylo, Y. (2022). AI generated works and copyright protection. *Entrepreneurship, Economy and Law*, *3*, 7–13. https://doi.org/10.32849/2663-5313/2022.3.01

Dimitrova, R. (2023). Are AI-Assisted Works Copyrightable? In *2023 International Scientific Conference on Computer Science (COMSCI)*, Sozopol, Bulgaria (pp. 1–4). https://doi.org/10.1109/COMSCI59259.2023.10315917

Elkin-Koren, N., Hacohen, U., Livni, R., & Moran, S. (2023). Can Copyright be Reduced to Privacy? *arXiv*, 2305.14822. https://doi.org/10.48550/arXiv.2305.14822

Epstein, Z., Hertzmann, A., Akten, M., Farid, H., Fjeld, J., Frank, M. R., Groh, M., Herman, L., Leach, N., Mahari, R., Pentland, A. "Sandy", Russakovsky, O., Schroeder, H., & Smith, A. (2023). Art and the science of generative AI. *Science*, *380*(6650), 1110–1111. https://doi.org/10.1126/science.adh4451

Fenwick, M., & Jurcys, P. (2023, February 11). *Originality and the future of copyright in an age of generative AI.*

Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. *Business & Information Systems Engineering*, *66*(1), 111–126. https://doi.org/10.1007/s12599-023-00834-7

Geiger, C. (2024). Elaborating a Human Rights friendly Copyright Framework for Generative AI. *International Review for Intellectual Property and Competition Law*, *55*(7), 1129–1165. https://doi.org/10.2139/ssrn.4634992

Gervais, D. (2022). AI Derivatives: the Application to the Derivative Work Right to Literary and Artistic Productions of AI Machines. *Seton Hall Law Review*, *53*, 1111–1136. https://doi.org/10.2139/ssrn.4022665

Hedrick, S. F. (2018). I "think," therefore I create: claiming copyright in the outputs of algorithms. *NYU Journal of Intellectual Property & Entreprenurial Law*, *8*(2), 324–375.

Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M., & Liang, P. (2023). Foundation Models and Fair Use. *arXiv*, 2303.15715. https://doi.org/10.48550/arXiv.2303.15715

Horzyk, A. (2023). How AI Affects Our Understanding of Musical Works That Should Be Protected by Copyright. In *2023 International Joint Conference on Neural Networks (IJCNN)*, Gold Coast, Australia (pp. 1–8). https://doi.org/10.1109/IJCNN54540.2023.10191524

Hutson, J., Lively, J., Robertson, B., Cotroneo, P., & Lang, M. (2023). Expanding Horizons: AI Tools and Workflows in Art Practice. In *Creative Convergence: The AI Renaissance in Art and Design* (pp. 101–132). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45127-0_5

Iaia, V. (2022). To Be, or Not to Be… Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works. *GRUR International*, *71*(9), 793–812. https://doi.org/10.1093/grurint/ikac087

James, T. B. (2024). Artificial Intelligence, Copyright Registration, and the Rule of Doubt. *Texas A&M Law Review Arguendo*, *12*(1), 20–31. https://doi.org/10.37419/lr.v12.arg.2

Jiang, H. H., Brown, L., Cheng, J., Khan, M., Gupta, A., Workman, D., & Gebru, T. (2023). AI Art and its Impact on Artists. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 363–374). https://doi.org/10.1145/3600211.3604681

Kasap, A. (2021). Copyright and creative artificial intelligence (AI) systems: A twenty-first century approach to authorship of AI-generated works in the United States. *Wake Forest Journal of Business & Intellectual Property Law*, *19*(4), 335–380. https://doi.org/10.31235/osf.io/gnyha

Kelby, S. (2020). *The digital photography book.* Rocky Nook. Inc.

Kibirige, H. (2024). The delving conundrum of intellectual property rights in the transformative era of artificial intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4841535

Klukosky, F. P., & Kohel, M. D. (2024). An Update on the State of Play with Generative Artificial Intelligence and Intellectual Property Issues. *Intellectual Property Litigation*, *34*(1), 10–17.

Kretschmer, M., Margoni, T., & Oruç, P. (2024). Copyright law and the lifecycle of machine learning models. *IIC-International Review of Intellectual Property and Competition Law*, *55*(1), 110–138. https://doi.org/10.1007/s40319-023-01419-3

Longpre, S., Mahari, R., Chen, A., Obeng-Marnu, N., Sileo, D., Brannon, W., Muennighoff, N., Khazam, N., Kabbara, J., Perisetla, K., Wu, X., Shippole, E., Bollacker, K., Wu, T., Villa, L., Pentland, S., & Hooker, S. (2023). The data provenance initiative: A large scale audit of dataset licensing & attribution in AI. *arXiv*, 2310.16787. https://doi.org/10.48550/arXiv.2310.16787

Lucchi, N. (2024). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation, 15*(3), 602–624. https://doi.org/10.1017/err.2023.59

Majumdar, S., Paul, S., Paul, D., Bandyopadhyay, A., Chattopadhyay, S., Das, P. P., & Majumder, P. (2023). Generative AI for software metadata: Overview of the information retrieval in software engineering track at FIRE 2023. arXiv, 2311.03374. https://doi.org/10.48550/arXiv.2311.03374

McCann, S. (2021). Copyright Throughout a Creative AI Pipeline. *Canadian JL & Tech*, *19*(1), 109–139. https://doi.org/10.2139/ssrn.3893972

Mensah, G. B. (2023). *Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems*. Preprint, November, 10. https://doi.org/10.13140/RG.2.2.23381.19685/1

Mia, M., Wessels, J., & Adam, S. (2023). The Use of Blockchain Technology to Improve Transfer-Pricing Compliance and Administration in South Africa. In *ICABR Conference* (pp. 357–378). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46177-4_20

Militsyna, K. (2023). Human Creative Contribution to AI-Based Output – One Just Can('t) Get Enough. *GRUR International*, *72*(10), 939–949. https://doi.org/10.1093/grurint/ikad075

Moreno, H., Gómez, A., Altares-López, S., Ribeiro, A., & Andújar, D. (2023). Analysis of Stable Diffusion-derived fake weeds performance for training Convolutional Neural Networks. *Computers and Electronics in Agriculture*, *214*, 108324. https://doi.org/10.1016/j.compag.2023.108324

Pellegrini, T. (2023). Digital Rights Management – Technologies, Application Areas, and Governance. In *Handbook of Media and Communication Economics: A European Perspective* (pp. 1–17). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34048-3_79-2

Ploman, E. W., & Hamilton, L. C. (2024). *Copyright: Intellectual property in the information age*. Taylor & Francis. https://doi.org/10.4324/9781003519973

Risi, S., & Togelius, J. (2020). Increasing generality in machine learning through procedural content generation. *Nature Machine Intelligence*, *2*(8), 428–436. https://doi.org/10.1038/s42256-020-0208-z

Samuelson, P. (2023). Generative AI meets copyright. *Science*, *381*(6654), 158–161. https://doi.org/10.1126/science.adi0656

Sobel, B. (2021). A Taxonomy of Training Data. In R. Hilty, J.-A. Lee, & K.-Ch. Liu (Eds.), *Artificial Intelligence and Intellectual Property*. Oxford University Press. https://doi.org/10.1093/oso/9780198870944.003.0011

Spica, E. (2024). Public Interest, the True Soul: Copyright's Fair Use Doctrine and the Use of Copyrighted Works to Train Generative AI Tools. *Texas Intellectual Property Law Journal*, *33*(1), 67–91.

Torrance, A., & Tomlinson, B. (2023). Training Is Everything: Artificial Intelligence, Copyright, and Fair Training. *arXiv*, 2305.03720. https://doi.org/10.48550/arXiv.2305.03720

Wagh, S., Peerzada, D., & Rote, P. (2023). AI And Copyright. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(3), 3431–3439. https://doi.org/10.52783/tjjpt.v44.i3.2053

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, 42, 105581. https://doi.org/10.1016/J.CLSR.2021.105581

Yu, R. (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, *165*, 1245–1270.

Author information



James Hutson – PhD, Lead XR Disruptor; Professor and Department Head of Art History, AI, and Visual Culture, College of Arts and Humanities, Lindenwood University
Address: 209 S. Kingshighway St, MO 63301, Saint Charles, United States
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57797793000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/38589773
Google Scholar ID: https://scholar.google.com/citations?user=CaXrV38AAAAJ

Conflict of interest

The author declare 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 – October 29, 2024
Date of approval – November 10, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:343.9:004.8
EDN: https://elibrary.ru/jvglrh
DOI: https://doi.org/10.21202/jdtl.2024.44

Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности

Амину Мухаммад Аувал

Университет Джоса, Джос, Нигерия

Сулеман Лазарус ✉

Лондонская школа экономики и политических наук, Лондон, Великобритания
Университет Суррея, Гилфорд, Великобритания
Портсмутский университет, Портсмут, Великобритания

Ключевые слова

виктимизация,
виктимология,
жертва киберпреступления,
киберкриминология,
киберпреступность,
кибершпионаж,
онлайн-мошенничество,
правовая политика,
цифровая криминология,
цифровые технологии

Аннотация

Цель: выявление основных проблем виктимизации в результате роста киберпреступности в мире в целом и в нигерийском обществе в частности с позиций социологических подходов и с помощью трехчастной концепции киберпреступности (Tripartite Cybercrime Framework, TCF), состоящей из геополитических, психосоциальных и социально-экономических категорий киберпреступности.

Методы: основу методологии составили социологический метод исследования. Процесс сбора данных включал распространение опросника среди 896 участников из академической среды, в том числе студентов и сотрудников университета, и анализ ответов респондентов. Представленные данные анализировались с помощью описательной статистики, особое внимание при этом было уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к онлайн-мошенничеству и виктимизации в результате киберпреступлений через призму концепции идеальной жертвы и социально-экономического разрыва между Севером и Югом.

Результаты: в статье представлен анализ трехчастной концепции киберпреступности. На основе изучения данных, полученных в ходе анкетирования, установлено, что 65,20 % участников опроса когда-либо становились жертвами киберпреступников. Выявлен гендерный перекос среди жертв киберпреступлений в сторону мужчин (64,69 %).

✉ Корреспондирующий автор
© Аувал А. М., Лазарус 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.

Установлены закономерности в распределении киберпреступлений. Все киберпреступления против опрошенных лиц относились к категории социально-экономических, что подчеркивает распространенность киберпреступности и актуальность противодействия ей в нигерийском социуме. Особое внимание уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к киберпреступлениям. Проблема виктимизации рассмотрена с точки зрения концепции идеальной жертвы. **Результаты** исследования позволяют получить представление о распространенности и распределении конкретных видов киберпреступности социально-экономической категории среди исследуемой группы населения.

Научная новизна: в исследовании впервые используется подход трехчастной концепции киберпреступности (TCF) для изучения виктимизации в результате киберпреступлений в нигерийском обществе. Новизна представленного исследования обусловлена еще и тем, что сложившиеся на глобальном Севере концептуальные основы противодействия киберпреступности не вполне применимы в Нигерии.

Практическая значимость: полученные результаты демонстрируют необходимость применения тщательно выверенных гендерных, инклюзивных и контекстуальных подходов к разработке национальной правовой политики борьбы с киберпреступностью, могут быть положены в обоснование разрабатываемых правотворческих решений в области предупреждения и противодействия проявлениям киберпреступности, а также в основу правовых мер защиты жертв киберпреступлений.

Для цитирования

Аувал, А. М., Лазарус, С. (2024). Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности. *Journal of Digital Technologies and Law*, *2*(4), 915–942. https://doi.org/10.21202/jdtl.2024.44

Содержание

Введение
1. Обзор литературы
   1.1. Киберпреступность и киберкриминология
   1.2. Трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF)
      1.2.1. Геополитическая категория киберпреступности
      1.2.2. Психосоциальная категория киберпреступности
      1.2.3. Социально-экономическая категория киберпреступности
   1.3. Проблемы и вызовы киберпреступности в Нигерии
   1.4. Рост экономической киберпреступности в Нигерии
   1.5. Исследования, ориентированные на жертв преступности
   1.6. Киберпреступники в нигерийском обществе (Yahoo Boys)
   1.7. Сходство и различия с предыдущими исследованиями
   1.8. Новизна данной работы

2. Методы и материалы
2.1. Анализ данных
3. Результаты
3.1. Гендерный аспект
3.2. Уровень образования
3.3. Подтвержденный негативный опыт в сфере киберпреступности
3.4. Типы киберпреступлений
3.5. Сообщения об инцидентах
3.6. Возврат украденных денег/Принятие соответствующих мер
4. Обсуждение
4.1. Гендерный аспект виктимизации в результате онлайн-мошенничества
4.2. Роль киберпреступности в социально-экономической динамике
4.3. Уровень образования жертв онлайн-мошенничества
4.4. Виктимизация в результате киберпреступлений, концепция идеальной жертвы и разрыв между Севером и Югом
Заключение
Список литературы

Введение

Киберпреступность – глобальная проблема, однако пространственные характеристики влияют на поведение людей на местном уровне и могут быть выявлены или скрыты с помощью пространственных элементов (Hall & Yarwood, 2024; Lazarus & Button, 2022). Цель данной статьи – описать ситуацию с киберпреступностью и провести количественный анализ эмпирических данных. Киберпреступность представляет собой серьезную социальную проблему в Нигерии; в последние годы ее распространенность возросла (Ibrahim, 2016a; Idem & Olarinde, 2023). Жертвам киберпреступности в различных контекстах посвящены многие научные труды. Например, эту проблему изучали в Австралии (Cross, 2020; Drew & Webster, 2024), Китае (Wang, 2023), Португалии (Murça et al., 2024), Великобритании (Lazarus et al., 2022b), России (Timofeyev & Dremova, 2022). Жертвам киберпреступности в Нигерии посвящены лишь несколько исследований. В отличие от других стран, особенно таких как Австралия (Cross, 2020; Drew & Websters, 2024; Meikle & Cross, 2024) и Великобритания (Button et al., 2014, 2015, 2021), в Нигерии исследований жертв киберпреступности недостаточно.

Например, в работе Aborisade et al. (2024) были использованы интерпретативный феноменологический анализ и полуструктурированные видеоинтервью; опрошены десять жертв нигерийских брачных аферистов из шести разных стран. В исследовании Tade и Adeniyi (2017) проанализированы данные, полученные в ходе подробных интервью с жертвами мошенничества с банкоматами; было показано, что жертвы получили психологическую травму и часто обращались к друзьям, родителям и родственникам, чтобы справиться с последствиями. Однако ни в одном из этих исследований не использовались количественные методы для изучения демографических характеристик респондентов и их опыта борьбы

с киберпреступностью. Наша работа направлена на устранение этого пробела путем изучения демографических характеристик и опыта респондентов в отношении киберпреступности. В частности, была предпринята попытка изучить распространенность, характеристики и динамику сообщений о киберпреступлениях среди респондентов. Исследование призвано внести вклад в недостаточно разработанную тему виктимизации в результате киберпреступлений в нигерийском обществе, используя данные, собранные в ходе распределенного опроса.

1. Обзор литературы

1.1. Киберпреступность и киберкриминология

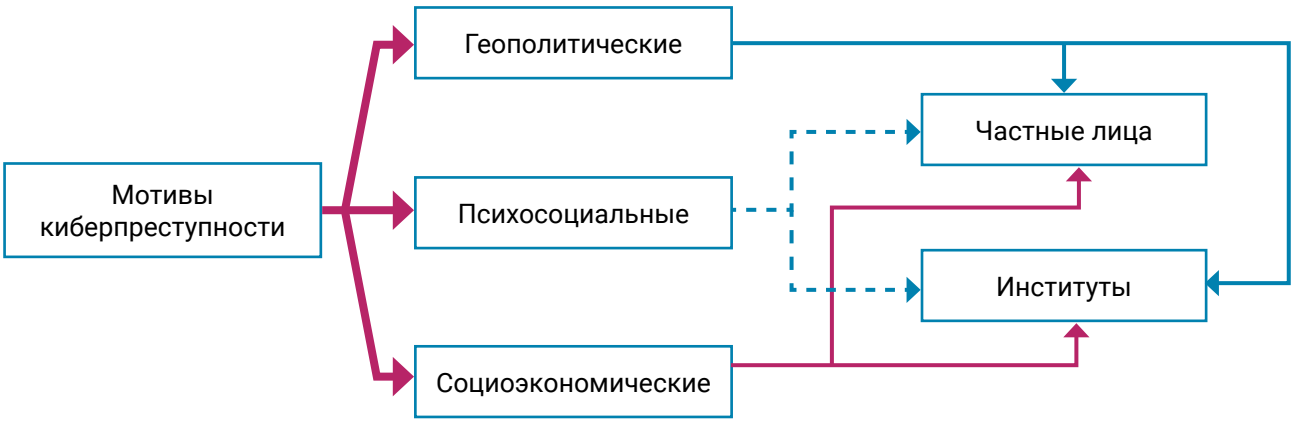
Идея о том, что разделение между физическим и цифровым мирами препятствует пониманию социальных сигналов в автономном режиме, которые также влияют на цифровую сферу, получила развитие в ряде работ (Jaishankar, 2007; Ibrahim, 2016a; Powell et al., 2018). Говоря о связи между офлайн- и онлайн-реальностью, исследователи использовали разные термины для выражения этой концепции. Например, McGerty (2000) писал, что «никто не живет только в киберпространстве», Jaishankar (2007, 2011, 2018) ввел понятие «киберкриминология», в то время как Powell с соавторами (2018) переименовали его в «цифровую криминологию». Эти различия в терминологии отражают споры в рамках научного дискурса по этой теме.

Понятие «киберпреступность» охватывает противоправную деятельность, осуществляемую с помощью Интернета и информационно-коммуникационных технологий (далее – ИКТ), включая «киберзависимые преступления» и «киберпреступления с использованием компьютерных технологий» (Button et al., 2023; Ibrahim, 2016a; Hall & Yarwood, 2024; Musotto & Wall, 2020). Они часто используются как синонимы для обозначения всех незаконных действий в Интернете, а органы безопасности, ученые и средства массовой информации часто объединяют различные цифровые правонарушения понятием «киберпреступность», игнорируя их уникальные признаки (Lazarus, 2019). Киберзависимые преступления совершаются даже без использования цифровых технологий или сетей, в то время как киберпреступления с использованием компьютерных технологий усугубляются за счет сетей. Мы фокусируемся на последней категории преступлений. Однако слияние таких категорий, как «киберпреступления с использованием компьютерных технологий»[1] и «киберпреступления, ориентированные на человека» (Gordon & Ford, 2006), затрудняет задачу разграничения между финансово мотивированными преступлениями, такими как «онлайн-мошенничество», и психологически мотивированными, такими как «порнография из мести» (Ibrahim, 2016a; Lazarus, 2019). В настоящей работе мы опираемся на подходы к киберпреступности, ориентированные на ситуацию в Нигерии, в частности, на концепцию Ibrahim (2016a). Тем самым мы стремимся внести свой вклад в дискуссию о виктимизации в результате онлайн-мошенничества и восполнить недостаточное внимание к идеям нигерийских ученых, как отмечено в работе Cross (2018a).

[1] McGuire, M., & Dowling, S. (2013, October). Cybercrime: a review of the evidence: Research Report 75. https://clck.ru/3F25c7

1.2. Трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF)

В эмпирической литературе (De Kimpe et al., 2020; Lazarus et al., 2022b) используется трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF). В ней проводится различие между киберпреступлениями, обусловленными психологией (психосоциальная киберпреступность), экономикой (социально-экономическая киберпреступность) и геополитикой. Это различие схематически показано на рисунке, основанном на оригинальной формулировке Ibrahim (2016a). В работе Ibrahim (2016a) разъясняется, что, хотя в нигерийском контексте киберпреступления обусловлены в первую очередь финансами, не все киберпреступления с использованием компьютерных технологий таковы, например, порнография из мести. Основываясь на этой классификации, мы выделяем уникальные характеристики киберпреступлений в Нигерии как особой подгруппы преступлений. Киберпреступность действительно является глобальной проблемой. Однако она также обладает пространственными характеристиками, влияющими на поведение людей в определенных регионах и проявляющимися в пространственных элементах, которые могут быть скрыты или выявлены (Hall & Yawood, 2024; Lazarus & Button, 2022).



Трехчастная концепция киберпреступности (Tripartite Cybercrime Framework, TCF)

1.2.1. Геополитическая категория киберпреступности

Геополитическая киберпреступность включает в себя киберпреступления, совершаемые по политическим мотивам, часто с участием государственных структур, негосударственных активистов или их представителей (Ibrahim, 2016a; Lazarus, 2019). Эти действия могут включать кибершпионаж или атаки на критически важную инфраструктуру. Однако киберпреступность, исходящая из Нигерии, редко попадает в эту категорию, в отличие от других стран, таких как Соединенные Штаты и Китай (Ibrahim, 2016a). Например, спонсируемые государством хакерские группы могут быть нацелены на иностранные правительственные учреждения с целью сбора разведданных для получения политических преимуществ в дипломатических переговорах или военных стратегиях (Akoto, 2021; Makridis et al., 2024). Основная мотивация этой категории киберпреступности носит политический характер, что соответствует геополитической категории в модели TCF (Ibrahim, 2016a).

1.2.2. Психосоциальная категория киберпреступности

Психосоциальная киберпреступность включает в себя преступления в сфере цифровых технологий, которые в первую очередь обусловлены психологическими мотивами и направлены на причинение страданий, мучений или вреда отдельным лицам (Ibrahim, 2016a; Lazarus, 2019). Денежная выгода в таких случаях не является основной целью. Примерами могут служить киберпреследование, киберзапугивание и онлайн-насилие, нацеленные на жертв в социальных сетях с целью нанести им психологический вред и подорвать их репутацию. Преступники получают удовлетворение от причинения страданий, что подчеркивает психосоциальный характер этих преступлений (Ibrahim, 2016a; Lazarus, 2019). Хотя преступники, занимающиеся порнографией из мести, часто обвиняют и унижают жертв, в случае мошенничества это не является основным мотивом, которым в этом случае являются деньги.

1.2.3. Социально-экономическая категория киберпреступности

Социально-экономическая киберпреступность связана с получением финансовой выгоды путем обмана с помощью компьютерных или интернет-технологий. Сюда относятся такие незаконные действия, как онлайн-мошенничество, брачные аферы, кража авторских прав и незаконное скачивание цифрового контента (Ibrahim, 2016a). Нигерия особенно уязвима к киберпреступлениям, относящимся к этой категории, включая подчинение, выдачу себя за законного пользователя, манипулирование, подделку документов, подлог, введение в заблуждение. Среди известных примеров – брачные аферы онлайн (Drew & Webster, 2024; Lazarus et al., 2023) и мошенническая схема «забой свиней» (Wang, 2023; Whittaker et al., 2024). Эти преступные схемы в первую очередь мотивированы финансовой выгодой.

Однако геополитические, психосоциальные и социально-экономические категории не определены жестко, и может иметь место сочетание нескольких мотивов. Например, если хактивисты [хакер-активист. – Прим. переводчика] публикуют украденную личную информацию в политических целях, то это может иметь психологические и геополитические последствия. Тем не менее TCF служит полезным инструментом для классификации отличительных особенностей различных киберпреступлений в Нигерии и за ее пределами. В Нигерии отсутствует статистика по другим видам киберпреступлений, например, кибершпионажу, киберпреследованиям и порнографии из мести, которые более распространены в таких странах, как Бельгия, Канада и Великобритания (Ibrahim, 2016a). Таким образом, концептуальные основы борьбы с киберпреступностью на глобальном Севере не вполне применимы в Нигерии, представляющей страны Африки к югу от Сахары (Ibrahim, 2016a). Стоит отметить, что ситуация с киберпреступностью в Нигерии сложна.

1.3. Проблемы и вызовы киберпреступности в Нигерии

Материалы недавних конференций проливают свет на различные аспекты судебного преследования за киберпреступления, регулирования и их влияния на ситуацию в Нигерии. Так, Idem с соавторами (2023a) выявили ключевые проблемы, препятствующие судебному преследованию киберпреступников в Нигерии, среди которых отсутствие четкого законодательства, неэффективное правоприменение,

судебные проволочки и ограниченные возможности криминалистического анализа. Основываясь на этом анализе, Idem и соавторы (2023b) подчеркивают настоятельную необходимость реформы органов по регулированию киберпреступности, чтобы изменить статус Нигерии как одной из трех стран с наибольшим ростом киберпреступности. Аналогичным образом, Idem (2023) предполагает, что принятый в Нигерии Закон о киберпреступности сыграл значительную роль в регулировании и сдерживании различных форм киберпреступности, защите и продвижении онлайн-бизнеса. Эти три взаимосвязанных исследования в совокупности освещают многогранные проблемы, связанные с киберпреступностью в Нигерии, и подчеркивают важность законодательных, нормативных и социально-экономических мер для их решения.

Далее, в работах Ojolo и Adewumi (2020) и Lazarus с соавторами (2023) освещается нормализация обстановки с киберпреступностью в нигерийском обществе, хотя выделены такие важные факторы ее распространения, как экономическая нестабильность, коррупция и влияние сверстников. В свою очередь, Lazarus с соавторами (2022a) проводят параллели между интернет-мошенниками (Yahoo Boys) и коррумпированными политиками (Yahoo Men) в Нигерии. Аналогичным образом, Olaiya с соавторами (2020), Monsurat (2020) и Adeduntan (2022) подчеркивают влияние политической коррупции, давления со стороны сверстников, экономических трудностей и неадекватных систем социальной поддержки. Кроме того, Ojolo и Singh (2023) и Aransiola и Asindemade (2011) раскрывают прибыльный характер этой деятельности и причастность коррумпированных сотрудников правоохранительных органов и отмечают, что финансовые стимулы пересекаются с институциональной уязвимостью, способствуя незаконным онлайн-практикам. В совокупности вышеприведенные исследования показывают, что киберпреступность – это сложное явление, коренящееся в социально-экономическом неравенстве, недостатках институциональной системы и культурных влияниях. При этом существует четкая закономерность, согласно которой в последние годы число случаев киберпреступности увеличилось.

1.4. Рост экономической киберпреступности в Нигерии

Рост экономической киберпреступности в Нигерии вызывает обеспокоенность у различных заинтересованных сторон. Idem и Olarinde (2023) освещают негативное влияние киберпреступности на развитие молодежи, экономику и управление в Нигерии. В качестве основных факторов вовлечения молодежи в киберпреступную деятельность они определяют безработицу, бедность, коррупцию и неэффективное управление, предлагая рекомендации по борьбе с этими проблемами. Согласно анализу отчетов о киберпреступлениях и инцидентах в области кибербезопасности, опубликованных Комиссией по экономическим и финансовым преступлениям (Economic and Financial Crimes Commission, EFCC)[2] за период с 2019 по 2022 г., число случаев онлайн-мошенничества резко возросло. Обобщим эту информацию, дающую представление о распространенности киберпреступности в нигерийском обществе, когда за четырехлетний период наблюдений резко увеличилось число вынесенных приговоров.

[2] EFCC, 2022: https://goo.su/TJjHS

Так, в период с 2019 по 2022 г. отмечено существенное увеличение числа сообщений о киберпреступлениях. В 2019 г. 877 человек сообщили об инцидентах, связанных с киберпреступностью; в 2020 г. это число увеличилось до 1890, т. е. на 115,5 %. В 2021 г. число зарегистрированных инцидентов увеличилось до 2400, что отражает ошеломляющий рост на 173,7 % по сравнению с базовым показателем 2019 г. Прогнозы на 2022 г. указывали на продолжающуюся тенденцию к росту: зарегистрировано 2900 инцидентов, что на 230,7 % больше по сравнению с первоначальными показателями 2019 г. Эти статистические данные свидетельствуют об экспоненциальном росте онлайн-мошенничества и подчеркивают необходимость научного исследования моделей виктимизации в стране. Наш анализ показывает заметный всплеск активности в сфере киберпреступности, что подтверждает растущее число осужденных за киберпреступления, о которых сообщает EFCC. Статданные доказывают значительный рост киберпреступности в Нигерии за указанный период, что говорит об активизации деятельности киберпреступных организаций, в первую очередь Yahoo Boys (Aborisade, 2023; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012).

1.5. Исследования, ориентированные на жертв преступности

Действия Yahoo Boys имеют глобальные последствия, что привело к увеличению числа исследований, затрагивающих проблему жертв онлайн-мошенничества. На тему виктимизации было проведено множество исследований, но большинство из них были посвящены западным обществам и азиатским странам, таким как Китай. В ряде исследований рассматривались такие африканские страны, как Нигерия, но они относительно редки. Например, исследования Button с соавторами (2014), Meikle & Cross (2024), Drew & Websters (2024), Cross (2020, 2018b), Whitty (2019) в основном фокусируются на жертвах из западных обществ и азиатских стран, таких как Китай (Tao, 2022; Wang, 2023; Wang & Topalli, 2024). Лишь немногие исследователи, такие как Aborisade с соавторами (2024), изучали виктимизацию в африканских странах, в частности, в Нигерии. Этот дисбаланс может быть вызван тем, что западные СМИ освещают исключительно жертв из западных стран, а также приоритетами в распределении финансирования исследований. Подобные тенденции закрепляют неравенство и непреднамеренно маргинализируют жертв из Нигерии. Наше исследование направлено на устранение этого неравенства; мы подчеркиваем, что пагубное влияние Yahoo Boys распространяется за пределы страны и выходит на глобальную арену. Освещая опыт жертв преступлений в таких африканских странах, как Нигерия, мы стремимся оспорить распространенный западноцентричный подход и подчеркнуть универсальность проблемы. Инклюзивный подход способствует более глубокому пониманию онлайн-мошенничества и его воздействия на жертв во всем мире.

1.6. Киберпреступники в нигерийском обществе (Yahoo Boys)

В ходе ряда качественных исследований были изучены действия нигерийских киберпреступников как внутри страны (Aransiola & Asindemade, 2011; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012), так и за ее пределами (Lazarus, 2024). Это позволило получить представление о различных аспектах деятельности этих преступников. Приведенная выше эмпирическая литература

неизменно указывает на то, что основными виновниками киберпреступлений являются лица мужского пола. Именно они в основном координируют социально-экономические цифровые преступления в Интернете, как показано на рисунке. Напротив, согласно свидетельствам, девушки-студентки, совершающие онлайн-мошенничества, преимущественно занимают подчиненные позиции при руководителях-мужчинах (Ogunleye et al., 2019). Приведенные выше результаты относятся к нигерийскому обществу, подчеркивая, что мужчины являются основными виновниками этих киберпреступных действий. Однако лишь в ограниченном числе исследований, включая работу Aborisade с соавторами (2024), был изучен опыт жертв киберпреступности в Нигерии.

1.7. Сходство и различия с предыдущими исследованиями

В нигерийском контексте многие исследования с использованием различных источников данных привели к сходным результатам. К ним относятся интервью с рядовыми сотрудниками правоохранительных органов (Lazarus & Okolorie, 2019), анализ мошеннических электронных писем (Genc et al., 2021; Rich, 2018), изучение текстов песен (Adeduntan, 2022; Lazarus et al., 2023), интервью с родителями (Aborisade, 2023; Ibrahim, 2016b), интервью с онлайн-мошенниками (Aransiola & Asindemade, 2011; Lazarus, 2024; Ojedokun & Eraye, 2012; Ogunleye et al., 2019), изучение твитов (Lazarus & Button, 2022). Последовательные и совпадающие результаты этих работ существенно повышают достоверность эмпирических исследований в целом, тем самым подтверждая фундаментальное понимание характеристик онлайн-преступников и категории киберпреступлений, которые они совершают. Более того, работы, не основанные на эмпирических данных, подтверждают выводы эмпирических исследований (Idem et al., 2023a, 2023b). Таким образом, выявленные признаки подкреплены данными, полученными с помощью различных методологий исследования. В Нигерии было проведено лишь ограниченное число исследований, посвященных жертвам киберпреступности, в частности, Aborisade et al. (2024), Mba et al. (2017), Tade и Adeniyi (2017).

1.8. Новизна данной работы

Настоящее исследование отличается от предыдущих в нескольких отношениях. Ранее при изучении жертв киберпреступлений в Нигерии (Aborisade et al., 2024; Mba et al., 2017; Tade & Adeniyi, 2017) не использовалось анкетирование. Предыдущие подходы, такие как в работе Aborisade с соавторами (2024) и Tade и Adeniyi (2017), основывались на качественных методах. В работе Mba с соавторами (2017) использовались данные форума сайта www.topix.com и поисковые системы в Интернете для выявления активных мошеннических и подобных онлайн-сообщений. В эмпирических исследованиях, в частности, бельгийских ученых De Kimpe с соавторами (2020), отправной точкой служила трехчастная концепция киберпреступности (TCF); однако эта концепция никогда не использовалась в явном виде, за исключением работы Lazarus с соавторами (2022b), в которой объединяются подходы TCF и феминистской эпистемологии преступности. В то же время Lazarus с соавторами (2022b) исследовали восприятие киберпреступлений в соответствии с категориями TCF в Великобритании, тогда как наше исследование направлено на изучение виктимизации в результате киберпреступлений в Нигерии через призму классификаций TCF. В качестве основы для нашего исследования мы используем «Социально-экономическую теорию киберпреступности в Нигерии», предложенную Ibrahim (2016a).

2. Методы и материалы

Для сбора данных мы использовали метод распределенного опроса различных групп студентов, сотрудников и работников из разных секторов экономики. Анкета разработана на основе концепции Ibrahim (2016a), которая подразделяет киберпреступность на социально-экономическую, геополитическую и психосоциальную категории, что позволяет выявить нюансы и особенности типов киберпреступности в Нигерии. Опрос проводился среди добровольных участников из разных демографических групп, которые могли тем самым лучше понять проблему киберпреступности. Хотя ответы участников были анонимными и конфиденциальными, для обеспечения соблюдения принципов научного исследования мы получили одобрение Совета по этике одного из университетов в Нигерии. Анкета была тщательно разработана и распространена через имеющиеся платформы для проведения опросов, что обеспечило эффективность и широкий охват исследования. Участники предоставили информированное согласие перед началом работы; были приняты строгие меры для обеспечения их анонимности и конфиденциальности на протяжении всего процесса сбора данных.

2.1. Анализ данных

Для определения географических кластеров и секторов, наиболее подверженных киберпреступности, мы провели анализ данных соседних стран. В сочетании с простыми статистическими методами и расширенной пространственной статистикой анализ данных позволил получить важную информацию о распространенности и характеристиках киберпреступности в исследуемой популяции. Кроме того, мы провели статистический анализ для выявления тенденций и закономерностей в частоте совершения киберпреступлений за определенный период. Описательные статистические данные, такие как средние значения и медианы, были рассчитаны с использованием электронных таблиц Excel, получены соответствующие количественные и процентные показатели. Хотя этот метод имеет свои ограничения, он обоснован с помощью следующих методов:

1. Исследовательский анализ. Описательная статистика служит ценным инструментом для проведения исследовательского анализа, позволяя получить первоначальное представление о данных путем обобщения ключевых характеристик, таких как центральная тенденция и изменчивость. Поскольку это предварительный этап исследования, такой подход позволяет выявить основные закономерности, связанные с киберпреступностью, не предполагая лежащих в их основе взаимосвязей, что важно, учитывая сложную социокультурную структуру нигерийского общества.

2. Представление данных. Описательная статистика имеет решающее значение для представления основных выводов в ясной и сжатой форме, что делает их доступными для широкой аудитории, включая студентов различных специальностей. Учитывая, что исследование фокусируется на опыте столкновения с киберпреступностью среди студентов и сотрудников университетов в Нигерии, описательная статистика позволяет напрямую донести важные выводы о распространенности и характеристиках киберпреступности до представителей этой группы населения.

3. Простые структуры данных. Инструментарий, использованный в исследовании, имеет относительно простую структуру с небольшим количеством переменных и прямыми взаимосвязями. Таким образом, описательная статистика хорошо подходит для решения поставленных задач и достижения целей данного

предварительного исследования. По итогам работы авторы пришли к выводу, что в более сложных аналитических методах нет необходимости, так как они лишь привели бы к излишней усложненности. Описательная статистика является эффективным способом анализа и обобщения данных, предоставляя ценную информацию об опыте виктимизации в результате киберпреступлений среди исследуемой группы населения.

3. Результаты

В данном разделе представлены результаты количественного анализа 896 ответов респондентов с указанием частот и процентных соотношений по каждой категории преступлений. Результаты показаны в таблице. Почти все участники (99,78 %) дали свое информированное согласие, что свидетельствует о высоком уровне готовности участвовать в исследовании. Лишь небольшая часть (0,76 %) предпочла не давать согласия, что говорит о том, что большинство участников были готовы к участию в опросе.

Краткое изложение результатов

Вопрос	Ответ	Кол-во	Процент
Получено информированное согласие	Да	896	99,78
	Нет	7	0,76
Распределение респондентов по полу	Мужской	584	64,69
	Женский	312	34,52
Уровень образования	Магистрант	522	57,80
	Аспирант	21	2,36
	Преподаватель и руководство	12	1,35
Становились ли жертвами киберпреступления	Да	588	65,20
	Нет	301	33,40
Пол жертвы киберпреступления	Мужской	303	51,53
	Женский	285	48,47
Тип киберпреступления, с которым сталкивались	Мошенничество с онлайн-банком/платежами/картами	554	61,45
	Кража личности	67	7,43
	Другое	295	32,68
Сообщали ли о киберпреступлении	Да	322	35,74
	Нет	577	63,94
Были ли возвращены украденные деньги/предприняты надлежащие меры	Да	54	5,99
	Нет	835	92,61

3.1. Гендерный аспект

Результаты исследования проливают свет на гендерную динамику виктимизации в результате киберпреступлений, выявляя заметное различие в опыте мужчин и женщин. Анализ данных показывает, что среди лиц, пострадавших от киберпреступности, 303 мужчины (51,53 %) и 285 женщин (48,47 %) сообщили о неблагоприятных последствиях. Это неравенство еще больше подчеркивается общим распределением жертв киберпреступлений: 64,69 % мужчин и 34,52 % женщин. Эти цифры свидетельствуют о гендерном характере виктимизации в результате киберпреступлений:

более высокая доля мужчин сталкивается с негативными последствиями по сравнению с женщинами. Полученные данные также подчеркивают необходимость применения гендерно ориентированных подходов к борьбе с киберпреступностью и принятия мер по смягчению ее последствий как для мужчин, так и для женщин. Кроме того, относительно сбалансированное распределение жертв среди мужчин и женщин подчеркивает важность учета гендерной динамики при понимании явлений киберпреступности и реагировании на них.

3.2. Уровень образования

Участники имели различный уровень образования. 37,80 % из них были студентами бакалавриата, 57,80 % – магистрантами, 2,36 % – аспирантами и 1,35 % – преподавателями и административными сотрудниками вуза. Такое разнообразие уровней образования усиливает неоднородность выборки и делает выводы более обобщающими.

3.3. Подтвержденный негативный опыт в сфере киберпреступности

Значительная часть участников (65,20 %) сообщили, что сталкивались с негативными инцидентами, связанными с киберпреступностью, что подчеркивает ее повсеместное воздействие на исследуемую группу населения. Однако 33,40 % респондентов указали, что они не сталкивались с какими-либо инцидентами, связанными с киберпреступностью, что указывает на наличие подгруппы лиц, не затронутых этим видом преступлений.

3.4. Типы киберпреступлений

Исследование выявило четкие закономерности в распределении киберпреступлений. Мошенничество с использованием электронных банковских услуг/платежных карт было наиболее распространенным видом мошенничества, на долю которого приходилось 61,45 % зарегистрированных случаев. На кражу личных данных приходилось 7,43 % инцидентов, в то время как на другие формы кражи в совокупности – 32,68 % случаев, таких как мошенничество с трудоустройством в Интернете. Эти данные позволяют получить представление о распространенности и распределении конкретных видов киберпреступности социально-экономической категории среди исследуемой группы населения.

3.5. Сообщения об инцидентах

Исследование показало, что 35,74 % участников сообщили об инцидентах, связанных с киберпреступностью, в соответствующие органы или организации, что свидетельствует об умеренном использовании соответствующих механизмов. Напротив, большинство (63,94 %) не сообщали о каких-либо инцидентах, что свидетельствует о возможном занижении отчетности и областях, требующих улучшения этой сферы правоохранительной практики.

3.6. Возврат украденных денег/Принятие соответствующих мер

Среди участников, сообщивших об инцидентах, связанных с киберпреступностью, лишь меньшинство (5,99 %) указали, что украденные средства были возвращены или в ответ были приняты соответствующие меры. И наоборот, подавляющее

большинство (92,61 %) сообщили об отсутствии мер по исправлению положения, что указывает на трудности в достижении реституции или разрешении проблемы после того, как они стали жертвами киберпреступлений. Эти результаты дают ценную информацию о распространенности киберпреступности, ее характеристиках и динамике сообщений среди участников, однако необходимы дальнейшие исследования для сравнения с имеющейся эмпирической литературой и выявления возможных последствий для политики, практики и будущих исследований.

4. Обсуждение

В данном разделе мы, опираясь на информацию, полученную с помощью метода распределенного опроса, попытаемся изучить проблему виктимизации в результате киберпреступлений в различных демографических группах. Мы рассмотрим четыре основные темы: (1) различия в опыте столкновения с киберпреступностью по гендерному признаку; (2) ключевая роль социально-экономических факторов в борьбе с киберпреступностью в Нигерии; (3) взаимосвязь между уровнем образования и уязвимостью к онлайн-мошенничеству и (4) исследование виктимизации в результате киберпреступности через призму социально-экономического разрыва между Севером и Югом.

4.1. Гендерный аспект виктимизации в результате онлайн-мошенничества

Проведенный анализ гендерных различий в виктимизации в результате киберпреступлений (таблица, п. 3.4 статьи) частично согласуется с результатами предыдущих исследований, но и расходится с ними. Например, согласно работе Lazarus с соавторами (2022b), женщины склонны воспринимать психосоциальные киберпреступления, такие как порнография из мести, как более тяжелые, чем мужчины; однако в отношении социально-экономических киберпреступлений, таких как онлайн-мошенничество с кредитными картами, заметных гендерных различий не наблюдается. Примечательно, что в отличие от вышеприведенных авторов наше исследование не изучает напрямую восприятие киберпреступности, но показывает гендерные различия в социально-экономической виктимизации в результате киберпреступности, что вносит свой вклад в научную дискуссию. Более того, многочисленные исследования (Näsi et al., 2023) позволили изучить сложную динамику виктимизации в результате киберпреступлений, пролив свет на различные влияющие на нее факторы. Исследование Kadoya с соавторами, проведенное в 2021 г. в Японии, указывает на пол и семейное положение в качестве потенциальных факторов, определяющих виктимизацию; другими словами, мужчины и состоящие в браке люди более подвержены мошенничеству с банковскими счетами. Аналогичным образом, исследование Whitty (2019), проведенное в Великобритании, подчеркивает гендерные различия в киберпреступности, особенно очевидные в случае брачных аферистов, где женщины подвергаются непропорциональной виктимизации. Хотя в нашем исследовании конкретно не задавались вопросы о семейном положении или брачных аферах, наши выводы перекликаются с выводами Kadoya с соавторами (2021) и Whitty (2019), подтверждающими важность гендерного фактора в виктимизации в результате киберпреступности.

Вариативность гендерного неравенства в различных контекстах дополнительно подтверждается исследованиями, проведенными в Финляндии (Näsi et al., 2023) и Нидерландах (Weijer et al., 2020). Первое не выявило статистически значимых

гендерных различий, однако голландское исследование показало, что женщины чаще сообщают в полицию о традиционных преступлениях, в то время как мужчины проявляют большую активность в сообщениях о киберпреступлениях (Näsi et al., 2023; Weijer et al., 2020). Следовательно, можно с уверенностью утверждать, что гендерные различия, выявленные в нашем исследовании, могут быть частично объяснены различиями в поведении при сообщении о преступлениях. Это подчеркивает неоднозначность данных о кибервиктимизации: о киберпреступлениях часто сообщают не в полицию, а в другие организации. Кроме того, гендерные различия существенно влияют на подверженность онлайн-мошенничеству, а такие психологические особенности, как склонность к риску и низкий уровень самоконтроля, еще больше повышают уязвимость (Norris et al., 2019). Хотя мы не изучали психологические особенности и их связь с виктимизацией при онлайн-мошенничестве, наши результаты свидетельствуют о том, что гендерные различия существенно влияют на подверженность онлайн-мошенничеству. Несмотря на эти гендерные нюансы, сам по себе гендер играет лишь второстепенную роль в прогнозировании кибервиктимизации, в то время как значительное влияние оказывают другие факторы, такие как мотивация мошенников и уязвимость цели.

4.2. Роль киберпреступности в социально-экономической динамике

Наше исследование выявило четкие тенденции в области киберпреступлений, в частности, выделив мошенничество с использованием электронных банковских услуг/платежных карт как наиболее распространенный вид преступлений, на который приходится 61,45 % всех зарегистрированных случаев (табл). На кражу личных данных приходилось 7,43 % инцидентов, в то время как на различные другие виды мошенничества, включая мошенничество с поиском работы в Интернете и фишинговые схемы, в совокупности приходилось 32,68 % случаев, и все они подпадали под социально-экономическую категорию киберпреступности (табл). Это подтверждает тот факт, что киберпреступность имеет пространственные характеристики, поскольку она распространяется, проявляется и влияет на поведение людей по-разному в различных регионах, а также может быть скрыта или выявлена с помощью пространственных элементов (Hall & Yawood, 2024; Lazarus & Button, 2022). Трехчастная концепция киберпреступности (TCF) подразделяет киберпреступления на три основных категории согласно мотивации: социально-экономическую, психологическую и геополитическую, подчеркивая различие между социально-экономическими и психосоциальными киберпреступлениями (Ibrahim, 2016a; Lazarus, 2019; Lazarus et al., 2022b).

В отличие от таких стран, как Канада, Россия, Китай и Великобритания, в Нигерии отсутствует существенная статистика по другим категориям киберпреступлений, в частности по геополитическим, таким как кибершпионаж, и психосоциальным, таким как порнография из мести (Ibrahim, 2016a). Геополитический и социокультурный контексты разных стран существенно влияют на их поведение в киберпространстве. Например, порнография из мести распространена в таких западных странах, как Португалия (Murça et al., 2024), Великобритания, Канада и др. (Harper et al., 2023), в то время как в Нигерии она не так заметна. Кроме того, в отличие от Нигерии, такие страны, как Соединенные Штаты, Россия, Китай и Великобритания, сталкиваются со значительными проблемами, связанными с кибершпионажем, спонсируемым государством (Akoto, 2021, 2024; Markridis et al., 2024). Эти социальные и контекстуальные нюансы бросают вызов представлениям о киберпространстве и физическом

пространстве как об отдельных сущностях с четкими границами, что подчеркивал Jaishankar (2007, 2011, 2018). В результате концептуальные рамки, обычно используемые в отношении «глобального Севера», могут быть не совсем применимы в Нигерии, представляющей Африку к югу от Сахары (Ibrahim, 2016a). Сложность ситуации с киберпреступностью в Нигерии очевидна. Хотя данные нашего опроса были получены из одного учреждения, результаты позволяют судить о распространенности и распределении видов киберпреступности в рамках категории социально-экономических преступлений.

Хотя в Нигерии нет существенной статистики по определенным категориям киберпреступлений, это не обязательно означает, что психосоциальные киберпреступления, такие как киберпреследование и киберзапугивание, отсутствуют или незначительны. Одно из возможных объяснений заключается в том, что социокультурная структура нигерийского общества определяет приоритетность социально-экономических видов киберпреступлений, таких как онлайн-мошенничество. Этот акцент проявляется в том, что EFCC, один из высших правоохранительных органов Нигерии, уделяет особое внимание финансовым преступлениям. Кроме того, отсутствие статистики может быть вызвано другими факторами, такими как ограниченные ресурсы или недостаточность инфраструктуры для выявления подобных киберпреступлений и сообщения о них. Также, хотя социокультурный и геополитический контексты влияют на поведение в киберпространстве, важно признать, что геополитические виды киберпреступлений часто не затрагивают обычных граждан, таких как студенты и преподаватели, которых мы изучали в данной работе. В результате наше исследование не охватывало геополитические аспекты, что может привести к неточностям в наших выводах.

4.3. Уровень образования жертв онлайн-мошенничества

Один из важных выводов, сделанных в ходе нашего исследования, касается уровня образования участников. Хотя более 99 % из них имели высшее образование или находились в процессе его получения, уровни образования значительно различались. В частности, среди участников 37,80 % были студентами бакалавриата, 57,80 % – магистрантами, 2,36 % – аспирантами и 1,35 % были преподавателями и административными сотрудниками вуза (п. 3.2 статьи). Несмотря на такое разнообразие в уровне образования, более 65 % всех участников сообщили, что стали жертвами киберпреступлений, и этот вывод частично согласуется с предыдущими исследованиями, но и расходится с ними.

Существующие исследования показывают, что на вероятность стать жертвой онлайн-мошенничества влияют несколько факторов, среди которых значительную роль играет уровень образования. Исследования показали, что лица с более низким уровнем образования более подвержены мошенничеству в потребительской сфере (Whitty, 2018). Однако исследования также свидетельствуют о наличии сложной взаимосвязи между уровнем образования и жертвами мошенничества. Например, люди, находящиеся на самом низком уровне образования, не имеющие законченного среднего или высшего образования, с меньшей вероятностью становятся жертвами мошенничества (Schoepfer & Piquero, 2009), что указывает на U-образную закономерность в этой взаимосвязи.

Более того, люди, получившие высшее образование и проводящие больше времени в Интернете, подвергаются большему риску стать мишенью мошенников (Paek & Nalla, 2015). Эта связь подчеркивает влияние повседневной онлайн-активности на риск виктимизации, а также роль онлайн-взаимодействий в повышении уязвимости к киберпреступности. Кроме того, пожилые люди, которые, как правило, имеют более высокий уровень образования, считаются особенно уязвимыми для кибермошенничества (Whitty, 2019). Эта демографическая группа часто проявляет такие черты, как высокая импульсивность, склонность к рискованному поведению в Интернете и тенденцию к зависимостям, что повышает их восприимчивость к онлайн-мошенничеству.

4.4. Виктимизация в результате киберпреступлений, концепция идеальной жертвы и разрыв между Севером и Югом

Результаты нашего исследования подчеркивают повсеместное влияние киберпреступности в Нигерии, при этом заметное большинство участников (65,20 %) сообщили о личном опыте виктимизации (Aborisade et al., 2024). Это говорит о широкомасштабном характере киберпреступности и ее существенном влиянии на исследуемую группу населения. И наоборот, 33,40 % респондентов указали, что они не сталкивались с инцидентами, связанными с киберпреступностью, что указывает на то, что в Нигерии есть группа лиц, не затронутых этой преступной деятельностью. Это противоречие заставляет задуматься о теории виктимизации и различиях между глобальным Севером и Западной Африкой (Нигерией), что редко рассматривается в литературе по онлайн-мошенничеству.

Группа Yahoo Boys, зародившаяся в Нигерии, но осуществляющая деятельность по всему миру, привлекла повышенное внимание к жертвам онлайн-мошенничества. Однако существующие исследования в основном сосредоточены на жертвах из западных обществ (Button et al., 2014, 2015; Cross, 2020; Drew & Webster, 2024) и на некоторых незападных контекстах, таких как Китай (Tao, 2022; Wang, 2023); при этом странам Западной Африки, таким как Нигерия, посвящено ограниченное количество исследований (Aborisade et al., 2024). Вполне вероятно, что неравномерное распределение исследовательского интереса к определенным вопросам объясняется тенденцией западных СМИ уделять особое внимание громким инцидентам с жертвами из западных стран. Кроме того, финансирование научных исследований часто ориентировано в первую очередь на Запад, что приводит к недостатку внимания и ресурсов для других регионов, включая западноафриканские страны, такие как Нигерия (Mosbah-Natanson & Gingras, 2014). Эти предубеждения закрепляют предвзятость и непреднамеренно маргинализируют жертв из незападных стран, тем самым подчеркивая концепцию «идеальных жертв», когда некоторые жертвы могут считаться более «идеальными», чем другие. Жертвы онлайн-мошенничества в западных обществах, таких как Соединенные Штаты, Великобритания и Австралия, имеют такое же значение, как и в Нигерии.

Опираясь на основополагающую работу Christie (1986), в которой описываются черты идеальной жертвы, наше исследование изучало динамику виктимизации в результате онлайн-мошенничества в контексте Нигерии. Christie (1986) утверждает, что идеальные жертвы воспринимаются как воплощения определенных черт, соответствующих общественным нормам невиновности, уязвимости и отсутствия вины,

что вызывает положительную реакцию общества. Такой общественный резонанс потенциально может предотвратить преступления или способствовать привлечению преступников к ответственности. Другие ученые использовали эту концепцию для изучения аспектов киберпреступности (Hock & Button, 2023; Loyens & Paraciani, 2023). Используя эту концепцию, мы рассматриваем не только динамику мошеннических преступлений, нацеленных на нигерийцев, но и реакцию мирового сообщества на преступления, жертвами которых становятся нигерийцы, включая выделение средств на исследования в этой области. Мы утверждаем, что соотношение сил между глобальными Севером и Югом, наряду со структурой мировой экономики, формирует отношение к жертвам. При этом жертвы из стран Запада воспринимаются как более заслуживающие статуса «идеальной жертвы», чем нигерийцы, что влияет как на региональные, так и на глобальные меры реагирования на преступления, совершаемые против нигерийцев. С учетом значительного роста числа жертв онлайн-мошенничества в Нигерии, например, в период с 2019 по 2022 г. этот вопрос вызывает глубокую озабоченность.

Однако стоит отметить, что динамика сил и экономические структуры, которые формируют отношение к жертвам, сложны и многогранны, и их не следует чрезмерно упрощать или сводить к одному фактору. Кроме того, региональные власти и правительство Нигерии несут главную ответственность за своих граждан и не должны перекладывать на внешние органы и международные сообщества (например, на западные страны) свои обязанности по оказанию поддержки жертвам онлайн-мошенничества в нигерийском обществе. Наконец, хотя ситуация с онлайн-мошенничеством действительно вызывает серьезную озабоченность в Нигерии, это явление не уникально и встречается также во многих других частях мира.

Заключение

Наше исследование с участием 896 человек позволило получить представление о виктимизации в результате киберпреступлений. Особое внимание было уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к онлайн-мошенничеству и виктимизации в результате киберпреступлений через призму концепции идеальной жертвы и социально-экономического разрыва между Севером и Югом. Наш анализ выявил гендерные различия в опыте виктимизации в результате киберпреступлений: более высокая доля мужчин сталкивается с негативными последствиями киберпреступлений, что согласуется с предыдущими исследованиями (Kadoya et al., 2021). Работа предлагает новый взгляд на этот дискурс, подчеркнув вариативность гендерного неравенства в разных контекстах и необходимость применения гендерно ориентированных подходов к борьбе с киберпреступностью. Во-вторых, в нашем исследовании подчеркивается ключевая роль социально-экономических факторов в распространении киберпреступности, особенно в Нигерии. Распространенность киберпреступлений, особенно в сфере электронного банкинга/мошенничества с платежными картами, свидетельствует о социально-экономической динамике в сфере киберпреступности в Нигерии и подчеркивает центральную роль данной категории киберпреступлений в этой стране. В-третьих, мы рассмотрели взаимосвязь между уровнем образования и уязвимостью к онлайн-мошенничеству. Хотя более 99 % наших участников имели высшее образование, распределение по уровням образования

было различным, что повлияло на подверженность киберпреступности. Наши выводы согласуются с существующими исследованиями (Whitty, 2018), указывающими на сложную взаимосвязь между уровнем образования и жертвами мошенничества. И последнее, но не менее важное: учитывая социально-экономический разрыв между Севером и Югом, мы рассмотрели проблему виктимизации в результате киберпреступности с точки зрения концепции идеальной жертвы. Опираясь на фундаментальную работу Christie (1986), мы изучили динамику роста числа жертв онлайн-мошенничества в Нигерии, обращая внимание на различия в уровне интереса исследователей и глобальных мер реагирования на киберпреступления, затрагивающие незападные страны. Наши выводы подчеркивают необходимость применения тщательно выверенных гендерных, инклюзивных и контекстуальных подходов к исследованию киберпреступности и разработке политики в Нигерии и за ее пределами, учитывая обсуждаемую динамику глобальной расстановки сил. Эти выводы показывают актуальность разработки многоаспектных и учитывающих контекст подходов к борьбе с киберпреступностью и смягчению ее последствий для уязвимых групп населения во всем мире.

Список литературы

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, *61*(1), 59–71. https://doi.org/10.1177/00223433231214417

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, *1*, 100012. https://doi.org/10.1016/j.jeconc.2023.100012

Button, M., Nicholls, C. M, Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, *54*(2), 193–211. https://doi.org/10.1111/hojo.12123

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2

Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, *3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, *30*(2), 88–99. https://doi.org/10.1080/19393555.2020.1804647

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, *48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, *35*(6), 748–783. https://doi.org/10.1177/10790632221082663

Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, *18*(7), 1311–1334. https://doi.org/10.1080/15564886.2023.2186996

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. https://doi.org/10.1109/icccf.2016.7740439

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050983

Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. https://doi.org/10.1109/cymaen57228.2023.10051047

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050896

Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050994

Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, *12*, 649565. https://doi.org/10.3389/fpsyg.2021.649565

Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, *10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men"). *Heliyon*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Loyens, K., & Paraciani, R. (2023). Who is the ("Ideal") Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors' Discretion. *The Sociological Quarterly*, *64*(1), 27–45. https://doi.org/10.1080/00380253.2021.1974321

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). https://doi.org/10.1145/3041021.3053892

McGerty, L. J. (2000). "Nobody lives only in cyberspace": Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, *3*(5), 895–899. https://doi.org/10.1089/10949310050191863

Meikle, W., & Cross, C. (2024). "What action should I take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, *3*, 100054. https://doi.org/10.1016/j.jeconc.2024.100054

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.3755848

Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, *62*(5), 626–646. https://doi.org/10.1177/0011392113498866

Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, *28*(1), 96–112. https://doi.org/10.1007/s12119-023-10100-3

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, *25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, *29*, 283–301. https://doi.org/10.1007/s10610-021-09497-0

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*, 231–245. https://doi.org/10.1007/s11896-019-09334-5

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2). https://doi.org/10.5281/zenodo.3702333

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55. https://doi.org/10.31920/2516-2713/2023/6n1a4

Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, *9*(4), 243. https://doi.org/10.31920/2634-3622/2020/v9n4a11

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-022-00342-5

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, *9*(2), 003.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626–642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. https://doi.org/10.4324/9781315205786

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*, 208–225. https://doi.org/10.1057/s41284-017-0095-0

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. *Media, Culture & Society*, *44*(6), 1199–1214. https://doi.org/10.1177/01634437221088952

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, *68*, 100520. https://doi.org/10.1016/j.ijlcj.2021.100520

Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, *0*(0). https://doi.org/10.1177/00111287231158571

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/10.1007/s12103-022-09706-4

Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Сведения об авторах



Амину Мухаммад Аувал – бакалавр в области информационных технологий, специалист в области информационных технологий, Университет Джоса
Адрес: Нигерия, PMB 2084, штат Плато, г. Джос
E-mail: i.elameenu@gmail.com
ORCID ID: https://orcid.org/0009-0005-1799-7876
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JFS-7098-2023
Google Scholar ID: https://scholar.google.com/citations?user=RDxPEr4AAAAJ



Сулеман Лазарус – PhD в области киберпреступности и криминологии, приглашенный специалист Центра криминологии им. Маннхайма, Лондонская школа экономики и политических наук; сотрудник Центра изучения старения населения, университет Суррея; почетный преподаватель Центра по изучению киберпреступности и экономической преступности, Портсмутский университет
Адрес: Великобритания, WC2A 2AE, г. Лондон, Хьютон Стрит; Великобритания GU2 7XH, г. Гилфорд, Стэг Хилл; Великобритания, PO1 2HY, г. Портсмут, Сент-Джордж Билдинг.
E-mail: suleman.lazarus@gmail.com
ORCID ID: https://orcid.org/0000-0003-1721-8519
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205679641
WoS Researcher ID: https://www.webofscience.com/wos/author/record/629543
Google Scholar ID: https://scholar.google.com/citations?user=Em8EXqcAAAAJ

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: 10.81 / Криминология
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 16 мая 2024 г.
Дата одобрения после рецензирования – 28 мая 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:343.9:004.8
EDN: https://elibrary.ru/jvglrh
DOI: https://doi.org/10.21202/jdtl.2024.44

Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization

Aminu Muhammad Auwal

University of Jos, Jos, Nigeria

Suleman Lazarus ✉

London School of Economics and Political Science, London, United Kingdom
University of Surrey, Guildford, United Kingdom
University of Portsmouth, Portsmouth, United Kingdom

Keywords

cybercrime victim,
cybercrime,
cybercriminology,
cyber-espionage,
digital criminology,
digital technologies,
legal policy,
online fraud,
victimization,
victimology

Abstract

Objective: to identify the main issues of victimization as a result of cybercrime growth in the world in general and in Nigerian society in particular from the standpoint of sociological approaches, using a Tripartite Cybercrime Framework (TCF), which comprises geopolitical, psychosocial and socio-economic categories of cybercrime.

Methods: the methodology is based on the sociological research method. The data collection included the distribution of a questionnaire among 896 participants from the academic environment, including students and university staff, and the analysis of the responses. The presented data were analyzed using descriptive statistics, with special attention to the issues of gender inequality, socio-economic factors, the impact of educational level on vulnerability to online fraud and victimization as a result of cybercrime through the prism of the ideal victim concept and the socio-economic gap between North and South.

Results: the article presents an analysis of the Tripartite Cybercrime Framework. The survey showed that 65.20% of the participants had been victims of cybercrime. There were more men among the victims (64.69%). The authors found patterns in the distribution of cybercrimes. All cybercrimes against the respondent were socio-economic ones, which underlines the

✉ Corresponding author
© Auwal A. M., Lazarus 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.

high frequency of cybercrime and the relevance of countering it in Nigerian society. Special attention was paid to the issues of gender inequality, socio-economic factors, and the impact of education on vulnerability to cybercrime. The article considers from the viewpoint of the ideal victim concept. The study results provide an idea of the prevalence and distribution of specific types of cybercrime in the socio-economic category among the studied population.

Scientific novelty: For the first time, the study uses the Tripartite Cybercrime Framework (TCF) to study victimization as a result of cybercrime in Nigerian society. The research novelty is also due to the fact that the conceptual foundations of countering cybercrime that have developed in the global North are not fully applicable in Nigeria.

Practical significance: the results obtained demonstrate the need to apply carefully calibrated gender-based, inclusive and contextual approaches to the development of a national legal policy to combat cybercrime. The results can be used to justify the law-making decisions which are being developed in the field of preventing and countering manifestations of cybercrime, as well as to form the basis for legal measures to protect cybercrime victims.

For citation

Auwal, A. M., & Lazarus, S. (2024). Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization. *Journal of Digital Technologies and Law, 2*(4), 915–942. https://doi.org/10.21202/jdtl.2024.44

References

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, *3*, 100044. https://doi.org/10.1016/j.jeconc.2023.100044

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, *61*(1), 59–71. https://doi.org/10.1177/00223433231214417

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, *1*, 100012. https://doi.org/10.1016/j.jeconc.2023.100012

Button, M., Nicholls, C. M, Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, *54*(2), 193–211. https://doi.org/10.1111/hojo.12123

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2

Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, *3*, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, *30*(2), 88–99. https://doi.org/10.1080/19393555.2020.1804647

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, *48*(4), 437–457. https://doi.org/10.1177/03091325241246015

Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, *35*(6), 748–783. https://doi.org/10.1177/10790632221082663

Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, *18*(7), 1311–1334. https://doi.org/10.1080/15564886.2023.2186996

Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. https://doi.org/10.1109/icccf.2016.7740439

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050983

Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. https://doi.org/10.1109/cymaen57228.2023.10051047

Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050896

Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. https://doi.org/10.1109/cymaen57228.2023.10050994

Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8. https://doi.org/10.5281/zenodo.1467308

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, *12*, 649565. https://doi.org/10.3389/fpsyg.2021.649565

Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, *10*(3), 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo men"). *Heliyon*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Loyens, K., & Paraciani, R. (2023). Who is the ("Ideal") Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors' Discretion. *The Sociological Quarterly*, *64*(1), 27–45. https://doi.org/10.1080/00380253.2021.1974321

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). https://doi.org/10.1145/3041021.3053892

McGerty, L. J. (2000). "Nobody lives only in cyberspace": Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, *3*(5), 895–899. https://doi.org/10.1089/10949310050191863

Meikle, W., & Cross, C. (2024). "What action should I take?": Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, *3*, 100054. https://doi.org/10.1016/j.jeconc.2024.100054

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.3755848

Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, *62*(5), 626–646. https://doi.org/10.1177/0011392113498866

Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, *28*(1), 96–112. https://doi.org/10.1007/s12119-023-10100-3

Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, *25*, 173–191. https://doi.org/10.1007/s12117-020-09397-5

Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, *29*, 283–301. https://doi.org/10.1007/s10610-021-09497-0

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*, 231–245. https://doi.org/10.1007/s11896-019-09334-5

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2). https://doi.org/10.5281/zenodo.3702333

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55. https://doi.org/10.31920/2516-2713/2023/6n1a4

Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, *9*(4), 243. https://doi.org/10.31920/2634-3622/2020/v9n4a11

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-022-00342-5

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, *9*(2), 003.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626–642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. https://doi.org/10.4324/9781315205786

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*, 208–225. https://doi.org/10.1057/s41284-017-0095-0

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. *Media, Culture & Society*, *44*(6), 1199–1214. https://doi.org/10.1177/01634437221088952

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, *68*, 100520. https://doi.org/10.1016/j.ijlcj.2021.100520

Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, *0*(0). https://doi.org/10.1177/00111287231158571

Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, *49*(1), 145–181. https://doi.org/10.1007/s12103-022-09706-4

Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Authors information



Aminu Muhammad Auwal – Bachelor of Science in Information Technology, IT Specialist, University of Jos
Address: PMB 2084, Jos, Plateau State, Nigeria
E-mail: i.elameenu@gmail.com
ORCID ID: https://orcid.org/0009-0005-1799-7876
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JFS-7098-2023
Google Scholar ID: https://scholar.google.com/citations?user=RDxPEr4AAAAJ



Suleman Lazarus – PhD in Cybercrime and Criminology, Visiting Fellow at the Mannheim Centre for Criminology, London School of Economics and Political Science; Fellow at the Centre of Excellence on Ageing, University of Surrey; Honorary Lecturer at the Centre for Cybercrime and Economic Crime, University of Portsmouth.
Address: Houghton Street, London, WC2A 2AE, United Kingdom; Stag Hill, Guildford, GU2 7XH, United Kingdom; St. George's Building, Portsmouth, PO1 2HY, United Kingdom.
E-mail: suleman.lazarus@gmail.com
ORCID ID: https://orcid.org/0000-0003-1721-8519
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205679641
WoS Researcher ID: https://www.webofscience.com/wos/author/record/629543
Google Scholar ID: https://scholar.google.com/citations?user=Em8EXqcAAAAJ

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 – May 16, 2024
Date of approval – May 28, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Преодоление нелегальной трансграничной передачи персональных данных

Дмитрий Валерьевич Бахтеев ✉

Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Анна Михайловна Сосновикова

Уральский государственный юридический университет имени В. Ф. Яковлева, Екатеринбург, Россия

Евгений Владимирович Казенас

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия

Ключевые слова

законодательство,
информационная безопасность,
информация,
инцидент,
компьютерная сеть,
персональные данные,
право,
связь,
трансграничная передача данных,
цифровые технологии

Аннотация

Цель: формирование комплексной междисциплинарной юридико-технологической модели управления рисками в сфере незаконной трансграничной передачи персональных данных посредством ликвидации законодательных лакун и создания системы автоматизированного контроля исходящих потоков информации, а также экспертного реагирования на выявленные инциденты.

Методы: в работе, помимо всеобщего диалектического и общенаучных, используются специально-юридические и кибернетические методы. Так, на основе сравнительно-правового анализа выявляются различия между национальным и международным регулированием трансграничных потоков персональных данных, а метод моделирования, положенный в основу второго раздела исследования, позволяет сформировать алгоритм выявления инцидентов информационной безопасности в сфере трансграничной передачи персональных данных и реагирования на них.

Результаты: сформулированы предложения по оптимизации законодательства в рассматриваемой сфере посредством введения специализированных охранительных норм за нарушение правил трансграничной передачи персональных данных, закрепления обязанности оператора уведомлять субъектов персональных данных о намерении осуществить передачу информации за рубеж. Во второй части работы описана концепция программного комплекса, предназначенного для детекции инцидентов информационной безопасности в рассматриваемой области, а также модель действия уполномоченного представителя оператора после получения сигнала от автоматизированной системы.

✉ Корреспондирующий автор

© Бахтеев Д. В., Сосновикова А. М., Казенас Е. 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: для решения заявленной проблемы в работе объединяются знания и компетенции ученых-юристов и специалистов в сфере информационной безопасности, что позволяет предложить междисциплинарный подход. Одновременно с этим вопросы незаконной трансграничной передачи персональных данных на сегодняшний день не получили должного освещения в науке, поскольку российское законодательство в данной сфере изменилось не так давно. Авторы настоящей работы предлагают не столько усилить санкцию за нарушение законодательства в рассматриваемой сфере, сколько обеспечить наказание лиц, совершающих кибератаки, и вооружить операторов персональных данных действенным инструментом минимизации рисков утечки информации.

Практическая значимость: результаты исследования могут быть использованы для совершенствования законодательства в сфере трансграничной передачи персональных данных и организации деятельности уполномоченных сотрудников оператора персональных данных по управлению рисками в рассматриваемой сфере.

Для цитирования

Бахтеев, Д. В., Сосновикова, А. М., Казенас, Е. В. (2024). Преодоление нелегальной трансграничной передачи персональных данных. *Journal of Digital Technologies and Law*, *2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Содержание

Введение
1. Правовые аспекты трансграничной передачи персональных данных
   1.1. История формирования правоотношений, связанных с трансграничной передачей персональных данных
   1.2. Регулирование трансграничной передачи персональных данных законодательством Российской Федерации и международными нормами
2. Технико-технологические аспекты трансграничной передачи данных
   2.1. Основные технические каналы связи, по которым осуществляется трансграничная передача персональных данных
   2.2. Модель выявления фактов незаконной трансграничной передачи персональных данных посредством технических средств и реагирования на них
Заключение
Список литературы

Введение

Стремительное развитие технологий и общества в целом привело к стиранию границ между странами в виртуальном пространстве. Данное явление влечет за собой множество положительных последствий: возможность международного общения, доступность зарубежного образования, способность покупать товары из-за рубежа

и т. д. Однако оно не лишено и негативных проявлений, одним из которых является нелегальная трансграничная передача персональных данных.

Сегодня в России действуют достаточно строгие правила для осуществления такой передачи, в результате чего операторы персональных данных не всегда оказываются способны точно их соблюдать. Помимо этого, с каждым годом все чаще совершаются злоумышленные атаки, в результате которых персональные данные широкого круга лиц оказываются в открытом доступе и на зарубежных серверах, что нарушает конституционные права граждан, подрывает национальную безопасность государства и выливается в значительные штрафы для юридических лиц.

В этой связи перед нами стояла цель предложить оптимальную комплексную юридико-технологическую модель минимизации рисков незаконной трансграничной передачи персональных данных, соблюдя при этом баланс интересов всех заинтересованных лиц. Для достижения этой цели нами были решены следующие задачи: изучена история формирования отношений в данной сфере; проанализированы действующие нормативные положения, регламентирующие трансграничную передачу персональных данных как на национальном, так и на международном уровнях; сформулированы предложения по оптимизации этих норм; установлены основные каналы, по которым персональные данные могут быть переданы за рубеж, и установлены узлы, посредством воздействия на которые возможно предотвратить несанкционированные потоки; предложен алгоритм выявления инцидентов информационной безопасности в данной области и реагирования на них.

Считаем, что практическая реализация изложенных в настоящей работе предложений и акцентуация внимания на затронутых проблемах не только представят интерес для научного сообщества, но и позволят уменьшить нелегальные трансграничные потоки персональных данных.

1. Правовые аспекты трансграничной передачи персональных данных

1.1. История формирования правоотношений, связанных с трансграничной передачей персональных данных

Сегодня персональные данные априорно ассоциируются с «чувствительной» информацией (Ji et al., 2023), несанкционированное попадание которой третьим лицам является крайне нежелательным. Однако так было не всегда: долгое время в мире господствовал порядок, при котором, с одной стороны, права отдельного человека не имели значения, а с другой – отсутствовали глобализационные явления, порождающие активное международное взаимодействие на частном уровне. В этой связи феномен персональных данных не представлял интереса для его правовой регламентации, а трансграничной передачи такой информации в принципе не существовало – персональные данные человека могли попасть в другое государство только вместе с ним или непосредственно в связи с его скорым прибытием в это государство (например, при путешествии или в рамках направления дипломатических представителей из одной страны в другую). В то же время, если «личность» кого-то похищалась и противоправно использовалась за рубежом, данный факт никак не сказывался на жизни того, чьи данные оказались у злоумышленников.

Вместе с тем развитие общества постепенно привело к системным изменениям и в сфере персональных данных: так, уже во время Великой французской революции был поднят вопрос об уважении личности, ее свобод и в том числе права на личную тайну.

В Российской империи подобные права были легализованы по инициативе самого императора: Александр II принял Почтовый и Телеграфный уставы, в которых закрепил неприкосновенность частной жизни и тайну переписки. Также в Уголовном уложении были предусмотрены санкции за нарушение указанных норм (Балашкина, 2007). Подобная гарантия соблюдения личной тайны была исключена из правового поля после Великой Октябрьской революции, однако в Конституции СССР 1936 г. вновь появились положения, предусматривающие неприкосновенность личности, тайну переписки[1].

Однако в строгом понимании концепция персональных прав человека была еще очень далека от устоявшегося сегодня понимания персональных данных и режима их защиты. Первым профильным явлением, приближенно отвечающим современным реалиям, стала теория С. Уоррена и Л. Брендайса – американских юристов, которые в 1890 г. сформулировали понятие privacy как права «быть оставленным в покое» (Балашкина, 2007). Спустя примерно полвека было дано судебное толкование данной категории, из которого следует, что под privacy подразумевается неприкосновенность персональных данных и этот принцип вытекает из первых поправок к Конституции США.

Широкое же развитие концепция персональных данных получила только во второй половине XX в. и примерно в то же время на фоне зарождающейся цифровизации и интенсифицирующихся глобализационных явлений возник феномен трансграничной передачи такого рода информации.

Оговоримся, что под трансграничной передачей данных мы понимаем перемещение из государства, в котором субъект добровольно предоставил определенные сведения, позволяющие идентифицировать (однозначно установить) его личность, конкретному лицу (оператору), в иное государство с предоставлением третьим лицам последнего, совершенное оператором, в том числе без уведомления субъекта. Таким образом, равно как и законодательные нормы, о которых будет сказано далее, мы не рассматриваем ситуацию самостоятельного сообщения субъектом сведений о себе представителям иного государства, например, в случае путешествия за границу, когда при заселении в отель человек предоставляет свой паспорт и его данные вносятся в базу данных зарубежной гостиницы.

Интерес международного сообщества к описанному явлению оформился только после начала «компьютерной эпохи» (Romansky & Noninska, 2020; Zheng, 2021), поскольку в это время стали очевидны многие риски, связанные с отсутствием единых стандартов межгосударственного оборота персональных данных и их защиты в процессе такого оборота.

С одной стороны, получение различных прав и привилегий, реализация естественных интересов людей в эпоху широкого распространения Интернета почти невозможны без трансграничных потоков различных персональных данных (Fuentes, 2020). Это связано с развитием международного бизнеса, когда учредитель расположен в одном государстве, а его филиалы и представительства

[1] Глушкова, С. И. (2002). Права человека в России: теория, история, практика: учеб. пособие. Екатеринбург.

функционируют во множестве стран; дистанционным оформлением зарубежных командировок внутренней кадровой службой; направлением тяжелобольного человека на лечение в другое государство и множеством иных, нередко самых бытовых ситуаций (Артемова, 2023). Отдельно следует описать практику, широко распространенную в России до 2015 г. и связанную с использованием зарубежных баз данных, расположенных вне пределов Российской Федерации, для хранения персональных данных, полученных отечественными компаниями. Подобное использование сторонних ресурсов было связано с их дешевизной и существованием как таковых (Смоленский, Левшин, 2016), поскольку ранее в России отсутствовал запрос на разработку собственных надежных и доступных бизнесу различного размера баз данных, способных обрабатывать значительные объемы информации и выдерживать злоумышленные атаки. На аналогичные проблемы указывается и в зарубежных публикациях (Abdulrauf et al., 2023).

С другой стороны, персональные данные – очень ценный ресурс в условиях современного мира. Их легальная обработка позволяет коммерческим компаниям производить более адаптированные под интересы целевой аудитории товары, создавать таргетированную рекламу, привлекая новых клиентов и увеличивая прибыль. Для государств персональные данные необходимы в целях борьбы с преступностью и различного рода правонарушениями (в части использования камер с автоматическим распознаванием лиц, проведения геномной и дактилоскопической идентификаций и пр.), агрегирования статистических данных о населении (состояние здоровья, уровень жизни и т. п.), прогнозировании политических решений, которые получат поддержку населения, и др. Одновременно с этим персональные данные интересны и для злоумышленников, поскольку предоставляют им возможность реализовать различного рода хищения, дискредитировать конкретную личность в медиапространстве, шифровать собственную личность при реализации противоправных действий и т. д.

Таким образом, формируется многосторонний конфликт интересов даже в рамках одного государства, где граждане ратуют за неприкосновенность и сохранение в тайне собственных персональных данных (Абрамова, 2020), коммерческие организации стремятся увеличить прибыльность собственного бизнеса за счет использования информации о клиентах, злоумышленники стараются похитить персональные данные, чтобы облегчить или обеспечить возможность совершения тех или иных преступных действий, а государство стремится к единоличному контролю за максимальным числом сведений о собственных гражданах.

Ситуация усугубляется, если добавить фактор трансграничности, поскольку у субъектов персональных данных значительно снижается контроль за сведениями о себе; в коммерческом секторе повышается конкуренция, а значит, возрастает и спрос на большие объемы персональных данных потенциальных потребителей; злоумышленникам становится легче остаться безнаказанными и неустановленными за счет распределения различных стадий преступной деятельности по разным странам с различными правовыми режимами, условиями защиты персональных данных и правилами по выдаче преступников; государства же теряют часть контроля за персональными данными собственных граждан и одновременно с этим приобретают потенциальную возможность получения соответствующих сведений о жителях других стран, что может становиться инструментом в международном противодействии и политическом давлении.

Законодательные и международные нормы призваны найти баланс между частными интересами свободы физических лиц, коммерческим интересом компаний и стремлением государств к обеспечению безопасности. Представляется, что современные нормы права вполне обеспечивают некий компромисс в этих отношениях, однако они основываются на презумпции добросовестности всех сторон взаимодействия, что приводит к упущению преступного элемента. Вместе с тем наибольшую угрозу и для естественных прав граждан, и для коммерческого интереса организаций, и для национальной безопасности государств несет злоумышленное похищение персональных данных или нарушение режима их секретности, в результате которого сведения о людях попадают в открытую сеть.

Так, только за 2023 г. было выявлено 168 утечек персональных данных, наиболее крупными из которых стали:

– из программы лояльности «Спасибо» от Сбербанка – 52,5 млн записей;
– из сети по продаже одежды для спорта «Спортмастер» – 46 млн записей;
– из онлайн-аптеки zdravcity.ru – 8,9 млн записей;
– из сервиса «Кассы.ру» – 4,5 млн записей;
– из магазина ювелирных изделий Zoloto585 – 9,9 млн записей;
– от страховщика «Согаз» – 8,3 млн записей.

Отдельно заслуживает внимания ситуация получения неправомерного доступа к персональным данным 1 000 000 пользователей МТС Банка. Всего было неправомерно обнародовано три файла с персональной информацией клиентов. Первый включал миллион строк с именами, номерами телефонов, полом, ИНН и гражданством. Во втором было три миллиона записей с типами, частью 16-значных номеров карт и датами их выпуска. Третий файл включал 1,8 млн телефонов, 50 000 e-mail и пользовательские идентификаторы[2].

Один из наиболее масштабных инцидентов произошел летом 2024 г., когда в открытый доступ попали сведения, обрабатываемые Департаментом информационных технологий Москвы, по состоянию на сентябрь 2023 г. В обнародованном файле содержится 13 462 446 строк со следующей информацией о москвичах и гостях столицы, которые использовали цифровые сервисы:

– фамилия, имя, отчество;
– номер телефона (7,2 млн уникальных номеров);
– адрес электронной почты (4,8 млн уникальных адресов, более 16 тыс. из которых находятся на домене @mos.ru);
– адрес регистрации и фактического места проживания;
– дата рождения;
– серия, номер паспорта или свидетельства о рождении;
– место рождения;
– номер социальной карты москвича;
– номер полиса обязательного медицинского страхования[3].

---

2 Талаш, А. Утечка персональных данных: громкие скандалы, кого оштрафовали в прошлом году и как будут наказывать в 2024? Rosco. https://clck.ru/3EmK8s

3 Нефедова, М. В ДИТ Москвы заявили, что опубликованные хакерами данные – это компиляция. Хакер. https://clck.ru/3EmK9J

Укажем, что на момент написания работы правительство Москвы не подтверждает факт произошедшей утечки, сообщая о компиляции данных, свободно находящихся в сети по вине самих граждан либо в результате нарушения безопасности иных операторов.

Во всех описанных ситуациях персональные данные россиян попадали также на информационные ресурсы зарубежных государств, т. е. осуществлялась явная незаконная трансграничная передача данных по принципу прорвавшейся плотины. Однако неменьшую опасность представляет более скрытая трансляция такого рода сведений за рубеж[4].

Всего же за 2023 г. в открытый доступ попало более 300 млн записей с персональными данными российских граждан, что обернулась для бизнеса штрафами на общую сумму свыше 4,6 млн рублей[5]. И это только статистика по Российской Федерации, тогда как проблема носит мировой характер (Jurcys et al., 2022). Однако представляется, что ужесточение ответственности юридических лиц за происходящие нарушения конфиденциальности персональных данных пользователей не является оптимальной мерой, поскольку направлено на разрешение симптомов, но не борьбу с первопричиной – злоумышленниками, осуществляющими кибератаки. Такая ситуация связана, на наш взгляд, со сложностью выявления утечек в процессе, когда конфиденциальность уже нарушена, но данные еще не стали широкодоступными, а также с фактом принадлежности преступников к другим государствам и использованию ими высокотехнологичных средств шифрования собственных личности и действий. В этой связи представляется необходимым, с одной стороны, развивать международное и национальное законодательство в части наказания действительно виновных в нарушении неприкосновенности персональных данных, а с другой – создавать и внедрять в практическую деятельность Роскомнадзора специальные технологические средства выявления и блокировки противоправной трансграничной передачи персональных данных. Именно анализу действующего законодательства в рассматриваемой сфере и описанию моделей подобных технологических решений будут посвящены следующие части настоящей работы.

1.2. Регулирование трансграничной передачи персональных данных законодательством Российской Федерации международными нормами

В Российской Федерации базовой нормой, определяющей порядок трансграничной передачи персональных данных, выступает ст. 12 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[6] (далее – 152-ФЗ), которая претерпела с 2006 г. четыре редакции. Если изначально в ней было только три части, то сегодня, с последними поправками от 14 июля 2022 г., она состоит из 15 частей. Указанное наглядно подтверждает тенденции, с одной стороны, к интенсификации

[4] Пояснительная записка к проекту Федерального закона «О внесении изменений в Федеральный закон “О персональных данных” и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных». СОЗД. https://clck.ru/3EmKC8

[5] Роскомнадзор зафиксировал 168 утечек данных в 2023 году. Право.ru. https://clck.ru/3EmKCx

[6] О персональных данных. № 152-ФЗ от 27.07.2006/ (2006, 31 июля). Собрание законодательства Российской Федерации, № 31 (ч. I), ст. 3451.

глобализационных процессов, а с другой – к увеличению случаев такой трансграничной передачи данных, которая, не будучи напрямую запрещенной законом, нарушает законные права и свободы граждан, интересы государства в целом. Мы не будем углубляться в историческое сопоставление, сосредоточив свое внимание на актуальном нормативном регулировании вопроса.

Так, современная редакция статьи детально регламентирует процедуру трансграничной передачи персональных данных, согласно которой:

1. Перечень государств, в которые могут передаваться персональные данные из России, условно ограничен теми странами, которые либо являются членами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, либо обеспечивают высокие стандарты защищенности персональных данных по национальному законодательству.

2. Данное правило не является абсолютным, так как в крайних случаях возможна передача персональных данных в иные государства.

3. Любой оператор персональных данных обязан направлять в уполномоченный орган – Роскомнадзор[7] – отдельное мотивированное уведомление о намерении передать персональные данные за границу, указывая цели передачи, страну и конкретных получателей этой информации.

4. Роскомнадзор может принять решение о запрете передачи персональных данных в определенное государство или в определенной ситуации.

5. Указанная возможность не является абсолютной, однако круг оснований очень широкий и включает в себя:

– защиту основ конституционного строя России, нравственности, здоровья, прав и законных интересов граждан;

– обеспечение обороны страны и безопасности государства;

– защиту экономических и финансовых интересов Российской Федерации;

– обеспечение дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других ее интересов на международной арене.

6. Если будет принято решение о недопустимости передачи персональных данных, когда такая передача уже состоялась, то переданные персональные данные должны быть уничтожены, за что отвечает первоначальный оператор.

Также необходимо отметить, что в тексте ст. 12 152-ФЗ предусмотрено, что трансграничная передача персональных данных осуществляется в соответствии с вышеназванным федеральным законом и международными договорами Российской Федерации, которые, учитывая положения Конституции Российской Федерации, не могут быть приняты, если их положения или толкование противоречит Основному закону. В этой связи при анализе международных актов считаем целесообразным остановиться только на документах, ратифицированных в Российской Федерации.

---

7 Постановление Правительства РФ № 228 от 16.03.2009. https://clck.ru/3EmKGN

Центральным международным договором, который применяется для решения вопросов трансграничной передачи данных, является Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[8] (далее – Конвенция). Данная конвенция была принята в 1981 г. и незначительно модернизирована в 2018-м (в нее включены нормы, регламентирующие использование систем на основе технологии искусственного интеллекта для автоматизированной обработки персональных данных). Изначально документ подписали 44 государства, на сегодняшний день ее членами наравне с Россией являются 55 государств: Австрия, Азербайджан, Албания, Андорра, Аргентина, Армения, Бельгия, Болгария, Босния и Герцеговина, Буркина-Фасо, Великобритания, Венгрия, Германия, Греция, Грузия, Дания, Ирландия, Исландия, Испания, Италия, Кабо-Верде, Кипр, Латвия, Литва, Лихтенштейн, Люксембург, Маврикий, Мальта, Марокко, Мексика, Молдова, Монако, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сан-Марино, Северная Македония, Сенегал, Сербия, Словакия, Словения, Тунис, Турция, Украина Уругвай, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония.

Данный нормативный акт регулирует отношения, возникающие при хранении персональных данных, т. е. любой информации об определенном или поддающемся определению физическом лице: осуществлении логических и/или арифметических операций с этими данными, их изменении, уничтожении, поиске или распространении, если эти действия осуществляются полностью или частично с помощью автоматизированных средств. В общих чертах положения Конвенции аналогичны нормам и гарантиям, закрепленным в 152-ФЗ, поскольку именно на основе Конвенции был принят закон Российской Федерации, однако, что естественно для международных соглашений, она носит более диспозитивный характер, оставляя широкий простор для усмотрения договаривающихся сторон. Мы не будем останавливаться на обзоре данной Конвенции, осветим лишь ту норму, которая непосредственно касается темы настоящего исследования.

Так, ст. 12 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных регулирует особенности трансграничной передачи персональных данных, устанавливая в качестве общего правила, что Стороны не могут запрещать или ограничивать трансграничные потоки персональных данных между собой только по мотиву защиты частной жизни. Вместе с тем из данного правила существует два исключения – в следующих ситуациях Стороны могут свободно запрещать или ограничивать передачу:

1) законодательное регулирование обработки отдельной категории персональных данных в стороне исхода отличается от аналогичных норм в принимающем государстве;

2) с территории принимающего государства персональные данные будут переданы в страну, не являющуюся Стороной Конвенции.

Таким образом, несмотря на, казалось бы, жесткое правило, гарантирующее свободную передачу персональных данных между Сторонами Конвенции, из него существуют два достаточно широких исключения и, кроме того, оно само не является

[8] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 (Страсбург, 28 января 1981 г.). (2014, 3 февраля). Собрание законодательства Российской Федерации, 5, ст. 419.

настолько строгим, как может показаться при поверхностном анализе. Запрещая ограничения по мотиву защиты частной жизни, рассматриваемое положение не запрещает государствам использовать иные основания для подобных ограничений. Например, в России закреплено, что трансграничная передача данных может быть ограничена или запрещена в целях обеспечения национальной безопасности и по иным не менее уважительным и весомым причинам. Из этого можно сделать вывод, что положения ст. 152-ФЗ и ст. 12 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных не противоречат друг другу, национальное законодательство лишь более детально регламентирует вопросы, обеспечивая большую защищенность для персональных данных своих граждан.

Представляется, что подобный подход является правильным, поскольку, как это было показано выше и отмечается учеными, персональные данные являются чувствительной информацией, попадание которой к злоумышленникам может существенно навредить как одному конкретному гражданину, так и обществу в целом (Акулин и др., 2020). Однако действующее на сегодняшний день нормативное и организационное регулирование трансграничной передачи персональных данных далеко от совершенства. Существует позиция, что наиболее правильной является модель свободной передачи персональных данных между странами, а условное или запретительное регулирование негативно влияет на процессы международного взаимодействия (Ferracane & Van der Marel, 2024). Вместе с тем, на наш взгляд, указанная точка зрения сосредоточена исключительно на интересах бизнеса и игнорирует вопросы прав человека, обеспечения национальной безопасности и риски преступной деятельности в рассматриваемой сфере, в связи с чем необходимо разрабатывать более консенсуальную охранительную модель.

В первую очередь необходимо отметить, что, как известно, норма права должна состоять из трех элементов: гипотезы (описывающей общественные отношения, подлежащие регулированию), диспозиции (указывающей на требуемое или запрещенное поведение в данных общественных отношениях) и санкции (предусматривающей наказание за нарушение требований (запретов) к поведению). Если какой-либо из частей нет, то норма является «мертвой» и в действительности не будет применяться, лишится регулятивной силы. В этой связи, для того чтобы установленные ст. 12 152-ФЗ строгие правила трансграничной передачи персональных данных соблюдались, за их нарушение должна быть предусмотрена ответственность, с которой все не так однозначно. КоАП РФ в ст. 13.11, состоящей из девяти частей, предусматривает ответственность за различные нарушения законодательства о персональных данных, однако специальной нормы в части трансграничной передачи указанных сведений не существует, в связи с чем приходится обращаться к общему составу.

Так, ч. 1 ст. 13.11 КоАП РФ предусматривает, что «Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, влечет наложение административного штрафа на граждан в размере от 2 000 до 6 000 рублей; на должностных лиц – от 10 000 до 20 000 рублей; на юридических лиц – от 60 000 до 100 000 рублей»[9].

[9] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. (2002, 7 января). Собрание законодательства Российской Федерации, № 1 (ч. I), ст. 1.

Однако применение данной нормы видится затруднительным за счет очень размытой формулировки диспозиции. Так, с одной стороны, под случаи, не предусмотренные законодательством, или несовместимые цели может подпадать почти любое действие оператора, а с другой – несложно представить ситуацию, когда осуществляется формально легальная, но по факту противозаконная трансграничная передача персональных данных. Помимо этого, санкция данной нормы, если накладывать ее на ситуацию противозаконной трансграничной передачи персональных данных, оказывается очень незначительной, ведь прибыль от указанных противоправных действий может превышать суммы штрафов в десятки, а то и сотни раз.

Вместе с тем практика Роскомнадзора идет по иному пути: за рассматриваемые нарушения организации привлекаются по ч. 9 ст. 13.11, которая предусматривает, что «невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети “Интернет”, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, влечет наложение административного штрафа на граждан в размере от 30 000 до 50 000 рублей; на должностных лиц – от 100 000 до 200 000 рублей; на юридических лиц – от 1 000 000 до 6 000 000 рублей»[10].

Безусловно, санкция в данном случае намного существеннее, однако формально юридически приведенная норма вводит ответственность только за один частный случай противоправной трансграничной передачи персональных данных – неиспользование отечественных баз данных, что нарушает правило, введенное в 2015 г. В свою очередь, данное нормативное положение появилось только в 2019 г. Аналогичную ситуацию можно наблюдать и сегодня – введенная в 2022 г. усложненная процедура для трансграничной передачи персональных данных не обеспечена на сегодняшний день санкцией за нарушение ее правил, что негативно сказывается на регулятивном механизме. Считаем, что требуется в кратчайшие сроки разработать и принять специальную охранительную норму, направленную на предотвращение незаконной трансграничной передачи персональных данных. При этом считаем, что диспозиция такой нормы должна закреплять умышленную форму вины, чтобы операторы персональных данных не подлежали наказанию за кибератаку, совершенную на них. Это позволит уменьшить латентность подобных инцидентов, обеспечит сотрудничество операторов с правоохранительными органами и реализацию принципа справедливости санкции, так как она будет направлена против действительно виновных лиц. Одновременно с этим, особенно в условиях недружественной международной атмосферы, считаем необходимым ввести дополнительный квалифицирующий признак в ст. 272, 273, 274.1 Уголовного кодекса Российской Федерации (далее – УК РФ), предусмотрев в нем последствия в виде получения неправомерного доступа к охраняемой законом компьютерной информации лицами, находящимися за пределами Российской Федерации.

[10] Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30.12.2001 (ред. от 23.11.2024). (2024). СПС «КонсультантПлюс». https://clck.ru/3ExqcF

Следующая проблема связана с требованием самой ст. 12 152-ФЗ, согласно которой в случае принятия Роскомнадзором решения о запрете или ограничении трансграничной передачи персональных данных «оператор обязан обеспечить уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им персональных данных»[11]. Представляется маловероятным, что правительство зарубежного, особенно недружественного, государства удалит полученные ранее из России персональные данные по указанию какой-либо коммерческой компании из нашего государства. Механизма, в соответствии с которым данное требование должно быть претворено в жизнь, не существует. Таким образом, учитывая уведомительный порядок трансграничной передачи персональных данных в государства, являющиеся Сторонами Конвенции Совета Европы или обеспечивающие адекватный уровень защиты персональных данных (еще 34 государства)[12], а также возможность в исключительных случаях осуществлять трансграничную передачу и в иные государства, создается весьма значительный риск утечек персональных данных россиян, их оставления на враждебной территории, после того как Роскомнадзор примет решение о том, что осуществленная передача не должна была произойти.

Если отойти от специальных норм, то можно выявить иную возможность защиты гражданами своих персональных данных от трансграничной передачи, предусмотренную п. 8 ч. 7 ст. 14 152-ФЗ, согласно которой субъект персональных данных вправе получать информацию об осуществленной или о предполагаемой трансграничной передаче его данных. В системном толковании с ч. 2 ст. 9 и ч. 1 ст. 14 152-ФЗ, предусматривающими, что субъект персональных данных может в любое время отозвать свое согласие на их обработку, а также может требовать от оператора удаления его персональных данных, в случае если человек не согласен с осуществлением трансграничной передачи его персональных данных, он может запретить осуществление таких действий оператором. Однако все описанные процессы должны быть инициированы самим субъектом, оператор не обязан сообщать о планируемой или осуществляемой трансграничной передаче персональных данных, пока от субъекта не поступит запрос на предоставление соответствующей информации. Вместе с тем большинство граждан, не обладая в должной мере развитой правовой культурой, могут не знать о данных особенностях, в связи с чем оказываются неспособными на практике защитить собственные интересы. К тому же, даже будучи осведомленным о приведенных правовых положениях, человек не способен отследить всех операторов, потенциально осуществляющих или планирующих осуществлять трансграничную передачу его персональных данных, поскольку таковых в отношении одного субъекта в современных условиях очень большое количество.

В этой связи считаем необходимым дополнить ст. 12 152-ФЗ правилом, предусматривающим обязательное уведомление субъекта персональных данных о намерении произвести трансграничную передачу информации о нем, а также предоставить

---

11 О персональных данных. № 152-ФЗ от 27.07.2006 (ред. от 08.08.2024). (2024). СПС «КонсультантПлюс». https://clck.ru/3Exr2K

12 Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций № 128 от 05.08.2022. https://clck.ru/3EmKNQ

ему возможность ограничить такую передачу в определенное государство или в конкретных ситуациях.

Несмотря на все сказанное выше, следует признать: в России предпринимаются комплексные меры для обеспечения максимальной защищенности персональных данных проживающих в государстве лиц. Так, нельзя не отметить Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21 июля 2014 г. № 242-ФЗ (так называемый Закон о локализации), внесший изменения в 152-ФЗ, согласно которым запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации должно осуществляться с использованием баз данных, находящихся на территории Российской Федерации[13].

Данное требование представляется весьма действенным для защиты персональных данных россиян, минимизации рисков утечек информации, обеспечения государственного контроля за сведениями о своих гражданах, а также исключения риска возникновения ситуаций, когда персональные данные российских граждан окажутся недоступными для отечественных компаний и государства по причине блокировки тех или иных зарубежных сервисов, отключения российских пользователей от зарубежных баз данных, будут использоваться для совершения преступлений. Однако данной позиции придерживаются не все – так, уже в 2015 г., когда описанная норма только вступала в силу, были разработаны сценарии ее обхода с целью минимизации убытков бизнеса (Веселицкий, 2015). В связи с чем на сегодняшний день можно ожидать широкое распространение серых схем, позволяющих в действительности хранить персональные данные российских граждан за рубежом.

Из всего описанного выше можно сделать вывод, что нормативная регламентация рассматриваемого вопроса не способна в должной мере обеспечить защиту персональных данных россиян. Однако предупреждение случаев незаконной трансграничной их передачи – фундаментальная задача российского государства, от решения которой зависит безопасность населения страны и устойчивость государственной власти. В этой связи необходимо не только совершенствовать законодательство, но и разрабатывать технологические механизмы, которые позволили бы эффективно выявлять и блокировать подозрительные потоки персональных данных за пределы территории Российской Федерации до выяснения всех обстоятельств и принятия квалифицированного решения.

2. Технико-технологические аспекты трансграничной передачи данных

2.1. Основные технические каналы связи, по которым осуществляется трансграничная передача персональных данных

Для того чтобы перейти к непосредственному описанию технических средств предотвращения незаконной трансграничной передачи персональных данных, необходимо определить каналы потенциальной утечки информации. В настоящее время передача

[13] О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях. № 242-ФЗ от 21.07.2014. (2014). https://clck.ru/3EmKSW

персональных данных, которая может представлять угрозу, осуществляется посредством компьютерных сетей. Безусловно, многие компании, например, ведут бумажные личные дела сотрудников, однако ситуация, при которой идентифицирующие сведения из них будут получены в большом объеме, сохранены, переданы через границу и опубликованы так, чтобы быть доступными широкому кругу лиц, в том числе в целях их последующего преступного использования, полностью посредством аналоговых форм, представляется нереалистичной. Именно поэтому нами будут рассмотрены именно технические каналы связи, представленные компьютерными сетями.

Для прогнозирования уровня угрозы от противоправного доступа к информации, а также определения возможностей минимизации кибератак и утечек важно точно определить территорию, в рамках которой действует канал связи. Так, выделяются:

1. Глобальные сети. Самой известной из них является Интернет; они опоясывают весь мир. Кроме того, к глобальным будут относиться и внутринациональные сети, функционирующие в пределах конкретной страны или региона. Обеспечить полноценную защиту информации в таких сетях почти невозможно из-за принципа открытости и общедоступности, лежащего в основе их функционирования.

2. Городские сети. Из названия очевидно, что они существуют в пределах города. Однако чаще к этому уровню относят только сети, обслуживающие мегаполисы или городские агломерации. Именно на уровне городских сетей изначально было организовано специальное программное обеспечение «Паутина».

3. Корпоративные сети (организаций, предприятий). Сети данного уровня, с одной стороны у́же городских, поскольку направлены на обслуживание отдельных предприятий, но с другой – такие сети действуют трансгранично, т. е. позволяют связывать между собой филиалы и подразделения, расположенные в разных городах, регионах и странах.

Отметим, что корпоративные сети являются наиболее уязвимыми с точки зрения информационной безопасности, защищенности от кибератак, поскольку охватывают значительную территорию, но обслуживаются частным сектором, который бывает ограничен в ресурсах для постоянного обновления протоколов безопасности и не связан столь строгими правилами защиты информации, как государственные предприятия.

Вместе с тем к корпоративным сетям будут относиться и ведомственные каналы связи, степень защищенности которых наивысшая, поскольку по ним передается информация ограниченного доступа.

4. Локальные сети сосредоточены на небольшой территории (обычно в радиусе 1–2 км). Они функционируют на территории одного предприятия (завода, больницы, образовательного учреждения и т. п.). Обычно такие сети защищены достаточно хорошо, так как организованы в секторе, где оборот охраняемой законом информации осуществляется на ограниченной территории и посредством идентифицированного оконечного оборудования, при наличии достаточных ресурсов для настройки и поддержания систем безопасности.

5. Персональные сети предназначены для взаимодействия устройств, принадлежащих одному владельцу (членам семьи), на небольшом расстоянии (обычно до 10 м). Несмотря на низкую степень территориальной распределенности, отдельный человек может не уделять достаточного внимания соблюдению правил информационной безопасности и цифровой гигиены, что ставит его инфраструктуру под угрозу.

Как очевидно из приведенной классификации, трансграничная передача персональных данных может осуществляться исключительно по глобальным и корпоративным сетям. Вместе с тем в последнем случае подобного рода информация защищается и, если происходит инцидент, безопасность нарушается, то сведения передаются на глобальные сети, где и становятся доступными широкому кругу лиц, в том числе представителям иных государств. В этой связи можно сделать промежуточный вывод, что контроль за незаконной трансграничной передачей персональных данных будет наиболее эффективным на границе защищенного канала связи и глобальной сети. Такой подход позволит минимизировать риски ложноположительных ошибок, когда блокироваться будут легальные внутренние (между государственными органами, внутри подразделений юридического лица, между устройствами одного пользователя) потоки.

Для обоснования данного тезиса считаем необходимым остановиться подробнее на характеристике глобальных компьютерных сетей. Основная их характерная черта заключается в том, что они имеют децентрализованную архитектуру, распределены по континентам, странам, а физически могут быть расположены не только на земной поверхности, но и над ней, под водой – где угодно. Часть сегментов глобальных сетей могут быть продублированы в том числе с помощью спутниковых коммуникаций. Это в совокупности с указанным ранее основополагающим принципом открытого доступа позволяет создать систему, при которой любое устройство, имеющее выход в глобальную сеть, может взаимодействовать с любым иным подключенным оборудованием.

Чаще всего глобальные компьютерные сети опираются на выделенные линии, на одном конце которых маршрутизатор подключается к локальной сети, а на другом – коммутатор связывается с остальными частями глобальной. Более подробно об этих элементах будет сказано далее, так как они имеют определенное значение для выявления фактов несанкционированной передачи персональных данных.

Отметим, что современные компьютерные сети очень многое унаследовали от своих предшественников – линий телефонной связи. Главное технологическое новшество, которое привнесли с собой первые, состояло в отказе от принципа коммутации каналов, при котором для взаимодействия требуется физическое подключение двух устройств, выделение для их связи отдельного канала. На смену ему пришла технология многоуровневой коммутации пакетов, когда информация разделяется на маленькие блоки, передающиеся адресату по разным маршрутам.

В связи с таким устройством глобальных компьютерных систем невозможно контролировать потоки информации (в том числе персональных данных), когда они оказываются внутри системы (Иванова и др., 2010), поэтому все мероприятия по блокировке канала передачи данных должны быть осуществлены на местном уровне, поддающемся централизованному администрированию.

Помимо уровня сети, важным для вопроса предотвращения несанкционированных потоков персональных данных является определение среды, по которой передается информация. Это может быть:

– оптоволокно;
– медные провода;
– инфракрасный канал;
– радиоканал (Wi-Fi, LTE, Bluetooth и др.).

Проще всего осуществлять перехват, а значит, и блокирование информации, передающейся по материализованным средам – оптическим волокнам и медным проводам, так как в этом случае, что будет показано далее, техническое устройство, выявляющее несанкционированные потоки персональных данных, можно установить непосредственно на сам канал. Однако в этом случае весьма затруднительно определить тип передающихся данных – для этого необходимо осуществить их расшифровку, что требует дополнительных временных затрат и использования специального оборудования. Поэтому намного полезнее иметь доступ к так называемым узлам инфраструктуры – локальному сетевому оборудованию, которое может быть активным или пассивным.

Активное оборудование – это те устройства, которые непосредственно подключены к сетям и в связи с этим обеспечивают передачу и маршрутизацию данных. С помощью них возможно осуществлять полный цикл обработки данных: прием, систематизацию, хранение, управление, передачу – для этого такие устройства оборудованы собственным процессором и оперативной памятью.

Пассивное оборудование может быть названо вспомогательным: оно характеризуется отсутствием собственного источника питания и поэтому не может оказывать какого-либо воздействия на проходящие потоки данных. Здесь можно провести метафорическую аналогию с мостом через реку, когда по обеим сторонам от него установлены светофоры, знаки, регламентирующие порядок движения, но сам он – только участок дороги, на котором получить новую информацию и модернизировать под ее влиянием поведение нельзя. Так и пассивное оборудование лишь создает среду для передачи данных, не управляя трафиком и не производя обработку данных. К пассивному оборудованию относятся, в частности:

– кабели (например, витая пара или оптоволоконный кабель), применяющиеся для соединения устройств и передачи данных между ними;

– разъемы, патч-панели и кроссовые поля, применяющиеся для соединения кабелей и устройств;

– разветвители или сращивающие коробки, применяющиеся для разделения или объединения оптоволоконных линий связи.

Таким образом, роль пассивного сетевого оборудования сводится к обеспечению более эффективного и надежного функционирования сети, в связи с чем блокировать потоки персональных данных на нем затруднительно.

Активное сетевое оборудование очень разнообразно и выполняет различные функции:

– распределение трафика между сетями;

– соединение локальных сетей на разных уровнях (от внутриорганизационного до мирового);

– обеспечение беспроводной связи между устройствами внутри локальной сети;

– определение целевого направления пакетов данных.

Последнее представляет особый интерес для настоящего исследования, поскольку таким образом возможно установить, что определенные чувствительные данные направляются за рубеж (на устройство, MAC-адрес которого зарегистрирован за рубежом).

Исходя из рассмотренных особенностей, следует, что для эффективного предотвращения несанкционированных трансграничных потоков чувствительной информации, минимизации рисков ложноположительных и ложноотрицательных ошибок при определении направления движения информации необходимо с помощью специализированных технических устройств воздействовать именно на активное сетевое оборудование.

Вместе с тем существует множество различных типов сетевых устройств, каждое из которых обладает своими уникальными особенностями, характеристиками и предназначением, в связи с чем мы остановимся только на кратком описании тех из них, на которые целесообразно воздействовать для предотвращения несанкционированных трансграничных потоков персональных данных.

1. Коммутатор, или свитч. Это устройство, имеющее временную (промежуточную) память, связывает конечное число устройств в единую сеть. Количество устройств, которые может связать коммутатор, зависит от числа имеющихся у него портов.

Общий принцип его работы можно представить следующим образом: на первом этапе на коммутатор поступают данные, которые передаются на все порты, при этом MAC-адрес отправителя идентифицируется и закрепляется за одним конкретным портом. Далее, если поступают пакеты, предназначенные для устройства с идентифицированным MAC-адресом, то они передаются только на закрепленный за ним порт. В противном случае данные передаются на все порты. Со временем происходит идентификация всех взаимодействующих в сети устройств.

В аспекте рисков несанкционированной трансграничной передачи данный коммутатор может быть полезен для детекции источника их исхода (т. е. определения личности виновного сотрудника), а также выявления самого факта передачи персональных данных.

Аналогичные функции, но в ином, более широком масштабе выполняют концентраторы (хабы), которые отличаются от коммутаторов большей уязвимостью к угрозам информационной безопасности за счет меньшей «интеллектуальности».

2. Роутер, или маршрутизатор, предназначен для передачи пакетов данных между разными компьютерными сетями. Для этого он использует таблицу маршрутизации, в которой содержатся MAC-адреса оконечных устройств и пути связи с ними. Роутер сопоставляет MAC-адрес получателя, указанный в пакете данных, с указанной таблицей и передает сведения адресату. Одновременно с этим маршрутизатор – модерируемая система, функционирующая по правилам, заданным администратором, который может указать на необходимость фильтрации трафика, шифрования (дешифрования) определенных данных, осуществления иной их обработки.

Таким образом, осуществлять детектирование инцидентов несанкционированной трансграничной передачи данных оптимальнее всего именно на уровне маршрутизатора, автоматизировав этот процесс посредством введения нескольких дополнительных правил на этапе его установки и настройки. Однако маршрутизатор не предназначен специально для такого контроля, в отличие от следующего элемента сетевой инфраструктуры.

3. Межсетевой экран, или Firewall, – программный или программно-аппаратный комплекс, специально функционирующий для защиты компьютерной сети от несанкционированного доступа, злоумышленных атак, хищения данных и других угроз внешней среды. Основные задачи, решаемые межсетевым экраном, сводятся к следующим:

– фильтрация трафика;

– блокировка попытки входа в сеть из неизвестных или недоверенных источников;

– блокировка передачи (приема) определенных типов трафика (например, трафика с вредоносным содержимым или персональными данными) и пр.

Безусловно, любое из описанных устройств может быть использовано для детекции потоков персональных данных, предотвращения или как минимум выявления не только их свободной передачи за рубеж, но и злоумышленного похищения. Однако наибольший эффект такие мероприятия будут иметь при их воспроизведении на узлах маршрутизаторов и межсетевых экранов. Далее мы рассмотрим несколько обобщенный сценарий указанных защитных мероприятий.

2.2. Модель выявления фактов незаконной трансграничной передачи персональных данных посредством технических средств и реагирования на них

Прежде чем перейти к описанию заявленной модели, оговоримся, что настоящая часть исследования будет предметно ограничена действиями внутри юридического лица или государственного органа, являющихся операторами персональных данных. Также мы не будем рассматривать методы предотвращения атак, нацеленных на хищение персональных данных, так как они в общем виде сводятся к постоянному обновлению протоколов безопасности и оборудования, соблюдению всех требований технических регламентов и Роскомнадзора в данной сфере, использованию сертифицированного и лицензионного программного обеспечения. Однако и эти меры не гарантируют безуспешность любых злоумышленных атак, поэтому считаем важным создать механизм выявления нелегальных трансграничных потоков персональных данных вне зависимости от того, по какой причине они произошли: в результате внешнего прорыва контура безопасности или вследствие неправомерных (либо ошибочных) действий со стороны самого оператора. При этом, поскольку основная проблема на сегодняшний день сосредоточена вокруг крупных операторов персональных данных в лице корпораций и государственных органов, мы сосредоточимся именно на детекции потоков из локальных, городских и корпоративных сетей, которые далее для упрощения будут обобщенно называться локальными.

Укажем, что базовым мероприятием, в рамках которого может быть выявлена и предотвращена несанкционированная трансграничная передача персональных данных, является контроль. Представляется, что он не только должен быть предусмотрен в локальных актах и инструкциях как обязательный элемент управления сетью, но и состоять из совместных усилий технических, в том числе автоматизированных, устройств и человека.

Процесс контроля работы сети обычно делят на два этапа: мониторинг и анализ. Вместе с тем большое значение имеет предварительная подготовка, которая подразумевает разработку локальных актов организации, нормативное закрепление порядка выявления, обработки информации об инцидентах информационной безопасности и реагирования на них (Rowe, 2003).

На этапе мониторинга собираются первичные данные, необходимые в дальнейшем для осуществления анализа ситуации и принятия обоснованного решения (Pascual et al., 2024). Мониторинг, особенно у крупных операторов персональных данных, может (и, скорее, должен) осуществляться с помощью технических средств.

Причем считаем необходимым разработать программно-аппаратный модуль, который можно будет интегрировать в оборудование конкретной организации, государственного органа, адаптировать под специфику деятельности оператора и его технико-технологические ресурсы, обеспечивая эффективное накопление всей релевантной информации. Такое устройство должно работать по следующему алгоритму:

1. Фиксация факта, исходящего за пределы локальной сети потока данных (любых).

2. Фильтрация потоков персональных данных (их задержка).

3. Определение направления данных потоков.

3.1. Если поток направлен за границу – его блокирование.

3.2. Если поток носит внутренний характер – его пропуск.

4. Информирование уполномоченного лица оператора о выявленном потоке, передача такому сотруднику всей сопроводительной информации (время, источник, направление и т. д.).

При этом может быть использована программная реализация, аналогичная той, которая уже положительно зарекомендовала себя при выявлении и обработке цифровых следов пользователя (Daniela & Amélie, 2022). Отметим также, что при необходимости такое устройство может быть настроено на блокировку любых потоков персональных данных или иного рода сведений до их предварительной проверки уполномоченным лицом.

Далее уполномоченным работником выполняется анализ – осмысление собранной на этапе мониторинга информации, сопоставление ее с профильными (целевыми) шаблонами и последующее принятие управленческого решения. На данном этапе человек должен оценить в части трансграничных потоков персональных данных:

1) передаются ли они в государство, являющееся стороной Европейской конвенции или обеспечивающее надлежащую защиту персональных данных;

2) уполномочен ли оператор на осуществление трансграничной передачи персональных данных;

3) направлено ли уведомление о данной передаче в Роскомнадзор;

4) соответствует ли информация, указанная в уведомлении, обстоятельствам и содержанию передающихся персональных данных;

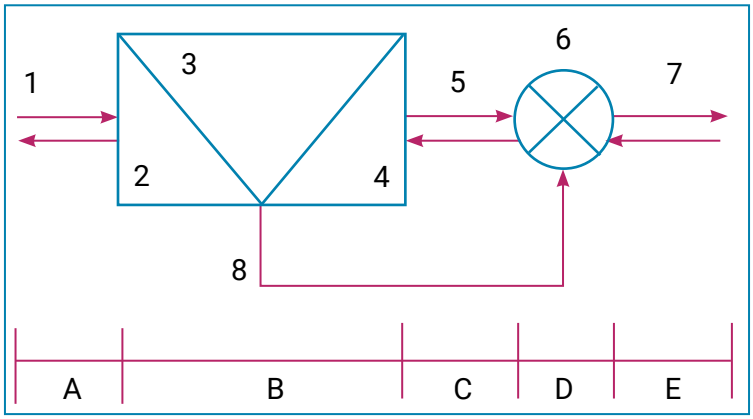
5) нет ли запрета или ограничения на передачу этих персональных данных в конкретное государство при существующих условиях;

6) не поступило ли возражение от субъекта персональных данных на передачу сведений о нем за границу;

7) не нарушают ли цели передачи персональных данных законодательства Российской Федерации;

8) кто является инициатором передачи персональных данных (сотрудники организации или внешний субъект, нарушивший безопасность локальной сети).

После ответа на все указанные вопросы уполномоченное лицо принимает решение, допустить трансграничную передачу персональных данных или сообщить руководителю (либо в правоохранительные органы) о выявленном и своевременно предотвращенном инциденте информационной безопасности. В общем виде описанная модель представлена на рисунке.



Графическое представление модели выявления факта трансграничной передачи персональных данных и принятия управленческого решения

На участке «A» цифрой 1 показаны входящие и исходящие потоки данных физического, сетевого, канального, транспортного, сеансового, представительского, прикладного уровней. Получение для последующего анализа информации от всех семи уровней модели ISO/OSI в простых, иерархических, маршрутных, агрегатных и прочих формах необходимо в связи с тем, что поступающие данные, в том числе персональные, могут иметь не только текстовое представление.

На участке «B» в модуле 2 происходит определение получателя данной информации путем анализа его IP-адреса, доменного имени, иных подобных сведений и сопоставления с официальными данными о регистрации данных IP-адресов.

Сведения о принадлежности IP-адреса к географической (страновой) локации и юридическому или физическому лицу могут быть получены из официальных ресурсов регистраторов доменных имен[14]. Разумеется, в рассматриваемой модели наивысший приоритет доверия будет принадлежать регистраторам доменных имен, осуществляющим свою деятельность на территории России (в силу норм действующего законодательства и регуляторных норм Федеральной службы по техническому и экспертному контролю, Федеральной службы безопасности Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и пр.).

Если получатель находится в пределах Российской Федерации, то дальнейший анализ пакета не производится и он пропускается без изменений на участок «D» модуля 6. Если получатель находится за пределами Российской Федерации, то далее пакет обрабатывается модулем 3.

На участке «B» в модуле 3 происходят сбор и нормализация информации (данных), предназначенных для получателей за пределами страны. Именно здесь предполагается работа уполномоченного работника организации (государственного органа).

Процедура нормализации данных представляет из себя программно-математические преобразования (в том числе, но не ограничиваясь: TLS/SSL, HTTPS, HTTPX, E1/T1, ATM и другие) любых представлений данных в текстовую форму.

[14] Координационный центр доменных имен .RU/.РФ. https://clck.ru/3EmLBZ

На участке «B» в модуле 4 происходит анализ нормализованных данных на соответствие атрибутивно-содержательным признакам подпадающих под определение персональных данных.

Для этого в организации должен быть на уровне локального акта или инструкции определен список обрабатываемых персональных данных и разработаны соответствующие шаблоны (например, регулярные выражения), в соответствии с которыми осуществляется процедура детектирования целевой информации. Укажем, что в зависимости от конкретных задач оператора персональных данных модуль 4 может располагаться перед модулем 3, т. е. предшествовать человеческому анализу.

Если в проанализированном трафике выявлены совпадения с шаблонами информации, недопустимой для передачи, то на участок «D» модуля 6 посылается управляющее воздействие (элемент 8) об уничтожении (отбрасывании) конкретного пакета и журналировании данного события. Такая команда в рассмотренной модели может быть подана уполномоченным сотрудником, однако нельзя исключать и полностью автоматизированную работу предлагаемого программного модуля.

На участке «D» в модуле 6 находится корпоративный межсетевой экран, который, помимо своих основных функций, также при появлении управляющего воздействия (команды) с участка «B» принимает решение об уничтожении (отбрасывании) конкретного пакета и журналировании события защиты информации.

Элементы 5 и 7 являются стандартными потоками информации внутри локальной сети и модуля автоматизированной обработки потоков исходящих данных.

Подобные алгоритмы предлагаются и зарубежными коллективами ученых (Liu et al., 2024; Pascual et al., 2024; Guaman et al., 2021; Yan et al., 2023), в связи с чем считаем небесполезным также налаживать международное сотрудничество в указанной сфере, чтобы наиболее эффективно достигать целей защиты чувствительной информации.

Оговоримся, что рассмотренные нами мониторинг и анализ – лишь части более детального алгоритма, который включает в себя сопутствующие организационные мероприятия (создание локальных актов в сфере обеспечения информационной безопасности, сотрудничество с регулирующими государственными органами, осуществление общей и частной превенции и т. д.). Однако настоящее исследование не претендует на полноту и исчерпывающий характер, в связи с чем считаем достаточным осветить непосредственно те стадии управления, в рамках которых могут быть задействованы специализированные технические средства, как это было заявлено изначально.

Заключение

Подводя итог описанному выше, подчеркнем следующее.

1. Отношения по трансграничной передаче персональных данных смогли развиться только в цифровую эпоху, когда глобальные потоки информации вне границ какого-либо государства стали обыденностью, в связи с чем нормативное и политическое регулирование данной сферы только формируется.

2. Персональные данные являются ценным ресурсом: содержат в себе сведения о личной жизни человека, которые он желает сохранить в тайне; необходимы для развития бизнеса; требуются для эффективной борьбы с преступлениями и правонарушениями; выступают важным компонентом преступной и иной противоправной

деятельности; могут быть фактором в межгосударственной и межполитической борьбе.

3. Нелегальные трансграничные потоки персональных данных несут в себе серьезную угрозу для прав личности, национальной безопасности и финансового благополучия организаций, однако действующие национальные и международные нормы права не обеспечивают достаточный для их предотвращения механизм.

4. Для разрешения указанной проблемы требуется ввести специальный состав за нарушение установленного порядка трансграничной передачи персональных данных в КоАП РФ, дополнить квалифицирующие признаки в статьях УК РФ, посвященных нарушению безопасности компьютерной информации; обязать оператора персональных данных сообщать их субъекту о намерении осуществить трансграничную передачу такого рода информации.

5. Одновременно с оптимизацией законодательства требуется внедрять в системы обеспечения информационной безопасности организаций и государственных органов, выступающих операторами персональных данных, специализированные технические средства детекции несанкционированных трансграничных потоков персональных данных.

6. Применение указанных средств должно производиться по следующему алгоритму: постоянный автоматизированный фоновый контроль всех исходящих потоков информации, определение их направления; выявление потоков, движущихся за границу государства; отнесение информации в данном потоке к персональным данным; блокировка потока, соответствующего двум указанным признакам; сообщение о выявленном потоке уполномоченному работнику организации (государственного органа); оценка человеком допустимости трансграничной передачи данных; принятие решение о пропуске или окончательной блокировке потока; сообщение в последнем случае о выявленном и предотвращенном инциденте информационной безопасности.

Представляется, что реализация описанного алгоритма, а также совершенствование нормативного регулирования в сфере трансграничной передачи персональных данных позволит снизить количество хищений и ненамеренных утечек данного рода чувствительной информации, тем самым защитить права граждан, обеспечить политическую устойчивость Российской Федерации, снизить число преступлений с использованием чужих персональных данных и добиться финансового благополучия у коммерческих организаций.

Список литературы

Абрамова, А. Г. (2020). Современные проблемы осуществления защиты персональных данных в сети: Основополагающие принципы защиты персональных данных. *Регион и мир*, *11*(4), 21–25. https://www.elibrary.ru/eveayh

Акулин, И. М., Чеснокова, Е. А., Гурьянова, Н. Е., Пресняков, Р. А., Летова А. Д. (2020). Возможность трансграничной передачи связанных со здоровьем персональных данных в рамках ЕАЭС: реальность, перспективы. *Менеджер здравоохранения*, *7*, 65–73. https://doi.org/10.37690/1811-0185-2020-7-65-73

Артемова, А. Н. (2023). Правовое регулирование трансграничной передачи персональных данных. *Юридическая наука и практика*, *19*, 3, 9–16. EDN: https://www.elibrary.ru/cgfugw. DOI: https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Балашкина, И. В. (2007). Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации. *Право и политика*, *7*, 92–105. https://www.elibrary.ru/hzyhnn

Веселицкий, О. И. (2015). Вопросы трансграничной передачи персональных данных в соответствии с требованиями 242-ФЗ. *Сборники конференций НИЦ Социосфера*, *53*, 275–279. https://www.elibrary.ru/vbvgev

Иванова, О. В., Иванов, П. В., Смелов, М. Н. (2010). Проблемы и алгоритмы поиска информации в глобальных компьютерных сетях. *T-Comm: Телекоммуникации и транспорт*, *4*(3), 23–25. https://www.elibrary.ru/ophpnz

Смоленский, М. Б., Левшин, Н. С. (2016). Локализация персональных данных граждан РФ как составляющая экономической и национальной безопасности России. *Наука и образование: хозяйство и экономика, предпринимательство, право и управление*, *2*(69), 111–114. https://elibrary.ru/item.asp?id=25423352

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Сведения об авторах



Бахтеев Дмитрий Валерьевич – доктор юридических наук, доцент, профессор кафедры криминалистики имени И. Ф. Герасимова, заведующий лабораторией цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=762765



Сосновикова Анна Михайловна – стажер-исследователь лаборатории цифровых технологий в криминалистике, Уральский государственный юридический университет имени В. Ф. Яковлева
Адрес: 620066, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1196069



Казенас Евгений Владимирович – студент, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Адрес: 620002, Россия, г. Екатеринбург, ул. Мира, 19
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

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 выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77 / Уголовное право
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 28 июня 2024 г.
Дата одобрения после рецензирования – 12 июля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/mjuigd
DOI: https://doi.org/10.21202/jdtl.2024.45

Overcoming Illegal Cross-border Transfer of Personal Data

Dmitry V. Bakhteev ✉
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Anna M. Sosnovikova
Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russia

Evgeniy V. Kazenas
Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russia

Keywords

communications,
computer network,
cross-border data transfer,
digital technologies,
incident,
information security,
information,
law,
legislation,
personal data

Abstract

Objective: to form of a comprehensive interdisciplinary legal and technological risk management model in the field of illegal cross-border transfer of personal data by eliminating legislative gaps and creating a system for automated control of outgoing information flows, as well as expert response to identified incidents.

Methods: in addition to general dialectical and general scientific methods, special legal and cybernetic methods were used. For example, based on comparative legal analysis, the authors reveal differences between national and international regulation of cross-border flows of personal data. In the second section, the modeling method allows forming an algorithm for identifying information security incidents in the field of cross-border transfer of personal data and responding to them.

Results: the article formulates proposals to optimize legislation in the field under study by introducing specialized protective norms for violating the rules of cross-border transfer of personal data and stipulating the operator's obligation to notify personal data subjects of the intention to transfer the information abroad. The second section describes the concept of a software package designed to detect information security incidents in the field under consideration, as well as a model of action of an authorized representative of the operator after receiving a signal from the automated system.

✉ Corresponding author
© Bakhteev D. V., Sosnovikova A. M., Kazenas E. 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: to solve the set problem, the work combines the knowledge and competencies of legal scientists and specialists in the field of information security, which allows an interdisciplinary approach. At the same time, it is stated that the issues of illegal cross-border transfer of personal data have not received proper coverage in science today, since Russian legislation in this area has changed recently. The authors propose not so much to strengthen the sanction for legislation violation in this area, as to ensure the punishment of persons who commit cyberattacks, and to equip personal data operators with an effective tool to minimize the risks of information leakage.

Practical significance: the research results can be used to improve legislation in the field of cross-border transfer of personal data and the organization of activities of authorized employees of the personal data operator for risk management in this area.

For citation

Bakhteev, D. V., Sosnovikova, A. M., & Kazenas, E. V. (2024). Overcoming Illegal Cross-border Transfer of Personal Data. *Journal of Digital Technologies and Law, 2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

References

Abdulrauf, L., Adaji, A., & Ojibara, H. (2023). Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research. *South African Journal of Bioethics and Law*, *17*(1), 44–48. https://doi.org/10.7196/sajbl.2024.v17i1.1969

Abramova, A. G. (2020). Contemporary issues of personal data protection in the network: fundamental principles of personal data protection. *Region i mir*, *11*(4), 21–25. (In Russ.).

Akulin, I. M., Chesnokova, E. A., Guryanova, N. E., Presnyakov, R. A., & Letova, A. D. (2020). Possibility of transboundary transfer of health-personal data within the EAEU: reality, prospects. *Menedzher Zdravookhranenia*, *7*, 65–73. (In Russ.). https://doi.org/10.37690/1811-0185-2020-7-65-73

Artemova, A. N. (2023). Legal regulation of cross-border personal data transfer. *Yuridicheskaya nauka i praktika*, *19*(3), 9–16. (In Russ.). https://doi.org/10.25205/2542-0410-2023-19-3-9-16

Balashkina, I. V. (2007). Features of the constitutional regulation of the right to privacy in the Russian Federation. *Pravo i politika*, *7*, 92–105. (In Russ.).

Daniela, V., & Amélie, M. (2022). A Frequency-Based Learning-To-Rank Approach for Personal Digital Traces. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2920–2929. https://doi.org/10.24251/hicss.2022.361

Ferracane, M., & Van der Marel, E. (2024). Governing personal data and trade in digital services. *Review of International Economics*. https://doi.org/10.1111/roie.12735

Fuentes, I. T. (2020). Legal Recognition of the Digital Trade in Personal Data. *Mexican Law Review*, *12*(2), 87–117. https://doi.org/10.22201/iij.24485306e.2020.2.14173

Guaman, D., Del Alamo, J., & Caiza, J. (2021). GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/ACCESS.2021.3053130

Ivanova, O. V., Ivanov, P. V., & Smelov, M. N. (2010). Problems and algorithms of information retrieval in global computer networks. *T-Comm*, *4*(3), 23–2. (In Russ.).

Ji, P., Shan, F., Li, F., Sun, H., Wang, M., & Shan, D. (2023). Adaptive Sensitive Information Recognition Based on Multimodal Information Inference in Social Networks. *Security and Communication Networks*, *2023*(1), 5627246. https://doi.org/10.1155/2023/5627246

Jurcys, P., Corrales, M. C., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a 'user-held' data model. *Computer Law & Security Review*, *46*, 105691. https://doi.org/10.1016/j.clsr.2022.105691

Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. *Electronics*, *13*(10), 1–23. https://doi.org/10.3390/electronics13101959

Pascual, H. A., Del Alamo, J., Rodríguez, D. T., & Dueñas, J. (2024). Hunter: Tracing anycast communications to uncover cross-border personal data transfers. *Computers & Security*, *141*, 103823. https://doi.org/10.1016/j.cose.2024.103823

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Math Biosci Eng*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Rowe, H. (2003). Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. *Computer Law & Security Review*, *19*(6), 490–496. https://doi.org/10.1016/S0267-3649(03)00609-5

Smolenskij, M. B., & Levshin, N. S. (2016). Localization of personal data of Russian citizens as a component of Russia's economic and national security. *Nauka i obrazovanie: khozyajstvo i ekonomika, predprinimatelstvo, pravo i upravlenie*, *2*(69), 111–114. (In Russ.).

Veseliczky, O. I. (2015). Issues of cross-border transfer of personal data in accordance with the requirements of 242-FZ. *Collections of conferences of the Sotsiosfera SIC*, *53*, 275–279. (In Russ.).

Yan, S., Odom, P., Pasunuri, R., Kersting, K., & Natarajan, S. (2023). Learning with privileged and sensitive information: a gradient-boosting approach. *Frontiers in Artificial Intelligence*, *6*, 1260583. https://doi.org/10.3389/frai.2023.1260583

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610

Authors information



Dmitriy V. Bakhteev – Dr. Sci. (Law), Professor, Department of Criminalistic named after I. F. Gerasimov, Head of Laboratory of Digital Technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: ae@crimlib.info
ORCID ID: https://orcid.org/0000-0002-0869-601X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57208909117
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABA-1494-2020
Google Scholar ID: https://scholar.google.ru/citations?user=h0zOOdcAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=762765



Anna M. Sosnovikova – probation researcher of the Laboratory for digital technologies in Criminalistic, Ural State Law University named after V. F. Yakovlev
Address: 21 Komsomolskaya Str., 620066, Yekaterinburg, Russia
E-mail: at@crimlib.info
ORCID ID: https://orcid.org/0000-0002-1631-9265
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KDP-3525-2024
Google Scholar ID: https://scholar.google.ru/citations?user=BLBhZHMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1196069



Evgeniy V. Kazenas – student, Ural Federal University named after the first President of Russia B. N. Yeltsin
Address: 19 Mira Str., 620002, Yekaterinburg, Russia
E-mail: kazenas03@mail.ru
ORCID ID: https://orcid.org/0009-0002-3301-9720

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 declare no conflict of interest.

Financial disclosure

The research was funded by the grant of the Russian Science Fund No. 23-78-10011, https://rscf.ru/project/23-78-10011/

Thematic rubrics

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

Article history

Date of receipt – June 28, 2024
Date of approval – July 12, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Противодействие кибератакам: пробелы международного права и перспективы их преодоления

Мохаммад Минхазур Рахман ✉

Государственный университет Бангладеш, Дакка, Бангладеш

Тапос Кумар Дас

Джахангирнагарский университет, Дакка, Бангладеш
Городской университет Гонконга, Гонконг

Ключевые слова

кибератака,
киберпреступность,
международная конвенция,
международное право,
права человека,
право,
принцип должной осмотрительности,
принцип соразмерности,
принципы международного права,
цифровые технологии

Аннотация

Цель: категорирование кибератак в национальном и международном правопорядках и определение юридических мер противодействия им на международном уровне.

Методы: представлены доктринальным юридическим анализом, формально-юридическим, сравнительно-правовым методами, синтезом, индукцией, дедукцией, а также методикой правового прогнозирования и моделирования. Исследованию подверглись международно-правовые документы и акты национального законодательства, судебные прецеденты, доктринальные источники.

Результаты: в статье определены юридические последствия кибератак, выявлены трудности определения и привлечения лиц и организаций к ответственности за их совершение, обозначены национальные меры противодействия кибератакам на основе принципа пропорциональности, систематизированы международно-правовые основы реагирования на кибератаки. Основное внимание в работе уделено актуальным проблемам выявления и проверки кибероружия, установления международных стандартов его использования, разработки методов разоружения или ограничения наступательных кибервозможностей. Поставлен вопрос обеспечения гуманитарной деятельности, защиты важнейших объектов инфраструктуры, а также населения с помощью мер кибербезопасности в военное время. Проанализированы правовые основы и выявлены пробелы и иные дефекты действующего регулирования в осуществлении юрисдикции в таких областях кибердеятельности, как международные операции, локализация данных и экстерриториальное исполнение национального законодательства.

✉ Корреспондирующий автор
© Рахман М. М., Дас Т. 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.

Разработаны и описаны параметры, в рамках которых государства вправе проводить упреждающие кибероперации для предотвращения или сдерживания кибератак (киберконтрмеры), основными из которых являются проявление должной осмотрительности, законность принятия решения о применении киберконтрмер, соразмерность защиты от последствий совершения противоправных действий.

Научная новизна: обусловлена представленными в статье прогрессивными решениями в области международно-правового регулирования принятия государствами киберконтрмер в ответ на киберпреступления, сформулированными с учетом влияния обозначенных мер противодействия на права и свободы человека и гражданина, в том числе такие, как право на неприкосновенность частной жизни и свобода слова.

Практическая значимость: результаты проведенного исследования могут быть взяты за основу при разработке и совершенствовании международно-правовых инструментов в области борьбы с кибератаками и обеспечения кибербезопасности, а также могут послужить образцом для национального законодателя при проектировании правотворческих решений противодействия киберпреступлениям.

Для цитирования

Рахман, М. М., Дас, Т. К. (2024). Противодействие кибератакам: пробелы международного права и перспективы их преодоления. *Journal of Digital Technologies and Law*, *2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

Содержание

Введение
1. Проблемы, связанные с легальностью или нелегальностью кибератак
   1.1. Проблема атрибуции кибератак
   1.2. Проблемы подотчетности негосударственных субъектов
   1.3. Императив сотрудничества в отношении кибертерроризма
   1.4. Проблемы прав человека при кибератаках
2. Масштабы и ограничения мер противодействия кибератакам
   2.1. Установление пропорциональности при кибероперациях
   2.2. Препятствия на пути глобального сотрудничества
   2.3. Правовые сложности в области упреждающей самозащиты
3. Инструментализация международного права и институтов для борьбы с кибератаками
   3.1. Преодоление лакун в международных нормах кибербезопасности
   3.2. Необходимость перевода правовых стандартов в киберпространство
   3.3. Неадекватность традиционных принципов ведения войны в киберпространстве
   3.4. Сложности работы вне суверенных границ
Заключение
Список литературы

Введение

Участившиеся кибератаки представляют серьезную угрозу для безопасности государств в современном мире. Страны пытаются понять, как защитить себя от кибератак, а правовые последствия кибернападений и мер противодействия им стали важным объектом изучения. Данное исследование рассматривает многочисленные области международного права, относящиеся к правовым последствиям и проблемам, связанным с различными аспектами контрмер в кибервойне. Основным препятствием для решения указанных проблем является определение лиц или организаций, ответственных за кибератаки (Etzioni & Rice, 2015). Для разработки эффективных контрмер необходима корректная атрибуция кибератак. Однако последняя затруднена из-за природы Интернета, который позволяет сохранять анонимность и применять сложные тактики для сокрытия личности. В данном исследовании рассматриваются существующие правовые основы установления ответственности при атрибуции кибератак в контексте контрмер и предлагаются методы такого установления.

Еще одна важная тема, затронутая в данном исследовании, – соразмерность защиты от кибербоевых действий. Соблюдение соразмерности при оценке масштабов и серьезности контрмер становится еще более важным, когда страны отвечают на кибератаки. Учитывая асимметричный характер кибероперации и широкий сопутствующий ущерб, который они могут нанести, необходимо тщательно изучить правовые нормы для установления соразмерности мер противодействия (Roscini, 2014). Мы рассмотрим существующие правовые стандарты и концепции, а также их актуальность для киберконтрмер. Международное сотрудничество играет крайне важную роль перед лицом все более сложных и транснациональных киберугроз. В данном исследовании рассматриваются правовые структуры и процедуры, способствующие международному сотрудничеству в борьбе с кибератаками. Обмен информацией, координация действий и разработка эффективных мер по противодействию киберугрозам – все это требует сотрудничества между государствами.

В статье рассмотрены также преимущества и недостатки международного сотрудничества в области киберпротиводействия путем изучения существующих международных правовых инструментов и каналов сотрудничества. Хотя главными участниками кибервойн являются государства, растет значимость и других игроков – киберпреступников и организаций хактивистов [хактивист – хакер-активист – лицо, использующее компьютерные сети для распространения той или иной идеологии. – Прим. переводчика] (Buchan, 2012). Поэтому в данном исследовании оцениваются трудности привлечения негосударственных субъектов к ответственности за кибератаки и рассматриваются средства правовой защиты, доступные государствам для реагирования в рамках международного права. При проведении оборонительных или наступательных кибероперациий у государств возникают опасения по поводу возможного нарушения основных прав человека, таких как право на неприкосновенность частной жизни и свободу слова. Чтобы найти баланс между соображениями национальной безопасности и сохранением прав личности, необходимо изучить правовые основы и концепции на стыке регулирования прав человека и использования кибернетических контрмер. Кроме того, в работе анализируются параметры, в рамках которых государства могут законно проводить упреждающие кибероперации для предотвращения или сдерживания кибератак (Hollis & Finnemore, 2016).

В данном исследовании изучаются аспекты упреждающих киберконтрмер путем анализа существующих норм в области упреждающей обороны и их значимости для киберконтрмер. Рассмотрена необходимость должной осмотрительности как критерия подотчетности правительства в рамках киберпротиводействия, а также нормы и обязательства, налагаемые на государства при принятии решений о законности киберпротиводействия. Исследование проливает свет на потенциальные последствия и средства правовой защиты для правительств, участвующих в незаконной кибердеятельности. Мы также затронем такие аспекты, как трудности определения, проверки и регулирования кибероружия, стандарты использования кибероружия в контексте контрмер, а также правовые основы и перспективные процедуры разоружения или ограничения наступательных кибервозможностей (Liivoja & Väljataga, 2021). Кроме того, мы рассмотрим правовые основы, регулирующие разведывательные действия в киберпространстве, границы допустимого шпионажа, диапазон законных государственных интересов и их возможное влияние на международные отношения. Авторы утверждают, что такой подход способствует лучшему пониманию правовых последствий и трудностей сбора киберразведданных (Putman & Albright, 2018).

Кроме того, данное исследование показывает, как гарантии кибербезопасности могут помочь в обеспечении безопасности населения, жизненно важных объектов инфраструктуры и гуманитарной деятельности в военное время. Тем самым оно дает представление о возможных ролях и обязанностях государств и негосударственных субъектов в сохранении киберпространства во время войн путем изучения правовых требований государств и потенциальной взаимосвязи между кибербезопасностью и международным гуманитарным правом. Наконец, в работе рассматриваются трудности и юридические прецеденты, связанные с утверждением юрисдикции в отношении незаконных действий в киберпространстве. Рассматривая юрисдикционные проблемы, возникающие в результате трансграничных кибероперациий, локализации данных и экстерриториального применения национальных законов, это исследование, наконец, рассматривает возможности международного правового сотрудничества (Andrew & Bernard, 2021). Данное исследование направлено на дальнейшее создание правовых рамок и норм, регулирующих контрмеры в кибервойнах, путем изучения этих многочисленных и недостаточно изученных областей международного права, направленных на преодоление трудностей и неясностей, связанных с киберугрозами, и углубление знаний о правовых последствиях этого меняющегося ландшафта (Knowles & Thomas, 2016).

В работе рассмотрены три важных вопроса. Во-первых, исследуется вопрос законности и незаконности кибератак в соответствии с международным правом и международными договорами, а также сравниваются подходы различных юрисдикций и при различных условиях. Во-вторых, изучены существующие правовые рамки и методы, используемые государствами и международными организациями для реагирования на кибератаки и смягчения их последствий, а также определены и изучены потенциальные пределы кибернетического противодействия и стратегий самообороны с точки зрения международного права. В-третьих, учитывая динамичный характер глобальной цифровой экосистемы, в работе изучены пути более эффективного использования или изменения международного права и институтов для решения растущей проблемы кибератак.

Кроме того, в работе затронуты недостаточно исследованные вопросы, связанные с правовыми последствиями киберпротиводействия. Эти вопросы сложны и многомерны, что требует применения всеобъемлющих исследовательских методов. Для тщательного изучения темы в исследовании используются качественные исследовательские методологии и доктринальные подходы. Рассмотрены научные публикации, книги, юридические тексты, материалы прецедентного права и международные правовые документы (Wren & Wren, 1986). Эти источники дают представление о правовых основах, философии и аргументах в отношении различных контрмер в киберпространстве. Юридические последствия контрмер, трудности с установлением виновности и конкретные случаи кибератак будут рассмотрены с помощью тематических исследований. Мы покажем, как различные правовые системы и механизмы международного сотрудничества борются с кибератаками (Van Hoecke, 2011). Для определения актуальной ситуации и возможностей ее улучшения в работе проводится сопоставление ключевых международных договоров, соглашений и подходов к сотрудничеству, принятых на сегодняшний день. Чтобы прояснить правовые стандарты, нормы и принципы, регулирующие компоненты кибернетических контрмер, авторы изучают доктрину международно-правовых инструментов, таких как международные договоры, международное обычное право и соответствующие правовые принципы (Watkins & Burton, 2013).

Чтобы ответить на поставленные вопросы, также необходимы интерпретация и применение правовых норм и прецедентов. Исследование фокусируется на трудностях и юридических последствиях разработки мер реагирования на кибератаки. Основными ограничениями исследования выступает неполнота знаний и опыта авторов в этой постоянно развивающейся области (Tyler, 2017). Несмотря на это, можно ожидать, что работа значительно расширит знания о правовых последствиях и трудностях противодействия кибервойнам.

1. Проблемы, связанные с легальностью или нелегальностью кибератак

1.1. Проблема атрибуции кибератак

Поскольку кибератаки часто не оставляют после себя доказательств, установление виновности в таких преступлениях является сложной и долгосрочной операцией (Tsagourias & Farrell, 2020). Первым ее этапом будет определение источника кибератаки. По словам Michael Schmitt (2013), установление виновности в кибератаках связано с трудностями. Ответственность за кибератаки не может определяться правовой системой. Однако существует множество правовых и инновационных подходов, помогающих в установлении виновности при кибератаках. Внедрение этих моделей и процедур позволит государствам более эффективно бороться с киберугрозами. По мнению Michael Schmitt, установить ответственность в случае кибератаки сложно из-за отсутствия единой правовой базы. Однако использование инновационных правовых подходов и методов повышает возможности стран по выявлению кибератак и разработке эффективных контрмер (Schmitt, 2013). Таким образом, в настоящее время существуют юридические инструменты, которые могут помочь в установлении виновности в случае чрезвычайных ситуаций в киберпространстве. James A. Lewis утверждает, что выявление лиц, совершивших

кибератаку, является важным первым шагом в реагировании на катастрофические события в киберпространстве. Если виновные не установлены, принятие надлежащих юридических, дипломатических или военных мер затруднительно. Анонимность Интернета и трудности с получением доказательств затрудняют установление тех, кто стоит за кибератаками. Тем не менее существует несколько вариантов решения проблемы идентификации. Это методы и ресурсы, с помощью которых государство может усилить свою защиту от киберугроз (Lewis, 2018). Это говорит о том, что, несмотря на трудности, существуют эффективные подходы к улучшению процессов атрибуции.

Аналогичным образом, в работе Gabriella Blum (Wittes & Blum, 2016) подчеркивается, что установление виновности в кибератаках является важным аспектом международного права. Сложно привлечь государство к ответственности за поведение в киберпространстве без установления виновности. Принципы ответственности государства, должной осмотрительности и соразмерности – это лишь некоторые из правовых рамок, которые используются для решения проблемы атрибуции атак через Интернет. Однако эти модели сложно применить на практике, так как для этого требуются более четкое формулирование и согласование правовых принципов определения виновных в кибератаках. Blum подчеркивает необходимость привлечения государств к ответственности за свои действия в киберпространстве и важность атрибуции с точки зрения международного права. Среди обсуждаемых ею правовых принципов, которые могут быть применены для установления виновности в кибератаках, – принципы ответственности государства, должной осмотрительности и пропорциональности (Wittes & Blum, 2016). Blum также признает сложность и реальные проблемы внедрения этих систем. Она подчеркивает важность более четкого определения и согласования правовых норм, регулирующих атрибуцию. Установление виновности имеет далеко идущие юридические последствия. Если одна страна докажет, что другая несет ответственность за кибератаку, то может подать на страну-нарушительницу в суд. Но государство не сможет предпринять юридические действия в случае кибератаки, если не определит, кто несет за нее ответственность (Ohlin et al., 2015).

Существуют и другие инновационные методы атрибуции кибератак в дополнение к существующим правовым рамкам. Киберкриминалистика занимается сбором и анализом цифровых доказательств, оставленных в результате кибератак. Эти данные могут быть использованы для установления лиц, совершивших кибероперации. Выявлению виновных в кибератаках способствует международное сотрудничество в области обмена информацией и ресурсами между государствами. В расследовании кибератак используется также сотрудничество государственного и частного секторов. Так, данные о кибератаках, полученные от частных лиц, могут быть переданы правительственным учреждениям и затем использованы для лучшего понимания и выявления киберугроз (Klimburg, 2018). Поскольку атрибуция кибератак является сложной и запутанной проблемой, нельзя полагаться на национальные правовые системы при установлении ответственности за них. Однако для установления виновности может быть использован ряд правовых рамок и нестандартных методов. Внедрение этих механизмов и методов позволит государствам эффективнее реагировать на киберугрозы.

1.2. Проблемы подотчетности негосударственных субъектов

Негосударственные организации, уклоняющиеся от ответственности за кибератаки, представляют значительные трудности для современного международного права. Юристы-международники отмечают трудности в судебном преследовании негосударственных субъектов за кибератаки. Однако в рамках международного права правительства располагают рядом юридических инструментов для реагирования на такие атаки. Среди жизнеспособных решений назовем подотчетность правительств, правовые контрмеры, целевые кибероперации и международное сотрудничество (Buchanan, 2017). Для выполнения своих международно-правовых обязательств государства должны тщательно продумывать законность и соразмерность своих действий.

Как отмечает Michael N. Schmitt (1999), кибероперации, осуществляемые негосударственными субъектами, подчиняются тем же традиционным нормам международного права, что и те, которые осуществляются государствами, а именно подотчетность государства и недопущение вмешательства. Schmitt подчеркивает, что обычные нормы международного права применимы и к негосударственным организациям, участвующим в кибератаках. Государство также может быть привлечено к ответственности за действия негосударственного субъекта, согласно принципу ответственности государства. Если негосударственные субъекты проводят кибероперации с территории одного государства против другого, также может применяться запрет на их участие. По мнению этого автора, одним из самых больших препятствий для привлечения негосударственных субъектов к ответственности за их действия является отсутствие четкой правовой базы, регулирующей атрибуцию кибератак негосударственным субъектам. Чтобы гарантировать законность и эффективность своих действий, государства должны сотрудничать в достижении общего понимания правовых стандартов, регулирующих кибероперации (Schmitt, 1999). Michael Schmitt обращает внимание на отсутствие четкой правовой базы и сложность установления причастности негосударственных субъектов к кибератакам. Термин «атрибуция» означает процедуру точного определения источника кибератаки. Трудно привлечь негосударственные структуры к ответственности за их поведение в отсутствие четко определенной правовой базы. Schmitt утверждает, что правительства должны сотрудничать в целях установления единых правовых норм в сфере кибердеятельности. Меры реагирования государств на киберугрозы могут быть успешными и законными, только если они основаны на общем понимании проблемы.

Таллиннское руководство 2.0 также предполагает, что законные меры, доступные государствам для борьбы с кибератаками, осуществляемыми негосударственными субъектами, включают дипломатические, экономические и юридические санкции. Согласно Таллиннскому руководству 2.0, правительства обладают широким спектром возможностей для реагирования на кибератаки со стороны негосударственных субъектов. Эти формы реагирования могут быть дипломатическими, экономическими или даже юридическими по своей природе, в зависимости от характера и обстоятельств правонарушения. Подобным же образом, как пишет Matthew C. Waxman, целенаправленные кибероперации применяются государствами против негосударственных субъектов, чтобы воспрепятствовать их деятельности, ослабить возможности и заставить их заплатить за свои атаки. По мнению этого автора, государства могут использовать целенаправленные кибероперации для пресечения операций и ресурсов негосударственных организаций, совершающих враждебные действия.

Также для предотвращения будущих кибератак на злоумышленников могут быть наложены штрафные санкции (Waxman, 2011). Однако для оценки законности и соразмерности таких мер следует руководствоваться нормами международного права.

1.3. Императив сотрудничества в отношении кибертерроризма

Согласно резолюции 71/256 Генеральной Ассамблеи ООН, государства должны работать сообща для обеспечения того, чтобы все усилия по предотвращению и ликвидации угрозы кибертерроризма были законными в соответствии со всеми применимыми международными договорами. В резолюции, принятой Генеральной Ассамблеей, также подчеркивается важность совместной работы правительств в борьбе с терроризмом, особенно кибертерроризмом, при соблюдении ими соответствующих обязательств по международному праву (Mačák, 2016). Поэтому, реагируя на кибератаки со стороны негосударственных субъектов, страны должны думать о международных правовых рамках. По словам Gabriella Blum, при любых попытках привлечь к ответственности негосударственные структуры отсутствие сотрудничества со стороны других стран является фундаментальной проблемой, которую необходимо решать. Эффективность мер реагирования государств зависит от их совместной работы по созданию механизмов сотрудничества. Gabriella Blum утверждает, что попыткам привлечь негосударственные структуры к ответственности за кибератаки препятствует отсутствие сотрудничества со стороны других стран. При борьбе с киберугрозами, исходящими от негосударственных субъектов, сотрудничество между правительствами имеет важное значение для сбора и совместного использования информации, обмена знаниями и координации операций. Blum утверждает, что для эффективного реагирования на киберугрозы странам необходимо создавать структуры для сотрудничества (Lewis et al., 2019). Примерами таких систем являются соглашения об обмене данными, проведении совместных исследований и координации ответных мер. Способность государств реагировать на негосударственные субъекты, участвующие в кибератаках, повышается за счет сотрудничества. Как обсуждалось выше, атрибуция кибератак негосударственным субъектам не регулируется какими-либо четкими международно-правовыми рамками. Эта двусмысленность усложняет задачу правительств по привлечению негосударственных субъектов к ответственности за их действия. Поскольку действия негосударственных субъектов сложно отследить и идентифицировать, принятие государствами мер против них затруднено, даже если негосударственные субъекты действительно причастны к нападению.

По ряду причин, включая политические соображения и опасения за последствия, страны не всегда сотрудничают с другими государствами в расследовании и наказании негосударственных субъектов. Невозможность совместной работы может затруднить привлечение негосударственных субъектов к ответственности. Несмотря на трудности, страны могут прибегать к правовым средствам при реагировании на кибератаки со стороны негосударственных субъектов. Проблема с негосударственным субъектом или государством, которое подозревается в укрывательстве негосударственного субъекта, может быть решена соответствующим государством с помощью дипломатических методов (Mazanec, 2015). Экономические санкции могут быть введены государствами как в отношении негосударственного субъекта, так и в отношении государства, которое предположительно предоставляет убежище

негосударственному субъекту. В ответ на кибератаки со стороны негосударственных субъектов государства могут прибегнуть к военным действиям. Однако этот выбор следует делать только тогда, когда все другие варианты будут исчерпаны, поскольку это может иметь серьезные последствия, включая эскалацию агрессии.

1.4. Проблемы прав человека при кибератаках

Кибератаки также могут негативно сказаться на правах человека, поскольку используются для самых разных целей, включая несанкционированный сбор данных, цензуру высказываний и сбои в работе систем. Последствия этого особенно существенны для таких категорий, как журналисты, активисты и представители маргинализированных сообществ. В контексте кибернетических мер противодействия существует ряд правовых механизмов, которые контролируют баланс между целями национальной безопасности и соблюдением прав человека (Kulesza & Balleste, 2015). Право на неприкосновенность частной жизни и возможность самовыражения – это лишь два из множества прав, гарантированных на международном уровне. Государства должны поддерживать эти свободы хотя бы в интересах национальной безопасности. Все вооруженные конфликты регулируются правом в области вооруженных конфликтов, также известным как международное гуманитарное право. Оно регулирует применение физических и виртуальных средств поражения. На национальном уровне может быть обеспечена более строгая защита прав человека; при определенных условиях предусмотрено ограничение применения контрмер в киберпространстве. Государства могут принимать различные меры, чтобы гарантировать соответствие своей деятельности в киберпространстве универсальным принципам прав человека. Право на неприкосновенность частной жизни и свободу слова – это два фундаментальных права, которые государства должны соблюдать при принятии контрмер в киберпространстве.

Принимаемые государствами кибернетические контрмеры должны соответствовать серьезности киберугрозы. Государства могут использовать любые кибернетические контрмеры, которые они считают подходящими для достижения этой цели (Watt, 2021). Применяя кибернетические контрмеры против любых государственных или негосударственных субъектов, государства должны принимать все возможные меры безопасности, чтобы гарантировать, что не пострадают гражданские лица или гражданское имущество. Любой ущерб, причиненный действиями государства в киберпространстве, должен быть компенсирован. В специальном докладе Совета ООН по правам человека по вопросу о поощрении и защите права на свободу мнений и их свободное выражение отмечалось, что права человека должны учитываться при разработке и внедрении политики и процедур кибербезопасности. В нем подчеркивалась необходимость соблюдения стандартов в области прав человека при осуществлении мер кибербезопасности и противодействия им. Меры должны быть законными, необходимыми, соразмерными и недискриминационными; они не должны выделять или дискриминировать каких-либо конкретных лиц или группы. Так, в деле Delfi AS v. Estonia ЕСПЧ неоднократно указывал, что право на свободное распространение и обсуждение любых идей, независимо от того, насколько они популярны или считаются неприемлемыми, является краеугольным камнем демократического общества. Это судебное дело показывает важность свободы слова в демократическом обществе (Wagner et al., 2019). В нем подчеркивается, что эта

свобода относится не только к общепринятой, но и потенциально спорной информации и мнениям. Поэтому, даже имея дело со спорными материалами, службы кибербезопасности должны обеспечить защиту этого права.

Кроме того, ст. 19 Международного пакта о гражданских и политических правах гласит, что каждый человек имеет право выражать свое мнение любым способом, который он считает нужным, будь то устно, письменно или печатно, средствами искусства или любыми другими средствами по своему выбору; это включает свободу искать, получать и распространять информацию и идеи любого характера, независимо от любых границ. Это положение закона подчеркивает широкий характер указанного права, включая в себя свободу доступа, потребления и распространения информации и идей любыми средствами массовой информации. Свобода выражения мнений и информации в цифровой сфере должна быть защищена от посягательств со стороны государств. Чтобы обеспечить проведение кибероперации в соответствии с международными нормами в области прав человека, требуется четкая и всеобъемлющая законодательная база (Mihr, 2017). Важное значение имеют такие аспекты этой системы, как подотчетность, мониторинг и судебный надзор. Прежде чем начинать какие-либо операции в киберпространстве, государства должны сначала провести всестороннюю оценку их воздействия на права человека. Они должны проанализировать, как ограничения повлияют на такие права, как неприкосновенность частной жизни и свобода слова, и убедиться, что эти ограничения не являются более жесткими, чем это абсолютно необходимо для достижения законных целей. Необходимо предусмотреть соблюдение надлежащих процессуальных норм, эффективные средства правовой защиты в случае предполагаемых нарушений, а также независимые и открытые методы надзора. Не ставя под угрозу законные интересы безопасности, государства должны информировать общественность о целях, масштабах и последствиях кибердеятельности, чтобы способствовать открытости и подотчетности. Им необходимо сотрудничать в глобальном масштабе для разработки руководящих принципов защиты прав человека в Интернете (Mihr, 2016). Созданию всеобъемлющих норм и предписаний способствует совместная работа с правительствами других стран, международными организациями и широкой общественностью. Государства могут найти баланс между правами человека и решением проблем национальной безопасности, обеспечив соответствие своей деятельности в киберпространстве международным нормам в области прав человека.

2. Масштабы и ограничения мер противодействия кибератакам

2.1. Установление пропорциональности при кибероперациях

Одним из краеугольных камней международного права является концепция пропорциональности, которая запрещает применение силы, несоразмерной серьезности угроз. К кибероперациям применяется то же правило, что и к любому другому виду военных действий. Соразмерность контрмеры должна оцениваться в свете специфики атаки, которую она призвана отразить. Ответная тактика, которая наносит больший ущерб, чем при первом нападении, скорее всего, будет считаться непропорциональной. Контрмера должна быть именно такой, какая необходима для предотвращения кибератаки. Непропорциональный ответ – это такой, который выходит за рамки того, что требуется для прекращения атаки. Контрмера не должна создавать больше проблем, чем решает. Если негативные последствия

контрмеры несоразмерны выгодам, то контрмера несправедлива. Применение идеи пропорциональности к кибероперациям может оказаться сложной задачей из-за уникального характера кибердеятельности (Dwan et al., 2022). Например, кибердеятельность может иметь непредвиденные последствия, и ее очень трудно отследить. Кибероперации создают уникальный набор проблем, когда речь заходит об определении соразмерности контрмер, что требует учета специфических особенностей кибератак и их последствий для концепции соразмерности. Актуальность современных принципов пропорциональности для кибероперацій нашла отражение в трудах многих ученых в области международного права. Так, по словам Michael N. Schmitt, чтобы соответствовать стандарту пропорциональности, государства должны оценить потенциальный сопутствующий ущерб гражданским объектам и сопоставлять его с потенциальным военным преимуществом. Этот автор подчеркивает необходимость сопоставления военного преимущества, получаемого в результате кибероперацій, с прогнозируемым ущербом гражданским объектам. Кибератаки подпадают под эту концепцию пропорциональности, согласно которой правительства должны сопоставлять возможную военную выгоду с любым сопутствующим ущербом гражданской инфраструктуре, таким как критически важные системы или службы (Schmitt, 2012a).

Согласно Таллиннскому руководству 2.0 по международному праву в области кибероперацій, те кибероперации, которые наносят серьезный ущерб основной инфраструктуре или приводят к человеческим жертвам, могут рассматриваться как акт войны. Следовательно, при оценке потенциальных результатов таких кибероперацій необходимо использовать критерий пропорциональности. Ущерб критической инфраструктуре, гибель или ранения людей – все это признаки того, что кибероперация переросла в военный акт. Аналогичным образом, по словам Marco Roscini (2014), государство – участник конфликта не должно предпринимать кибератаку на гражданский объект, если прогнозируемый ущерб гражданскому населению или случайные повреждения будут несоразмерны ожидаемому военному преимуществу в соответствии с принципом пропорциональности. Этот автор подчеркивает важность ограничения последствий кибератак для невинных людей. При проведении кибероперации прогнозируемый ущерб гражданским объектам или лицам не должен превышать прогнозируемый военный выигрыш. Эта идея также актуальна в сфере кибервойн (Roscini, 2014). Также, по словам Christopher C. Joyner (2011), кибервойны должны регулироваться концепцией пропорциональности, которая гласит, что ответ участника боевых действий должен быть соизмерим с опасностью, исходящей от вооруженных сил противника. По словам этого автора, применение силы в кибервойне должно быть ограничено необходимостью и соизмеримо с опасностью, которую представляют военные возможности государства-мишени. Это означает, что кибероперации не должны наносить больше ущерба, чем это абсолютно необходимо для устранения текущей угрозы.

По мнению ученых (Frowe, 2022), пропорциональность в кибероперациях определяется путем оценки прогнозируемого военного преимущества по сравнению с ожидаемым ущербом гражданским объектам. Кибератаки отличаются от других видов атак и должны тщательно рассматриваться в контексте соразмерности из-за их потенциальной возможности нанести ущерб ключевой инфраструктуре или гражданскому населению. Уместность и законность кибероперацій в свете возможных последствий можно оценить, используя действующие правовые нормы и принципы,

относящиеся к категории соразмерности в вооруженных столкновениях. Кибератаки могут осуществляться государствами, располагающими гораздо меньшими ресурсами, чем у их целей. Возможности злоумышленника могут быть неизвестны или их трудно предсказать, что затрудняет определение того, являются ли контрмеры соразмерными или нет. Таким образом, две отличительные черты кибероперaций – сложность и непредсказуемость (Schmitt, 2011).

Из-за сложности прогнозирования всех возможных последствий может быть трудно определить, являются ли контрмеры соразмерными. Выявить источник кибератак также непросто, поскольку они могут быть предприняты откуда угодно. Это затрудняет определение цели для принятия контрмер. Кибератаки сложно оценить с точки зрения их масштаба и серьезности. Они могут нанести большой ущерб, но его степень трудно определить из-за их анонимности и сложности. Это затрудняет оценку адекватности ответных мер по отношению к серьезности атаки. Обоснование контрмер в киберпространстве является еще более сложной задачей. При большом количестве потенциальных способов реагирования на киберугрозы такое решение оказывается непростой задачей. Существует вероятность того, что при определенных обстоятельствах ответные действия окажутся чрезмерными. Прогнозирование потенциальных результатов контрмер в киберпространстве может быть затруднено.

2.2. Препятствия на пути глобального сотрудничества

Существует множество препятствий, которые мешают государствам совместно разрабатывать законные меры противодействия кибератакам. Деятельность в киберпространстве не регулируется каким-либо общепризнанным сводом законов. Эта неопределенность препятствует сотрудничеству государств в разработке эффективных мер противодействия. Атрибутировать кибератаку конкретному злоумышленнику часто бывает непросто. Поскольку страны не всегда уверены в том, на кого нацелена кибератака, это усложняет реагирование на такие удары (Friis & Ringsmose, 2016). Кибератаки могут иметь самые разнообразные преднамеренные и непредвиденные последствия. Однако сотрудничество государств для создания законной и эффективной киберзащиты имеет важное значение. Эксперты в области права указывают как на трудности, так и на возможные решения. Например, по словам Duncan Hollis (Hollis & Finnemore, 2016), взаимосвязь кибератак и уязвимостей требует международного сотрудничества для выработки решения, поскольку ни одно государство не может успешно справиться с этим в одиночку. Автор отмечает, что ни одно государство не может адекватно противостоять киберугрозам в одиночку, и указывает на взаимосвязанность, лежащую в основе киберпространства. Это подчеркивает необходимость совместной работы государств по обмену информацией, навыками и ресурсами для укрепления своей киберзащиты.

По мнению Christopher S. Yoo, затраты на сбор информации, координацию и обеспечение соблюдения норм могут быть снижены, а успешность мер кибербезопасности повышена за счет широкого распространения соответствующих данных от имени государств. Исследователь подчеркивает необходимость обмена информацией в области кибербезопасности между государствами. Это обеспечит кибербезопасность при одновременном сокращении расходов, связанных со сбором и координацией данных. Более эффективная защита от кибератак может быть достигнута за счет обмена информацией об угрозах, передовым опытом

и техническими навыками (Yoo & Blanchette, 2015). Международная стратегия США в отношении киберпространства предусматривает, что вместе с другими странами Соединенные Штаты будут укреплять киберстандарты, основанные на уважении прав человека, и стремиться снизить вероятность конфликтов, вызванных распространением и использованием информационно-коммуникационных технологий. Документ подчеркивает важность совместных усилий разных стран по распространению передовых практик в области кибербезопасности и поощрению ответственного поведения. Работая сообща, страны смогут создавать и внедрять стандарты и руководящие принципы для защиты прав человека, а также сделать Интернет более безопасным для всех.

Таллиннское руководство 2.0 предлагает такой же подход, отмечая, что соглашения о киберзащите между государствами могут содержать конкретные шаги по сотрудничеству, предпринимаемые для оказания помощи друг другу в случае кибератаки. Что касается кибернетических мер противодействия, то в Таллиннском руководстве 2.0 также рекомендуются двусторонние соглашения между странами. Такие соглашения служат основой для обмена информацией и ресурсами в случае кибернетического кризиса или кибератаки. Это укрепляет взаимное доверие и повышает эффективность реализации инициатив в области кибербезопасности (Tsagourias, 2012). Кроме того, согласно рекомендации Группы правительственных экспертов ООН (далее – ГПЭ ООН) по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, для повышения способности всех стран предотвращать, расследовать, реагировать на инциденты, связанные с ИКТ, и восстанавливаться после них государства должны сотрудничать в разработке и осуществлении мер по наращиванию потенциала, включая взаимопомощь и сотрудничество. Сотрудничеству и координации между странами в значительной степени способствуют международные организации, такие как Организация Объединенных Наций (Henriksen, 2019).

Специалисты в области международного права отмечают преимущества и недостатки международного сотрудничества в разработке законных и эффективных средств защиты от киберугроз. Взаимосвязанность киберпространства требует от государств совместной работы, обмена данными и повышения их коллективной готовности. Многосторонние институты, такие как Организация Объединенных Наций, способствуют координации усилий и оказывают содействие в разработке стандартов и программ по наращиванию потенциала, тогда как двусторонние соглашения определяют конкретные шаги к сотрудничеству. Действуя совместно, государства укрепляют свои возможности в области кибербезопасности и могут реагировать на кибератаки, используя эти инструменты. Несмотря на имеющиеся сложности, существует ряд возможностей для международного сотрудничества в создании законных, но эффективных средств киберзащиты (Katagiri, 2021). Международные организации, такие как Организация Объединенных Наций, развивают сотрудничество между правительствами в целях разработки эффективных контрмер. Эти группы могут служить платформой для совместной разработки стратегий противодействия киберугрозам. Двусторонние соглашения между правительствами также помогают разработке эффективных мер противодействия. Эти соглашения служат основой для координации действий правительств в ответ на киберугрозы и обмена информацией о них.

Глобальный центр обмена информацией и анализа (Global Information Sharing and Analysis Centre, GISAC) – еще одна структура, которая способствует сотрудничеству между правительствами в целях выработки более эффективных ответных мер (Faga, 2017). Эти инструменты позволяют странам координировать свои действия в ответ на киберугрозы и обмениваться информацией о них. Существуют значительные препятствия для международного сотрудничества в разработке эффективных и правовых средств защиты от киберугроз. С другой стороны, существует также множество способов, позволяющих работать вместе для общего блага. Кибербезопасность – это общая ответственность, и сотрудничество между государствами должно приводить к принятию более эффективных мер защиты.

2.3. Правовые сложности в области упреждающей самозащиты

Превентивные кибероперации, проводимые странами для предотвращения или сдерживания возможных кибератак, являются предметом постоянных дискуссий, равно как и условия, при которых такие операции могут проводиться на законных основаниях. Существующие конвенции и правовые рамки, касающиеся упреждающей самообороны, не всегда применимы к кибератакам, и по этому вопросу нет достаточного согласия. Устав ООН, решение Международного суда по делу Никарагуа и обычное международное право являются наиболее важными нормами и правовыми рамками, относящимися к упреждающей самообороне (Dean, 2013). Применение силы против суверенитета или территориальной целостности государства прямо запрещено Уставом Организации Объединенных Наций. Напротив, ст. 51 Устава ООН разрешает государствам применять силу в целях самообороны. В деле Никарагуа международный суд постановил, что лицо имеет право применить силу в целях самообороны, даже если нападение еще не произошло. Тем не менее Международный суд подчеркнул, что риск нападения должен быть немедленным, всеобъемлющим и не оставляющим выбора средств и времени для обдумывания. Право на самооборону также признается международным обычным правом, которое содержит рекомендации в ситуациях самообороны, хотя их содержание не всегда очевидно. Некоторые юристы считают, что государства должны использовать все доступные дипломатические пути для урегулирования конфликта, прежде чем прибегать к силе. Однако другие утверждают, что правительства имеют право применять силу в целях самообороны перед лицом нападения, даже если дипломатические решения конфликта все еще возможны.

Продолжается дискуссия о том, применимы ли действующие нормы и правовые рамки, касающиеся упреждающей самообороны, при кибератаках (Lucas, 2016). Мнения экспертов о том, можно ли применять концепции самообороны в киберпространстве, разделились из-за особого характера кибератак. Сложность определения причин атак является основным препятствием для разработки стратегий самообороны в киберпространстве. В реальном мире установить личность преступника, совершившего нападение, обычно не составляет особого труда, однако отследить источник нападения в киберпространстве может быть непросто. Это снижает способность государств оценивать угрозы и осуществлять право на самооборону. Еще одна проблема, связанная с переносом традиционных концепций самообороны в киберпространство, заключается в определении того, насколько близка угроза нападения. В реальном мире обычно легко определить, произойдет ли нападение в ближайшее время. Однако оценить непосредственную угрозу нападения в киберпространстве

может быть непросто. Это усложняет для правительств вопрос о том, имеют ли они право осуществлять самооборону перед лицом неминуемой угрозы (Levite & Perkovich, 2017).

Превентивные кибероперации, при которых государство активно предпринимает действия, чтобы остановить или пресечь атаку, являются спорной темой для обсуждения среди экспертов. Существующие нормы и правовые рамки, касающиеся упреждающей самообороны, не всегда очевидны или уместны в киберпространстве, и по этому вопросу нет четкого консенсуса. Согласно решению по делу Nicaragua v. United States of America (1986), принятому Международным судом, в случае вторжения или другого вооруженного нападения каждое суверенное государство имеет право применить военные действия для защиты своей территории. Это подтверждает неотъемлемое право на самооборону. Международный суд постановил, что право на самооборону включает в себя способность принимать меры перед лицом непосредственной угрозы насилия (Travis, 2016), а также что действия по самообороне, включая применение силы, должны быть обоснованы.

По словам Michael Schmitt, чтобы применение силы в целях упреждающей самообороны было оправданным, оно должно быть необходимым, соразмерным и применяться в ответ на неминуемое незаконное вооруженное нападение. Ученый предполагает, что упреждающая самооборона оправдана только в тех случаях, когда применение силы необходимо и уместно, угроза вооруженного нападения неизбежна и законных альтернатив применению силы нет[1]. Аналогичным образом, Bruce Schneier утверждает, что государства должны избегать участия в упреждающих кибероперациях, поскольку они потенциально разрушительны и непредсказуемы. Странам будет сложнее работать сообща над решением проблем кибербезопасности, если эта напряженность усилится. Ученый считает, что превентивные кибероперации приведут к обострению споров и затруднят совместную работу стран по устранению угроз кибербезопасности (Schneier, 2013). В целом эти мнения юристов-международников подчеркивают, что ситуация с превентивными кибероперациями неоднозначна и законодательство в этой области все еще находится в стадии разработки. Единодушного мнения по этому вопросу нет. Однако ученые-юристы считают, что важнейшими критериями легитимности превентивных кибероперациий являются следующие: неизбежность угрозы, необходимость применения силы, пропорциональность применения силы и различие между комбатантами и гражданскими лицами.

Опасности и выгоды от проведения превентивных кибероперациий должны сопоставляться с этими правовыми ограничениями. Превентивные кибератаки чреваты разжиганием более масштабной войны (Ossoff, 2021). Они могут иметь тяжелые последствия, если нанесут ущерб международным связям и затруднят совместную работу правительств в области кибербезопасности. Ситуация с превентивными кибероперациями сложна, и выбор в пользу их применения должен приниматься в каждом конкретном случае. Правовые, стратегические и политические последствия таких операций должны тщательно рассматриваться государствами до их проведения.

---

[1] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

3. Инструментализация международного права и институтов для борьбы с кибератаками

3.1. Преодоление лакун в международных нормах кибербезопасности

Существующие международные организации пока не в состоянии справиться со сложностью и динамичностью киберугроз. Примером является ситуация с ГПЭ ООН. Усилиям ГПЭ по созданию добровольных нормативных рамок препятствует тот факт, что они основаны на консенсусе. Это замедляет их разработку и иногда приводит к тупиковым ситуациям в результате конкурирующих национальных интересов и геополитических конфликтов. Еще одной серьезной проблемой является неспособность существующего международного права выносить решения и применять санкции в отношении правительств, которые совершают кибератаки или содействуют им. Поскольку существующие процедуры обеспечения соблюдения основаны преимущественно на традиционных представлениях о военных действиях, имеются лакуны в институциональной защите государств, которые проводят враждебные кибероперации. Это подчеркивает необходимость в новой международной конвенции, которая более точно определяла бы незаконные действия в киберпространстве и обеспечивала эффективные механизмы судебного разбирательства и правоприменения. В связи с постоянно развивающимся характером технологий также требуется разработать новую международную конвенцию.

Современные технологические достижения опережают возможности существующего международного права и институтов по эффективному реагированию. Например, появление квантовых вычислений и кибератак, управляемых искусственным интеллектом, порождает новые проблемы, которые еще не учтены существующими системами. Конвенция, ориентированная на будущее, может принести пользу, если будет изначально разработана с учетом возможностей адаптации и гибкости, роста и развития параллельно с развитием технологий. Более того, идея глобального сотрудничества подчеркивает важность разработки новой международной конвенции (Gow et al., 2019). Кибербезопасность – это международная проблема, требующая согласованных усилий. Различные национальные интересы и отсутствие доверия между странами мешают существующим международным организациям наладить активное глобальное сотрудничество. Развитию сотрудничества, укреплению доверия и обеспечению коллективной кибербезопасности могут способствовать согласованные на глобальном уровне рамки, предусмотренные международной конвенцией. Отрадно, что существующие международные организации пытаются решить проблему кибератак. Однако из-за постоянно меняющегося характера киберугроз и ограничений существующих международных правовых и институциональных рамок реакция на эти риски до сих пор не была адекватной. Новая международная конвенция, направленная на противодействие киберугрозам, имеет большие перспективы. Эта система может стать прозрачной, всеобъемлющей и гибкой, чтобы способствовать международному сотрудничеству, определять преступные деяния и устанавливать процедуры правоприменения.

Принятие такой конвенции стало бы важным шагом на пути к более надежному и безопасному Интернету. Что касается урегулирования споров и толкования международного права, Международный суд ООН и другие международные судебные органы находятся в авангарде (Harrison Dinniss, 2012). Однако существует ряд

проблем, снижающих их эффективность и применимость в борьбе с кибератаками. Международный суд должен обладать юрисдикцией в отношении того или иного вопроса, чтобы выносить по нему решение, и это обычно достигается при сотрудничестве правительств участвующих стран. Однако установить причастных к кибератакам людей и заручиться согласием соответствующих государств довольно сложно, поскольку происхождение этих лиц часто неизвестно и они могут действовать из разных юрисдикций. При вынесении своих решений Международный суд и другие аналогичные суды часто ссылаются на прецеденты и устоявшиеся принципы международного права. Поскольку военные действия в киберпространстве еще находятся в зачаточном состоянии, ориентирами могут служить лишь несколько примеров. Учитывая сложность и новизну этой ситуации, суд может испытывать сложности с применением существующих правовых норм (Bucci, 2018).

Рассмотрение дел в международных судах может занимать годы из-за сложности соответствующего законодательства. Однако кибератаки происходят с головокружительной скоростью и требуют быстрого реагирования. Судебной системе трудно адекватно разрешать киберконфликты из-за несоответствия между темпами судебных разбирательств и быстро развивающимся киберпространством. Нет единого мнения о том, как следует толковать суверенитет, невмешательство и применение силы в соответствии с традиционным международным правом в контексте кибероперациий. В 2018 г. генеральный прокурор Великобритании Джереми Райт выступил с лекцией, в которой утверждал, что киберинфраструктура страны должна рассматриваться как часть ее суверенной территории[2]. Из-за этих несоответствий международные суды иногда выносят решения, противоречащие друг другу. Устав Организации Объединенных Наций, Женевские конвенции и некоторые другие нормативные документы, не имеющие обязательной силы, составляют в международном праве основу для определения допустимости действий. Проблемы атрибуции, причинения нефизического вреда и подотчетности правительства в киберпространстве нелегко решить с помощью этих законов, поскольку они были написаны задолго до появления Интернета. Например, легкость совершения кибератак затрудняет их отслеживание до государственного субъекта в случае их осуществления. Юридическая оценка таких операций еще более осложняется отсутствием ясности в отношении того, что представляет собой «вооруженное нападение» в киберпространстве.

Принятие новой Международной конвенции позволит ввести четкие определения, стандарты и нормы, адаптированные к цифровой среде (Nissenbaum, 2015). Существующие правовые рамки представляют собой серьезные препятствия для принятия мер противодействия кибератакам. Остается спорным вопрос о том, имеют ли правительства право на самооборону от кибератак в соответствии со ст. 51 Устава Организации Объединенных Наций. В отличие от традиционных боевых действий, нет единого мнения о том, являются ли такие действия в киберпространстве необходимыми или соразмерными (Cornish, 2021). Новая международная конвенция сделает возможным установление более четких стандартов для принятия контрмер, включая характерные для киберпространства концепции пропорциональности, необходимости и дифференциации. Организация Объединенных Наций

[2] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

и другие международные организации предприняли ряд важных шагов в борьбе с киберпреступностью. Однако они не всегда успешны из-за таких факторов, как противоречащие друг другу законы и вопросы юрисдикции. Чтобы должным образом противостоять кибератакам, необходимо использовать международное право и институты. Однако для этого потребуются масштабные изменения, чтобы адаптироваться к постоянно меняющемуся характеру киберугроз и справиться с вызовами, возникающими в цифровой сфере. Частоту и серьезность кибератак можно снизить путем принятия новых международных конвенций, которые бы определяли, стандартизировали и обеспечивали применение контрмер.

3.2. Необходимость перевода правовых стандартов в киберпространство

Из-за нетрадиционного характера кибероперациий к кибератакам и кибернетическим контрмерам может быть сложно применить традиционные правовые стандарты, такие как различение, соразмерность и военная необходимость. Например, к комбатантам и гражданским лицам следует относиться по-разному, и в соответствии с концепцией различения следует атаковать только военные объекты. Из-за анонимности и идентификации, присущих киберпространству, определение источника и типа атаки является основной проблемой в кибервойнах. Проведение различий в киберпространстве сопряжено с серьезными трудностями из-за дублирования военных и гражданских компьютерных систем, сетей и инфраструктуры. Также, согласно концепции пропорциональности, атака может быть предпринята только в том случае, если ожидаемое военное преимущество оправдывает риск для населения и гражданской инфраструктуры. В условиях кибервойны сложно точно оценить возможные последствия атаки и сопутствующий ущерб, который она может нанести. Непредвиденные вторичные последствия кибероперации и каскадные воздействия бывает трудно предвидеть из-за взаимосвязанной структуры компьютерных систем и сетей. Более того, для достижения законных военных целей может быть использована сила, однако чрезмерное применение силы запрещено в соответствии с концепцией военной необходимости (Singer & Friedman, 2014). Определение законной военной цели в кибервойне является проблематичным и сложным. Помимо обычных военных целей, целями кибероперациий являются ключевые объекты инфраструктуры, экономические системы и информационные сети. Поскольку последствия кибероперациий могут выходить далеко за рамки традиционных военных целей, определение того, когда в них отпадает необходимость, представляет собой значительную трудность.

По словам Michael Schmitt (2013), те же правила различения, соразмерности и военной необходимости, которые применяются в обычных конфликтах, применимы и к кибервойнам. Он утверждает, что стороны в боевых действиях должны видеть разницу между гражданскими лицами и комбатантами и наносить удары исключительно по первым. Стороны конфликта обязаны в соответствии с концепцией пропорциональности применять только тот уровень силы, который является необходимым и пропорциональным их ожидаемому военному преимуществу. Участвующие стороны обязаны в соответствии с концепцией военной необходимости применять силу не более, чем это требуется для достижения цели, которая может быть оправдана применением силы. По мнению указанного ученого, кибервойну можно рассматривать через ту же призму, что и обычную войну, то есть необходимо

руководствоваться концепциями различения, пропорциональности и военной необходимости. Он утверждает, что в случае кибератаки вовлеченные стороны также должны отличать военных от гражданских лиц и сосредоточить свои атаки на первых. Принцип пропорциональности диктует, что для достижения конкретной военной цели следует применять силу только в разумных масштабах. Согласно принципу военной необходимости, сила должна применяться только в случае абсолютной необходимости для достижения законной военной цели. Schmitt отмечает, что эти руководящие принципы позволят странам участвовать в кибероперациях, не нарушая международных норм (Schmitt, 2013).

Однако, по мнению профессора Cordula Droege (2012), особенности кибероперациий не позволяют применять традиционные критерии различения, пропорциональности и военной необходимости к киберконфликту. По его словам, кибератаки могут иметь непредвиденные последствия, и иногда их трудно идентифицировать. Ученый считает, что страны должны найти новые подходы к применению критериев различения, пропорциональности и военной необходимости к кибервойнам. Он утверждает, что эти критерии трудно применимы к кибероперациям из-за их специфического характера. Droege согласен с тем, что определение ответственности за последствия кибероперациий может быть сложной задачей. Поэтому, по его мнению, странам необходимо внедрять инновации, чтобы адаптировать эти идеи к кибервойнам (Droege, 2012). Сложность кибероперациий требует новых подходов и концепций. Более того, по словам Russel Buchan (Buchan, 2012), они должны интерпретироваться таким образом, чтобы учитывать особый характер кибероперациий. Последствия кибероперациий могут быть как физическими, так и нефизическими, объясняет ученый. По его словам, правительства должны проявлять осторожность при проведении кибероперациий. Buchan предлагает учитывать указанные критерии в качестве средства достижения справедливого баланса в киберконфликтах. Однако он отмечает, что эти понятия необходимо интерпретировать с учетом специфики кибероперациий. Как признает ученый, кибероперации могут иметь ряд конкретных и нематериальных последствий. Поэтому он предостерегает от нарушения норм осторожности и ответственности при проведении кибероперациий (Buchan, 2012).

3.3. Неадекватность традиционных принципов ведения войны в киберпространстве

Одной из самых больших проблем, связанных с созданием принципов ведения кибервойн, которые соответствовали бы традиционным боевым действиям, является атрибуция. Отследить источник или начало кибератаки не всегда возможно (Denardis, 2020). Это затрудняет привлечение государств к ответственности за эти действия и предотвращение атак до их начала. При адаптации традиционных методов разрешения конфликтов к цифровой среде сложно исключить непредвиденные последствия. Кибератаки могут иметь самые разнообразные физические и нефизические последствия. Например, атака на правительственную компьютерную сеть может привести к непреднамеренному отключению основных служб, таких как электросети или водоснабжение. Это усложняет задачу обеспечения разумности и уместности действий в киберпространстве. Операции в киберпространстве сложны, и их не всегда легко понять (Winterfeld & Andress, 2013). Из-за этого трудно применять концепции пропорциональности, дифференциации и военной необходимости. Иногда

бывает невозможно определить, направлена ли кибероперация против военного объекта или гражданского населения. Оценка возможных физических и нефизических последствий кибератак также может быть сложной задачей.

Существует ряд проблем, которые необходимо решить, прежде чем адаптировать традиционные принципы ведения вооруженных конфликтов к кибервойнам. Именно по этой причине кибервойне трудно дать точное определение, а также установить общепринятые принципы их ведения в глобальном масштабе. В сфере кибербезопасности отсутствует всемирная нормативно-правовая база, что препятствует совместной работе государств по борьбе с киберугрозами (Whyte & Mazanec, 2018). Темпы технического развития в киберпространстве очень высоки. Это затрудняет принятие новых законов и норм для своевременного устранения возникающих киберугроз. Несмотря на препятствия, необходимо приложить усилия для изменения норм ведения обычных боевых действий, чтобы они могли применяться к кибервойнам. Необходимы правила и конвенции по контролю за кибервойнами в связи с возрастающей опасностью, которую они представляют.

3.4. Сложности работы вне суверенных границ

По мнению Michael Schmitt (2012), правовые основы, определяющие юрисдикцию в отношении кибератак, сложны и находятся в процессе развития. Государства имеют значительную свободу действий в выборе того, как они будут осуществлять юрисдикцию в отношении кибероперации, и, как отмечает ученый, нет ни одной международной конвенции, которая бы напрямую решала этот вопрос. Schmitt утверждает, что нации могут руководствоваться различными всеобъемлющими принципами, такими как концепции территориальности, гражданства и универсальности (Schmitt, 2012b). Способность национального государства регулировать поведение в Интернете внутри своих границ основана на идее территориальности. Это означает, что, даже если жертвы киберпреступления находятся в другой стране, виновные могут быть привлечены к ответственности государством, в котором было совершено преступление (Schmitt, 2014). Принцип гражданства гласит, что страна несет ответственность за преступные деяния своих граждан в любой точке мира, в том числе когда они совершаются через Интернет. Таким образом, независимо от местонахождения жертв, государство может выдвигать обвинения против своих граждан, совершающих киберпреступления. Согласно принципу универсальности, любое киберпреступление, которое соответствует определению преступления по международному праву, может преследоваться в судебном порядке любым государством, независимо от того, где и кем было совершено преступление. Киберпреступников можно преследовать в судебном порядке в государстве, даже если они не являются резидентами этого государства, если их действия квалифицируются как преступления по международному праву, а их жертвы находятся в другой стране (Shackelford, 2014).

Однако Thomas J. Holt с соавторами (Holt et al., 2015) утверждают, что установление юрисдикции в отношении действий, совершаемых в киберпространстве, сопряжено с серьезными трудностями. Он указывает на трудности, связанные с отслеживанием происхождения кибератак и их возможного воздействия на глобальном уровне. Исследователь подчеркивает, что для того, чтобы государства могли осуществлять контроль за кибератаками, им необходимо внедрять новые формы сотрудничества. Это связано с тем, что иногда бывает трудно определить источник кибератаки, когда она только начинается. В результате становится все

сложнее привлекать государства к ответственности и предотвращать возможные нападения. Возможность непредвиденных последствий является еще одной трудностью при установлении юрисдикции в отношении кибератак. Последствия кибератак, как физические, так и иные, могут быть весьма разнообразными. Например, атака на правительственную компьютерную сеть может привести к непреднамеренному отключению основных служб, таких как электросети или водоснабжение (Shackelford, 2012). Это усложняет задачу обеспечения разумности и уместности действий в киберпространстве. По словам Peter M. Shane (Shane & Hunker, 2013), по мере роста масштабов кибератак трудности в установлении и применении юрисдикции в отношении них будут только возрастать. По его мнению, государствам необходимо прибегнуть к нестандартным подходам, чтобы справиться с трудностями, связанными с осуществлением их полномочий в отношении онлайн-активности. Ожидается, что трудности, связанные с осуществлением юрисдикции в отношении кибероперации, будут возрастать по мере дальнейшего развития кибертехнологий. Для преодоления этих трудностей государствам потребуется внедрять новые формы сотрудничества и координации (Shane & Hunker, 2013). Им также придется разработать ряд совершенно новых норм для контроля поведения в Интернете.

Отличаются сложностью и постоянно развиваются также проблемы юрисдикции, связанные с кибероперациями. Поскольку деятельность в киберпространстве не регулируется единой международной конвенцией, правительства отдельных стран имеют значительную свободу действий в определении сферы своей юрисдикции. Однако есть ряд общих принципов, которые могут использоваться для регулирования поведения государств. Эти понятия включают территориальность, национальную принадлежность и универсальность. Существуют значительные трудности в обеспечении соблюдения юрисдикции в отношении киберактивности (Roscini, 2010). Лица, стоящие за кибератаками, не всегда очевидны, а последствия их действий могут ощущаться по всему миру. Успешное определение юрисдикции в отношении кибератак требует новых форм сотрудничества между государствами. По мере расширения масштабов кибератак трудности с определением юрисдикции в отношении них, вероятно, сохранятся. Проблемы, связанные с установлением государственной власти над онлайн-активностью, требуют от правительств принятия упреждающих мер. В сфере кибербезопасности отсутствует всемирная нормативно-правовая база. Это препятствует совместной работе государств по борьбе с киберугрозами. Темпы технического развития в киберпространстве очень высоки (Gheciu & Wohlforth, 2018). Это затрудняет принятие новых законов и норм для своевременного устранения возникающих киберугроз. В рамках международного сотрудничества проблемы кибербезопасности решаются недостаточно активно. Необходимы совместные усилия по созданию и внедрению глобальных стандартов поведения в киберпространстве.

Заключение

В данном исследовании рассмотрены правовые последствия и трудности, связанные с кибератаками и мерами противодействия этим атакам в киберпространстве. Авторы подчеркивают, насколько сложно точно определить источник кибератак и насколько важно учитывать соразмерность при разработке контрмер в киберпространстве. В исследовании также обсуждается влияние кибернетических контрмер на права человека, правовые последствия контрмер против негосударственных

субъектов и правовые основы международного сотрудничества. Кроме того, рассмотрены правовые параметры превентивных кибероперaций, уровень подотчетности государства, трудности определения и проверки кибероружия, регулирующие структуры для разведывательных операций, роль мер кибербезопасности в защите гражданского населения и критически важной инфраструктуры, трудности установления юрисдикции в отношении кибердеятельности, а также взаимосвязь между кибербезопасностью и правом на развитие. Считая эти вопросы недостаточно изученными в рамках международного права, исследователи надеются внести свой вклад в формирование правовых систем и норм, регулирующих контрмеры в кибервойнах, способствуя тем самым инклюзивному и устойчивому росту при сохранении прав личности и международной кибербезопасности. По мере того как мир становится все более взаимосвязанным, риски, связанные с киберпространством, остаются насущной проблемой. Национальные границы становятся неэффективными, а существующие международные правовые системы сталкиваются с различными вызовами. Цифровая сфера является «серой зоной» с неопределенными правовыми принципами, что осложняет вопрос о том, являются ли кибератаки на самом деле преступными или нет. Отсутствие консенсуса в отношении определения кибератак и того, как общепринятые принципы международного права должны применяться к этим проблемам современности, является существенным пробелом в правовой системе. Для решения сложных проблем киберпространства требуется отдельная международная конвенция. Существующие рамки имеют свои ограничения и юрисдикционные проблемы, которые должна прояснить подобная конвенция. Это сложная задача, но ее необходимо решить для поддержания глобальной стабильности в эпоху, когда войны с такой же вероятностью будут вестись в Интернете, как и на земле. Международные организации пытались решить проблему кибератак, однако надлежащего ответа пока не удается добиться из-за постоянно меняющегося характера киберугроз и ограничений, налагаемых существующим международным правом и институциональными рамками. Новая международная конвенция, направленная на борьбу с киберугрозами, вселяет надежду на решение этого вопроса. Эта конвенция должна быть прозрачной, всеобъемлющей и гибкой, чтобы способствовать международному сотрудничеству, дать четкое определение уголовным деяниям и установить процедуры обеспечения их соблюдения. Такая конвенция стала бы огромным шагом вперед в деле повышения защищенности и безопасности Интернета. Поэтому важно пересмотреть и адаптировать существующую правовую инфраструктуру или изучить возможность создания специального международного органа, который мог бы эффективно реагировать на особенности военных действий в киберпространстве.

Список литературы

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic.

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.

Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0

Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583

Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960

Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001

Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878

Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466

Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001

Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759

Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527

Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009

Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870

Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384

Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009

Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.

Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.

Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.

Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546

Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231

Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.

Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.

Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001

Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014

Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr

Mihr, A. (2017). *Cyber Justice: Human Rights and Good Governance for the Internet*. Springer.

Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002

Nissenbaum, D. (2015). *A Street Divided: Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012a). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012b). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.
Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.
Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526
Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838
Shane, P. M., & Hunker, J. A. (Eds.) (2013). *Cybersecurity: Shared Risks, Shared Responsibilities*. Carolina Academic Press.
Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001
Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217
Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2
Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057
Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410
Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.
Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724
Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352
Watt, E. (2021). *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. Elgar. https://doi.org/10.4337/9781789900101
Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.
Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504
Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier.
Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.
Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.
Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Сведения об авторах



Рахман Мохаммад Минхазур – магистр права, преподаватель, кафедра права, Государственный университет Бангладеш
Адрес: Бангладеш, 1461, г. Дакка, Канчан, Саут Пурбачал
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450



Дас Тапос Кумар – магистр права, доцент, кафедра права и юстиции, Джахангирнагарский университет; кандидат на соискание степени PhD, Школа права, Городской университет Гонконга
Адрес: Бангладеш, 1342, г. Дакка, Савар; Гонконг, Коулун, Коулун Тонг, Тат Чи Авеню, 83
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

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: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 1 апреля 2024 г.
Дата одобрения после рецензирования – 18 апреля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them

Mohammad Minhazur Rahman
State University of Bangladesh, Dhaka, Bangladesh

Tapos Kumar Das
Jahangirnagar University, Dhaka, Bangladesh
City University of Hong Kong, Hong Kong

Keywords

cyberattack,
cybercrime,
digital technologies,
human rights,
international convention,
international law,
law,
principle of due diligence,
principle of proportionality,
principles of international law

Abstract

Objective: to categorize cyber attacks in the national and international legal sytems and to define legal measures to counter them at the international level.

Methods: include doctrinal legal analysis, formal legal, comparative legal methods, synthesis, induction, deduction, as well as methods of legal forecasting and modeling. International legal documents and acts of national legislation, judicial precedents, and doctrinal sources were studied.

Results: the article defines the legal consequences of cyberattacks, identifies difficulties in determining and holding individuals and organizations accountable for their commission, identifies national measures to counter cyberattacks based on the principle of proportionality, and systematizes the international legal framework for responding to cyberattacks. The main focus is on the urgent problems of identifying and verifying cyber weapons, establishing international standards for their use, developing methods of disarmament or limiting offensive cyber capabilities. The authors raise the issue of ensuring humanitarian activities, protecting critical infrastructure and the population through cybersecurity measures in wartime. The legal framework is analyzed; gaps and other defects are identified in the current regulation of exercising jurisdiction in such areas of cyber activity as international transactions, data localization and extraterritorial enforcement of national legislation. The parameters were developed and described within

✉ Corresponding author
© Rahman M. M., Das T. 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.

which states may conduct proactive cyber operations to prevent or deter cyberattacks (cyber countermeasures). The main parameters are due diligence, legal decisions on using cyber countermeasures, proportionality of protection measures to the consequences of illegal actions.

Scientific novelty: this is due to the progressive solutions in the field of international legal regulation of cyber countermeasures by states responding to cybercrime. The solutions are formulated taking into account the impact of the countermeasures on human and civil rights and freedoms, including the right to privacy and freedom of speech.

Practical significance: the research results can be used to develop and improve international legal instruments in the field of combating cyberattacks and ensuring cybersecurity, and can serve as a model for national legislators when designing law-making solutions to counter cybercrime.

For citation

Rahman, M. M., & Das, T. K. (2024). Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them. *Journal of Digital Technologies and Law, 2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

References

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic.

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.

Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0

Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583

Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960

Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001

Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878

Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466

Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001

Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759

Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice: Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002
Nissenbaum, D. (2015). *A Street Divided: Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012a). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012b). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.
Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.

Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526

Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838

Shane, P. M., & Hunker, J. A. (Eds.) (2013). *Cybersecurity: Shared Risks, Shared Responsibilities*. Carolina Academic Press.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217

Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2

Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057

Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410

Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.

Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724

Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352

Watt, E. (2021). *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. Elgar. https://doi.org/10.4337/9781789900101

Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.

Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier.

Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.

Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.

Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Authors information



Mohammad Minhazur Rahman – LLM, Lecturer, Department of Law, State University of Bangladesh
Address: South Purbachal, Kanchan, Dhaka-1461, Bangladesh
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450



Tapos Kumar Das – LLM, Associate Professor, Department of Law & Justice, Jahangirnagar University; PhD Student, School of Law, City University of Hong Kong
Address: Savar, Dhaka-1342, Bangladesh; 83 Tat Chee Avenue, Kowloon Tong, Kowloon, Hong Kong
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

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 declare 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 1, 2024
Date of approval – April 18, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:341:004.4
EDN: https://elibrary.ru/ocdmla
DOI: https://doi.org/10.21202/jdtl.2024.47

Международное сотрудничество в преодолении цифрового неравенства: правовые основы, барьеры и параметры развития

Ксения Михайловна Беликова ✉

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Москва, Россия

Рафаэл Диас Мартинс

Интерсистемас, Натал, Бразилия

Евгений Тенгизович Казанба

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Москва, Россия

Ключевые слова

доступность технологий,
законодательство,
международное право,
международное сотрудничество,
право,
сеть Интернет,
цифровое неравенство,
цифровое пространство,
цифровой разрыв,
цифровые технологии

Аннотация

Цель: на основе системного анализа достигнутого уровня международного сотрудничества в преодолении цифрового неравенства определить параметры его дальнейшего развития с учетом современных правовых и иных барьеров и глобальных вызовов, обусловленных переходом от экономики знаний к экономике данных.

Методы: методологическая основа исследования представлена диалектикой, сравнительно-правовым и историко-правовым подходами, методом системного анализа.

Результаты: проблема цифрового неравенства рассмотрена по следующим ключевым аспектам: доступ к сети Интернет; различия в уровне цифровой грамотности; особенности использования технологий и многогранность цифрового неравенства. Отмечается, что доступ к сети Интернет и цифровым технологиям должен стать основным правом человека, чтобы обеспечить равные возможности для всех слоев общества, поскольку изначально кристаллизация отчетливо выраженных цифровых различий основывается на существующих офлайн социальных различиях. Установлено, что для успешного преодоления цифрового неравенства наряду со стимулированием рационального

✉ Контактное лицо

© Беликова К. М., Диас Мартинс Р., Казанба Е. Т., 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.

использования технологий и обеспечением понимания людьми работы с ними и получаемых посредством них данных развитие цифровых навыков и грамотности среди населения является важнейшей глобальной задачей в решении вопроса преодоления цифрового неравенства. Предлагается расширить и углубить сотрудничество развитых стран с менее развитыми, чтобы последние могли производить больше данных, которые будут служить метрикой и основой для создания стратегий развития; при этом следует обеспечить большую прозрачность, предоставляя эффективные и доступные средства, чтобы владелец данных мог ясно понять, кем и с какой целью обрабатывались его персональные данные. Утверждается, что переход от экономики знаний к экономике данных требует адаптации стратегий международного сотрудничества для обеспечения справедливого доступа к данным и их обработки, что позволит ускорить научные открытия и поддержать инклюзивное экономическое развитие. Проанализированы вопросы фрагментации и дефрагментации международного права.

Научная новизна: обусловлена отсутствием в настоящее время результатов научного анализа достигнутого на сегодня уровня международного сотрудничества в преодолении цифрового неравенства с позиции параметров его системного развития и основных (юридических и иных) барьеров.

Практическая значимость: результаты исследования могут найти применение при совершенствовании правовой основы и стратегий международного сотрудничества в преодолении цифрового неравенства для обеспечения справедливого доступа к данным и их обработки.

Для цитирования

Беликова, К. М., Диас Мартинс, Р., Казанба, Е. Т. (2024). Международное сотрудничество в преодолении цифрового неравенства: правовые основы, барьеры и параметры развития. *Journal of Digital Technologies and Law*, *2*(4), 1003–1030. https://doi.org/10.21202/jdtl.2024.47

Содержание

Введение
1. Параметры развития международного сотрудничества в преодолении цифрового неравенства
   1.1. Общий контекст
   1.2. Доступ к сети Интернет: практические воплощения и барьеры
   1.3. Глобальный цифровой разрыв по линии «Север – Юг» и способы его преодоления
   1.4. Делокализация цифрового пространства как механизм международного сотрудничества: примеры подходов
2. Сотрудничество в преодолении цифрового неравенства на региональном уровне
   2.1. Вопрос фрагментации международного права и сетевое партнерство
   2.2. Цифровые навыки пользователей: параметр (барьер) развития
   2.3. Препятствия к полной реализации потенциала цифровых технологий: пример Бразилии и опыт СССР

2.4. Неравенство данных (data inequality): новый вызов экономики данных и использование персональных данных
Заключение
Список литературы

Введение

Юридические и другие науки всегда нацеливались на решение разнообразных общественных проблем, включая вопросы (не)равенства. Попытки стран снижать социальные неравенства не всегда были успешны, а научные исследования этих вопросов начинали проводиться спустя время после практической реализации этих попыток[1]. Быть может, в отношении цифрового неравенства/разрыва/пропасти (digital inequality/divide/gap) есть время найти решения и не упустить начинающие расти неравенства, все быстрее становящиеся социальными: в эпоху цифровизации часто наблюдается перенос социальных неравенств в приобретающее все большее значение в жизни людей цифровое пространство. Особенно учитывая тот факт, что достижение и соблюдение цифрового равенства в ходе цифровизации может стать эффективным инструментом борьбы с социальным неравенством.

1. Параметры развития международного сотрудничества в преодолении цифрового неравенства

1.1. Общий контекст

Если говорить о параметрах развития международного сотрудничества в преодолении цифрового неравенства как входных данных, то имеем следующую картину. В 2008 г. Генеральным секретарем ООН была созвана Группа высокого уровня по цифровому сотрудничеству (The High-level Panel on Digital Cooperation)[2] для продвижения предложений по укреплению сотрудничества в цифровом пространстве между правительствами, частным сектором, гражданским обществом, международными организациями, техническими и академическими сообществами и другими соответствующими или заинтересованными сторонами. Ожидается, что дискуссионный форум повысит осведомленность о преобразующем воздействии цифровых технологий на общество и экономику и внесет вклад в более широкую общественную дискуссию о том, как обеспечить безопасное и инклюзивное цифровое будущее для всех с учетом соответствующих норм в области прав человека. Как один из результатов работы этой Группы в 2019 г. вышел доклад «Эпоха цифровой взаимозависимости»[3] (сопредседатели – небезызвестные Мелинда Гейтс и Джек Ма), в котором утверждается, что «Цифровые дивиденды сосуществуют с цифровым разрывом»[4].

---

1 Киселева, Е. В., Маркелова, М. Н. (2022). Комплексный подход ООН к защите прав человека на примере детей-беженцев. В кн. А. Х. Абашидзе (ред.), Международное право: учебник для аспирантов (с. 300–329). Москва: РУДН.

2 Secretary-General's High-level Panel on Digital Cooperation. https://clck.ru/3EYpgr

3 The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. (2019, June 10). https://clck.ru/3EYpiU

4 Там же. P. 6.

Вероятно, поэтому традиционная схема анализа цифрового неравенства включает в себя три ключевых аспекта, которые мы также полагаем рассматривать одновременно и как параметры развития международного цифрового сотрудничества в рассматриваемой сфере, и как его барьеры, это: 1) неравный доступ к сети Интернет (access… as the 'first-level digital divide'); 2) различия в уровне цифровой грамотности среди пользователей как сети Интернет, так и различных цифровых продуктов, технологий и услуг (skills/usage …as the 'second-level digital divide'); 3) многогранность цифрового неравенства, подчеркивающая важность мотивации пользователей и особенностей использования технологий для достижения желаемых выгод (benefits/outcomes …as the 'third-level digital divide') (Li et al., 2024; Гладкова и др., 2019; Cinnamon, 2019; Du & Wang, 2024; Kuo-Hsun, 2022)[5].

Несмотря на то, что на современном этапе нельзя говорить о цифровом неравенстве всего лишь относительно доступа (отсутствия доступа) к сети Интернет, естественно, без такого доступа все остальные уровни просто не имеют никакого значения. По этой причине эти три уровня (параметра, барьера) получили достаточное внимание как в названном выше докладе «Эпоха цифровой взаимозависимости», так и в докладе Генерального секретаря ООН «Дорожная карта по цифровому сотрудничеству»[6]. В последнем через ссылку на доклад Группы 2019 г. указываются пять рекомендаций по совместной работе международного сообщества над оптимизацией использования цифровых технологий и снижением рисков, и первая в их числе – построение инклюзивной цифровой экономики и общества (в числе иных – развитие человеческого и институционального потенциала; защита прав человека и укрепление правозащитных организаций; укрепление цифрового доверия, безопасности и стабильности и содействие глобальному цифровому сотрудничеству). Тем самым указывается, что обращать внимание на доступ к сети Интернет и цифровым технологиям – необходимый шаг, но недостаточный. Нужно обеспечить использование технологий инклюзивным образом[7]. Кроме того, утверждается, что права человека реализуются как в Сети, так и вне ее, особенно в отношении безопасности и тайны личной жизни.

1.2. Доступ к сети Интернет: практические воплощения и барьеры

Начиная с вопроса доступа к сети Интернет, отметим, что в практическом плане проект Starlink от компании Space X, например, представляет собой уникальную инициативу, направленную на обеспечение цифрового равенства по всему миру. «Старлинк» (Starlink) – это глобальная сеть спутникового Интернета, которую разрабатывает и предоставляет компания SpaceX, основанная Илоном Маском[8]. Ее девиз – "Connect at home or on the go" («Подключайтесь дома или в дороге»). Предполагалось, что эта технология будет доступна по всему миру, однако на данный момент это не так по причине ограничений в разных странах, которые могут варьироваться и быть связанными с различными мотивировками, включая регулирование радиочастот,

5 Там же. Pp. 4, 6, 7–9, 11–13, 32.

6 Report of the Secretary-General Roadmap for Digital Cooperation. (2020, June). https://clck.ru/3EYpsV

7 Там же. P. 4.

8 High-speed internet around the world. https://clck.ru/3EYpuN

защиту конфиденциальности данных, безопасность и др.[9] Однако суть ограничений заключается не столько в наличии или отсутствии оборудования (например, по свежей информации в открытой печати, оборудование для работы «Старлинк» снова можно купить в России[10]) либо спутников, необходимых для работы спутникового Интернета, летающих на малой орбите и нарушающих территориальные границы различных стран, сколько в подходах к обеспечению информационной безопасности государств[11]. Озабоченность этим вопросом выливается в тексты различных актов и документов и в их проекты, например, ранее Минкомсвязь предложила внести в Кодекс РФ об административных правонарушениях статью, регламентирующую штраф за нарушение правил использования на территории России спутниковых сетей связи, находящихся под юрисдикцией иностранных государств[12]. Стоит упомянуть в этой связи и Постановление Правительства РФ от 20 октября 2021 г. № 1800 «О порядке регистрации радиоэлектронных средств и высокочастотных устройств»[13], установившее перечень подлежащих регистрации радиоэлектронных средств и высокочастотных устройств и правила их регистрации . Основывается этот подход, по-видимому, на идее цифрового суверенитета[14] и положениях Указа Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации»[15]. Стоит упомянуть, что спутники «Старлинк» уже давно в некотором роде мешают астрономам, а теперь группа специалистов из Китая опубликовала исследование в рецензируемом научном журнале Radio Engineering, обвинив SpaceX в том, что спутники ее системы «Старлинк» нарушают правила безопасности и могут привести к катастрофе на орбите, не соблюдая дистанцию между собой[16]. В частности, 30 июня 2022 г. два спутника «Старлинк» приблизились друг к другу на расстояние всего 4,9 км, притом что общепринятое минимальное расстояние составляет 10 км. Согласно этому исследованию, экстремальное сближение было не случайным, а результатом сложной схемы SpaceX, направленной

---

9 См., напр.: Сеть Starlink не будет работать в России, Китае, Белоруссии и Иране. (2022, 19 сентября). https://clck.ru/3EYpvS

10 См.: В России снова начали продавать терминалы Starlink. Где и как ими можно пользоваться? (2024, 6 февраля). clck.ru/3EYpwA

11 См., напр.: Starlink и OneWeb не могут работать в России из-за приоритета российской заявки на частоты. (2022, 15 декабря). https://clck.ru/3EYpya; Постановление Правительства РФ № 1194 от 14 ноября 2014 г. (2014, 24 ноября). ССЗ РФ. № 47, ст. 6554.

12 Минкомсвязь предлагает штрафовать за использование в России иностранных спутниковых сетей. (2019, 11 июня). https://clck.ru/3EYpzQ

13 СЗ РФ (2021, 1 ноября), № 44 (часть III), ст. 7411.

14 Зиновьева, Е., Яцзе, Б. (2023, 29 мая). Практика цифрового суверенитета в России и КНР. https://clck.ru/3EYq26

15 Указ Президента РФ № 646 от 05.12.2016. (2016, 12 декабря). СЗ РФ, № 50, ст. 7074.

16 Источник не говорит об этом, но в данном случае китайские ученые имеют в виду синдром Кесслера – теоретическое развитие событий, описывающее фактически принцип домино в масштабе околоземного пространства, когда появившийся, к примеру, в результате столкновения двух спутников космический мусор сталкивается с другими спутниками, образуя все больше и больше осколков, из-за чего в кратчайшие сроки вся орбита становится непригодной для размещения там космических аппаратов. См.: SpaceX с ее спутниками Starlink угрожает всей космонавтике? Китайские ученые призвали компанию придерживаться правил. (2022, 30 ноября). https://clck.ru/3EYq4q

на максимальную производительность системы лазерной связи. Указанный случай был якобы не единственным. До этого, в 2021 г., Китай обратился в ООН с жалобой на «Старлинк». В обращении указано, что за 2021 г. китайской космической станции пришлось дважды совершать маневр уклонения, чтобы избежать столкновения со спутниками Илона Маска[17]. Обращение основано на положениях Договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела[18], согласно ст. V которого «Государства – участники Договора незамедлительно информируют другие государства – участники Договора или Генерального секретаря Организации Объединенных Наций об установленных ими явлениях в космическом пространстве, включая Луну и другие небесные тела, которые могли бы представить опасность для жизни или здоровья космонавтов», а согласно его ст. VI, «Государства – участники Договора несут международную ответственность за национальную деятельность в космическом пространстве, включая Луну и другие небесные тела, независимо от того, осуществляется ли она правительственными органами или неправительственными юридическими лицами, и за обеспечение того, чтобы национальная деятельность проводилась в соответствии с положениями, содержащимися в настоящем Договоре...»[19]

Несмотря на подобные позиции, нельзя отрицать, что технология спутникового Интернета и ее правовой режим могут играть немаловажную роль в решении проблемы цифрового неравенства на уровне доступа к цифровым технологиям со стороны как развитых, так и развивающихся стран (Rabbani, 2024). Так, 5 июня 2024 г. генеральный директор ФГУП «Космическая связь» А. Волин на круглом столе по устранению цифрового неравенства в России, который прошел в Комитете Совета Федерации по экономической политике, отметил, что «Космическая связь» находится в тесном взаимодействии с Министерством цифрового развития в части подключения небольших населенных пунктов. «В России сейчас 13,8 тыс. поселений, в которых живут от 50 до 100 человек, и еще 20 тыс. поселков с населением от 11 до 25 человек. Это территории, куда оптоволокно не придет никогда. Мы посчитали, что потребуется 50 лет, чтобы провести во все эти места связь и Интернет с помощью кабеля, а цена подключения на одного абонента будет порядка 600 тыс. рублей». И, хотя спутник может предложить меньшую скорость, время и стоимость подключения потребителей в этом случае будет значительно меньше[20].

Исследователи отмечают, что яркий представитель цифровых технологий сеть Интернет была создана как средство передачи данных между университетами, а цель ее состояла в создании открытого доступа к знаниям (Pool et al., 1999), однако даже одна из самых старых глобальных сетей с коммутацией пакетов, ARPANET, была создана агентством DARPA (в то время – ARPA), заключившим контракт на разработку программного обеспечения с фирмой Bolt, Beranek and Newman из Кембриджа,

---

17 Китай подал жалобу в ООН на Starlink из-за угроз для своей космической станции. (2021, 29 декабря). Miltroen. https://clck.ru/3EYq5m

18 Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела [рус., англ.] Принят резолюцией 2222 (XXI) Генеральной ассамблеи от 19 декабря 1966 г. Подписан в гг. Вашингтоне, Лондоне, Москве. (1967, 27 января). https://clck.ru/3EYq6h и https://clck.ru/3EYq8V

19 Там же.

20 Цифровое равенство и спутниковое братство. (2024, 11 июня). https://clck.ru/3EYqBJ

штат Массачусетс, в конце 1968 г. Физически ARPANET состояла из приблизительно 50 мини-компьютеров C30 и C300 корпорации BBN, называемых узлами коммутации пакетов (PSN). Линии данных точка – точка, арендованные у фирм, предоставляющих глобальные линии связи, соединяли вместе PSN, образуя из них сеть. Так, арендованная линия связи соединяла PSN, находящийся в университете Пурдью, с PSN в Карнеги-Меллоне и с PSN в Университете Висконсина[21]. Да, фактически территориально они были в университетах, но DARPA[22] – это американское Управление перспективных оборонно-исследовательских проектов Министерства обороны США (Advanced Research Projects Agency с то появляющимся, то исчезающим первым словом Defence – «оборонных»)[23]. Действительно ли она изначально предполагала открытость? Ответ зависит от того, какой виделась цель ее создания (а сейчас – функционирования), а не промежуточного апробирования на инфраструктуре университетов.

Анализ других национальных актов об электронных коммуникационных сетях, электронном правительстве и услугах, например, Австрии, Дании, Нидерландов[24], самого Европейского союза[25], показывает, что целью правового регулирования выступает, с одной стороны, обеспечение равенства граждан и иных субъектов регулируемых отношений (например, людей с ограниченными возможностями здоровья и остальных), а с другой – наложение обязанностей на поставщиков услуг (например, органы государственной власти), что показывает отсутствие целостного регулирования даже на уровне национальных законодательств, его фрагментарность, – ситуация, которая могла бы быть устранена в России с принятием цифрового кодекса, идея которого не перестает обсуждаться.

1.3. Глобальный цифровой разрыв по линии «Север – Юг» и способы его преодоления

Вместе с тем обозначенная проблема доступа к технологиям приобретает новый окрас с позиции цифрового разрыва глобального Севера и глобального Юга, неравенства доступа к цифровой инфраструктуре между развитыми и развивающимися странами, между богатыми и бедными (так называемое inequality of technological opportunities (Cinnamon, 2019; Gallardo & Whitacre, 2024; Wang & Zhang, 2024)). И термин «цифровой неоколониализм» уже отнюдь не редок. Он вызван дисбалансом в ресурсах, доступных развитым и развивающимся странам. Дорогостоящие

---

21 Мировые информационные ресурсы. Тема 2. Обзор эксплуатирующихся информационных сетей. https://clck.ru/3EYqC8

22 DARPA. https://clck.ru/3EYqDF

23 См.: DARPA: как создавшее Интернет агентство родилось из продаж бытовой химии и страха перед «Спутником». (2022, 17 декабря). Erwinmal. Блог компании RUVDS.com. https://clck.ru/3EYqE2

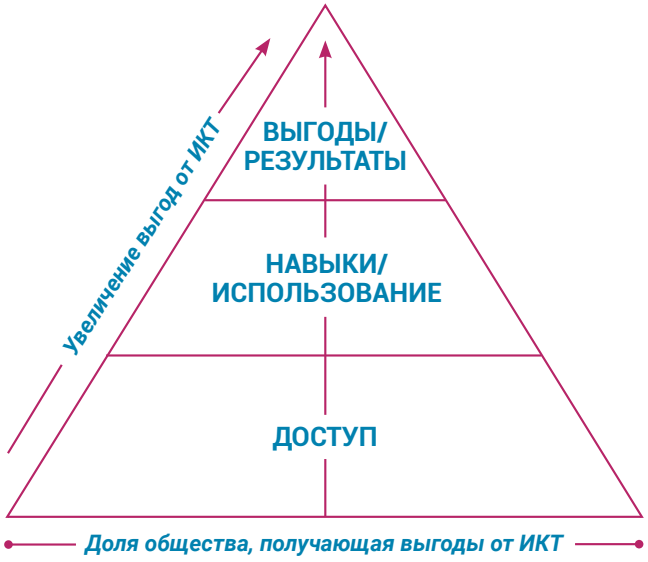
24 Данилов, Н. А. (2013). Правовое регулирование электронного правительства в зарубежных странах: автореф. дис. … канд. юрид. наук. Москва: ВШЭ; Данилов, Н. А. (2012). Социальная справедливость в информационном обществе: проблема цифрового равенства. Информационное право, 2(29), 5–6 и др.

25 Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. (2016, December 2). OJ L, 327, 1–15. https://clck.ru/3EYqFk; Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services. (2019, June 7), OJ L, 151, 70–115. https://clck.ru/3EYqHA

технологические решения, вызванные неприменением стратегии открытых патентов[26] и открытых инноваций (далее – ОИ) для пользователей – сейчас ОИ применяются для удобства и выгоды самих компаний ввиду отсутствия у них средств, специалистов и прочего для решения возникающих вопросов в одиночку – создают неравенство. Транснациональные компании монополизируют рынок и не способствуют развитию бедных стран. В результате бедные страны остаются зависимыми от богатых. При этом очень часто в цифровой сфере присутствует фактическая ситуация монополизации тех или иных решений, платформ и услуг.

Глобальный цифровой разрыв может усиливаться и из-за направления ресурсов на зеленую трансформацию. Поэтому, например, Программа индийского председательства в G20 выделяет цифровое равенство как приоритет. Без фундаментальной смены мировоззрения будет сложно достичь равного доступа к цифровой инфраструктуре и устойчивого развития[27]. Эта идея развивается в теме председательства Индии в G20 «Одна земля – одна семья – одно будущее» (“One Earth – One Family – One Future”), направленного на достижение единодушия для коллективного и эффективного решения глобальных проблем[28].

Тем самым можно представить следующую схему формирования цифрового неравенства (рис.), где цифровизация изначально определяется доступом к технологическим возможностям, хотя могут существовать дополнительные различия в технических навыках и способах использования технологий, а также в том, кто может извлечь выгоду и получить ощутимые результаты от использования технологий.



Уровни цифрового неравенства

Источник: (Cinnamon, 2019).

[26] Open Source Patents: Everything You Need to Know. Updated November 3, 2020 & February 01, 2023. https://clck.ru/3EYqHn

[27] См. подробнее: Барабанов, О. Н. (2023, 14 марта). Практики неоколониализма и глобальное цифровое равенство. https://clck.ru/3EYqLk

[28] Konishi, T. (2023, June 19). India’s G20 Presidency: An Opportunity to Steer the World Toward Inclusive and Sustainable Growth. https://clck.ru/3EYqMe

Если говорить о возможных механизмах, позволяющих решать проблему равенства в цифровой сфере, параметрах развития международного сотрудничества в рассматриваемой сфере, показывающей перспективы, то вопрос нехватки финансирования и дисбаланса в богатстве между развитыми и развивающимися странами можно решить через аналогию с климатической политикой, в рамках которой считается и пропагандируется, что развитые страны могут взять на себя обязательство по финансовой поддержке зеленого перехода развивающихся стран (Gritsenko, 2023; Liu et al., 2024). Подобным образом предлагается придерживаться принципа, согласно которому развитым странам надлежит помогать бедным странам с цифровой трансформацией и доступом к цифровым услугам[29]. В этой связи представляется, что готовность развитых стран давать деньги развивающимся странам на зеленый переход объясняется тем, что один из его элементов наряду с другими (использование возобновляемых источников энергии, экологически чистого транспорта, зеленое финансирование и внедрение ESG-стандартов в деятельность компаний) – это «декарбонизация» экономики (Поляков и др., 2022) (скажем, на примере литейной промышленности), что требует достаточных поставок экологически чистого водорода и энергии из возобновляемых источников по конкурентным ценам, а их производство даже в Европе еще необходимо наладить, при этом для широкомасштабного электролиза для производства «зеленого» водорода необходимы значительные объемы электроэнергии, производимой без использования ископаемого топлива, а это, в свою очередь, требует все больших инвестиций[30]. Тем самым на примере развивающихся стран можно видеть, что зеленый переход потребует колоссальных инвестиций и уничтожения существующей «карбонизированной» промышленности, а это, как представляется, ослабит данные страны как конкурентов на мировом рынке и с позиции конкуренции выгодно тем, кто хочет такого ослабления. Хотя сама по себе идея альтернативных источников энергии, безусловно, заслуживает внимания, одобрения на концептуальном уровне и развития, и обсуждается идея постановки ИКТ на службу декарбонизации (Wang et al., 2024). Тогда как равенство в цифровой сфере, наоборот, будет служить повышению конкурентоспособности этих стран на мировой арене. Желательно ли это, зависит от цели, которую преследует цифровизация вообще и отдельные ее проявления, например майнинг[31], в частности: так, «выращивание», развитие и функционирование «сильного искусственного интеллекта» будет требовать все новых и новых данных[32], что, в свою очередь, объективно потребует всеобщей цифровизации, если возникновение искусственного интеллекта – явление объективное, как законы природы (например, вода кипит при 100 градусах и др.), закономерно возникающее при определенном развитии событий (как изобретение пороха, колеса и пр.), а не субъективное (погоня за конкурентными преимуществами компаний, стран и т. д.).

---

29 Барабанов, О. Н. (2023, 14 марта). Практики неоколониализма и глобальное цифровое равенство. https://clck.ru/3EYqPP

30 Ермоленко, Г. (2024, 4 января). Декарбонизация металлургии требует снижения стоимости «зеленого» водорода – аналитики. https://clck.ru/3EYqQj

31 Колобова, М. (2024, 4 июня). Какие ваши коды: майнинг в РФ скоро станет видом экономической деятельности. Как это изменит рынок добычи криптовалют и поможет бюджету. https://clck.ru/3EYqSH. Для сравнения см., напр., рассказ: Кларк, А. (1953). Девять миллиардов имен Бога. (Arthur C. Clarke. The Nine Billion Names of God). https://clck.ru/3EYqTP

32 Бывший сотрудник OpenAI опубликовал прогнозы о будущем ИИ (2024, 5 июня). РБК Тренды. https://clck.ru/3EYqVG

Эта идея появилась не вчера – перед второй Всемирной встречей на высшем уровне по вопросам информационного общества в Тунисе в 2005 г. Генеральный секретарь ООН К. Аннан призвал ведущих производителей современных наукоемких и информационно-коммуникационных технологий расширить свою деятельность, сфокусировавшись на помощи развивающимся странам в развитии инноваций. Он отметил, что эффективность и устойчивость новой экономической модели – экономики, основанной на знаниях, – могут быть достигнуты только через всеобщее распространение принципов этой модели, удовлетворение потребностей человечества в коммуникации и информации, а также заинтересованность стран в достижении целей тысячелетия и уважение прав человека. Этот призыв также послужил основой для Тунисской программы по информационному обществу, принятой 15 ноября 2005 г. На предыдущей встрече в Женеве в 2003 г. были приняты Декларация о построении информационного общества как глобальной задачи в новом тысячелетии (12 декабря 2003 г.) и План действий по обеспечению развития информационного общества в глобальной перспективе (Перфильева, 2007). И так далее.

В этот же период появились и работы основоположника упоминавшейся выше стратегии открытых инноваций Г. Чесборо – Open Innovation: The New Imperative for Creating and Profiting from Technology (Harvard Business School Press, Boston, MA (2003)) и Open business models. How to thrive in the new innovation landscape (Harvard Business School Press, Boston, MA (2006).

1.4. Делокализация цифрового пространства как механизм международного сотрудничества: примеры подходов

Есть мнение о необходимости выделения цифрового пространства из ведения суверенитетов стран мира при создании отдельных юрисдикций международных органов на основе либо уже знакомых наднациональных, международных институтов, таких как Генеральная Ассамблея ООН и Совет Безопасности ООН, либо новых, работающих на основе координации усилий различных стран и организаций, в виде, например, такого международного органа, ответственного за законодательную деятельность в области цифрового равенства, как Международный совет по цифровому равенству (далее – МСЦР), и формировании нового нормативного регулирования и универсальных принципов, на которых оно будет строиться. Тем не менее основа такого представления создана давно. Так, идею сети Интернет как суверенной цифровой территории и отдельной юрисдикции выдвигали многие ученые. К примеру, Д. Р. Джонсон и Д. Г. Пост еще в 1996 г. рассматривали проблемы юрисдикции в киберпространстве и утверждали, что традиционные территориальные принципы права неприменимы к сети Интернет, предлагая концепцию киберпространства как независимого правового пространства (Johnson & Post, 1996). В свою очередь Д. Р. Рейденберг, рассматривая в 1997 г., как технологические решения могут формировать правовые нормы в киберпространстве, разработал концепцию lex informatica, высказал идею сети Интернет как самостоятельной юрисдикции и утверждал, что это может быть полезно для централизации законодательного вектора и впоследствии (Reidenberg, 1997).

Идеи делокализации сейчас принимают различные формы, например, идея делокализованного арбитража[33] коренится в концепции автономии международного коммерческого арбитража (далее – МКА) от национальных правовых систем и состоит в том, что МКА функционирует независимо от конкретных национальных правовых систем, формирует свою автономную правовую среду, в основном на уровне процедур, когда рассматривает и разрешает споры, так как вопросы процессуального и материального характера должны решаться на основе правил, выбранных сторонами или согласованных ими. При этом место нахождения арбитража не должно влиять на его работу, например, при определении своей компетенции, поскольку, как правило, стороны хотят видеть нейтральных арбитров и удобный (даже и территориально с позиции доступности) форум, поэтому решение этих вопросов в значительной степени не имеет прямого отношения к сути спора. Поскольку большинство решений МКА исполняются добровольно, а отказ в исполнении или отмена решения в одной стране не означает, что это решение не может быть применено в другой стране (как покажет дело ниже), то даже вопрос обязательного исполнения решения МКА не всегда связывает арбитраж с национальной правовой системой.

С инициативой создания принципиально нового инвестиционного арбитражного института на площадке БРИКС выступил Санкт-Петербургский университет: «Главное – мы предлагаем создать постоянно действующий институт, который будет учитывать не только особенности правовых систем, но и правовой политической культуры государств, в первую очередь, конечно, наших партнеров по БРИКС. Новый институт позволит учитывать публичные интересы в спорах инвестиционного характера, не ставить всегда на первое место только экономические интересы инвесторов, а искать сбалансированный подход, который будет обеспечивать интересы обеих сторон в инвестиционных отношениях. На наш взгляд, это должно стать серьезным стимулом для развития инвестиций», – сказал декан юридического факультета СПбГУ[34].

Пример действующих арбитражей такого типа – арбитраж посредством использования электронных телекоммуникационных сетей – on-line arbitration (например, интернет-суды трех городов Китая – Пекина, Гуанчжоу и Ханчжоу).

Пример реализации делокализации на практике – дело PT Putrabali Adyamulia v. Rena Holding[35]: согласно решению арбитража от 10 апреля 2001 г., отказ французской компании Rena Holding оплатить товар, купленный у индонезийской компании Putrabali, был признан законным. Последняя обжаловала его в Высоком суде Лондона, который направил дело на повторное рассмотрение арбитражной коллегии, которая 21 августа 2003 г. вынесла новое решение, обязывающее Rena Holding выплатить 163 086 долл. компании Putrabali. Параллельно в сентябре 2003 г. Rena Holding добилась признания и исполнения решения арбитража 2001 г. во Франции. В свою очередь Putrabali добилась признания и исполнения решения арбитража 2003 г. во Франции. 27 июня 2007 г. Кассационный суд Франции постановил, что решение арбитража 2001 г., признанное во Франции, не может быть изменено решением 2003 г., так как оно соответствует требованиям французского правопорядка,

---

33 См, напр.: Ученые СПбГУ предложили сделать Санкт-Петербург столицей международного инвестиционного арбитража [для стран – участниц БРИКС. – Авт.]. (2024, 8 мая). https://clck.ru/3EYqWj

34 Там же.

35 Enforcement of arbitration awards in France. (2008, July 29). Reed Smith LLP. https://clck.ru/3EYqYB

для того чтобы быть признанным, несмотря на то, что впоследствии оно и было изменено судом по месту арбитража. Решение арбитража 2003 г. было отменено на том основании, что оно было признано во Франции позже, чем решение от 2001 г.

Как видно из этих примеров, понимание делокализации арбитражного разбирательства различается как сущностно (как перенос места рассмотрения спора из одной страны в другую), так и институционально (как действие арбитражей в онлайн-среде). В этих условиях для его внедрения, как способа решения вопроса не только недоверия к арбитражам (включая инвестиционные), но и иных имеющихся к работе арбитражей вопросов, требуется выработка более четкого понимания данного понятия.

Возвращаясь к идее делокализации правового регулирования сети Интернет, ключевой правовой принцип, заложенный в основу работы МСЦР, мог бы заключаться в признании сети Интернет как глобального общественного блага, фактически устанавливая право на него как (квази?)право человека, доступное всем людям, независимо от их национальной принадлежности, социального статуса или физических возможностей (идея установления цифровой инклюзии как одного из основных прав человека предусмотрена сейчас Проектом конституционной поправки ст. 5 Конституции[36]).

МСЦР мог бы:

– устанавливать правовую основу для управления сетью Интернет, разрабатывая и принимая международные договоры (конвенции) и иные акты, имеющие обязательную силу для всех участников цифрового пространства, – например, регламенты, директивы и решения, которые, в свою очередь, устанавливали бы стандарты и нормы для различных аспектов использования и управления Интернетом. Тем самым провозглашаемый принцип равного доступа к сети Интернет закреплялся бы в международных актах, ратифицируемых странами-участницами, становясь частью их национальных правовых систем, а интернет-юрисдикция МСЦР действовала бы через совокупность международных договоров и национальных законодательных актов, обеспечивая их интеграцию в национальные правопорядки и унификацию, особое внимание уделяя вопросам защиты прав пользователей, включая защиту персональных данных и обеспечение кибербезопасности. В этой области МСЦР мог бы разрабатывать международные стандарты и протоколы, которые обязаны были бы соблюдать все участники цифрового пространства. Эти стандарты включали бы меры по предотвращению киберпреступности, защите конфиденциальности и обеспечению безопасности цифровых коммуникаций;

– устанавливать юридические механизмы мониторинга и обеспечения соблюдения принимаемых им нормативных актов. В такую систему входили бы специализированные органы надзора и контроля, которые имеют право проводить расследования, оценивать соответствие установленным стандартам и принимать меры по устранению нарушений. В случае несоблюдения требований международного законодательства МСЦР сможет применять санкции, включая штрафы и ограничение доступа к интернет-ресурсам;

– инициировать и поддерживать международные программы и проекты, направленные на развитие цифровой инфраструктуры и повышение цифровых навыков

[36] Proposta de Emenda à Constituição n° 47, de 2021. https://clck.ru/3EYqZ4

населения. Эти программы могли бы финансироваться через международные фонды и реализовываться в сотрудничестве с национальными правительствами и частным сектором и были бы направлены на создание справедливой, инклюзивной и безопасной цифровой среды, будучи закрепляемыми через международные договоры и соглашения о сотрудничестве, которыми определялись бы обязательства сторон и условия их выполнения;

– в рамках своей юрисдикции активно сотрудничать с другими международными организациями, такими как ООН, Всемирный банк и Всемирная организация здравоохранения для координации усилий и обеспечения комплексного подхода к решению глобальных проблем цифрового (не)равенства. Такое взаимодействие основывалось бы на международных правовых соглашениях и механизмах (инструментах), которые определяли бы взаимные обязательства и способы координации действий.

Таким образом, сеть Интернет, как международная юрисдикция под управлением МСЦР, представляла бы собой сложную правовую структуру, основанную на международных договорах и национальных законодательных актах, направленную на обеспечение равного доступа, защиты прав пользователей и устойчивого развития цифрового пространства.

Это, как представляется, на текущий момент некий идеальный вариант для будущего. На сегодня же можно, в условиях фрагментации международного права и экономики (о которых будет сказано ниже), конечно, говорить о фрагментированной сети Интернет в будущем, например, объединенной сети Интернет нескольких стран – стран БРИКС или Россия – Иран – Северная Корея и пр.

Тогда как на сегодня в связи с отсутствием всеобъемлющих правовых источников международного характера возникает вопрос, а возможно ли вообще достижение цифрового равенства с текущим правовым регулированием? Ведь обозначенных подходов и их воплощений недостаточно, чтобы решить вопрос цифрового неравенства, но они являются необходимым шагом для этого.

2. Сотрудничество в преодолении цифрового неравенства на региональном уровне

2.1. Вопрос фрагментации международного права и сетевое партнерство

Вместе с тем никто не отменял давно существующую фрагментацию международного права, которой способствуют такие факторы, как регионализация, специализация международного права, начавшие развиваться с определенного момента в прошлом объединительные идеи на уровне государств (Соединенные штаты Европы / ЕС, МЕРКОСУР, НАФТА), экономик (АТЕС, АСЕАН) и стратегий (БРИКС и др.), которые вносили и вносят свой вклад, с одной стороны, в процесс регионализации и тем самым фрагментации (например, договоры Монтевидео 1960 и 1980 гг.), с другой – в процесс глобализации и унификации, работая на (де)фрагментацию путем создания правовых способов преодоления национальных границ при формировании глобальной экономики и выявления сохранившихся и на сегодняшний день особых правовых запретов, пределов дозволенного и ограничений на примере существующих объединений и ряда входящих в них государств и реалии современности. Результатом фрагментации международного права становится

перенос усилий государств по обеспечению различных вопросов международной повестки на уровень региональных и иных интеграционных объединений. Так, в п. 33 Йоханнесбургской декларации-II. БРИКС и Африка: партнерство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности[37] говорится о важности цифровой экономики для глобального экономического развития с позиции положительного влияния торговли и инвестиций на содействие устойчивому развитию, национальной и региональной индустриализации, а также переходу к устойчивым моделям потребления и производства; акцентируются вызовы, стоящие перед странами БРИКС в цифровую эпоху, включая неравенство в цифровом развитии, и необходимость преодоления связанных с вызовами проблем. Участники выражают поддержку созданию Рабочей группы БРИКС по цифровой экономике и подчеркивают роль открытости, эффективности, стабильности и надежности в стимулировании международной торговли и инвестиций, приветствуя дальнейшее партнерство между странами БРИКС для укрепления взаимосвязей в цепочках поставок и системах платежей с целью поощрения торговли и инвестиционных потоков (Сэндтон, Гаутенг, ЮАР, 23 августа 2023 г.). В п. 74 говорится о стремлении укреплять обмен навыками и сотрудничество между странами БРИКС, поддержке цифровизации в сфере образования и ТПОП, поскольку каждая страна БРИКС на национальном уровне стремится обеспечить доступность и справедливость образования, а также содействовать развитию качественного образования, обмениваться цифровыми образовательными ресурсами, создавать интеллектуальные образовательные системы, совместно содействовать цифровой трансформации образования в странах БРИКС и развитию устойчивого образования путем укрепления сотрудничества в рамках Сетевого университета БРИКС и других инициатив в этой области, включая Лигу университетов БРИКС, включить в Сетевой университет больше университетов стран БРИКС, обмениваться передовым опытом по расширению доступа к комплексному воспитанию и образованию детей младшего возраста для обеспечения лучших условий для развития детей в странах БРИКС, содействовать обмену между странами БРИКС по вопросам формирования у учащихся навыков, пригодных для будущего, с помощью различных форм обучения[38]. Тем самым мы видим, что на уровне БРИКС обозначен и подход к признанию (обозначению) и снятию второго из обозначенных выше параметров (барьеров) в преодолении цифрового неравенства – навыка пользователей.

2.2. Цифровые навыки пользователей: параметр (барьер) развития

Говоря об этом втором параметре (барьере), отметим, что вопрос о навыках использования будет решаться быстрее и более значительно среди молодого населения, которое могло бы оказывать помощь другим слоям населения (Ren & Zhu, 2024). В любом случае из трех параметров (барьеров), думается, вопрос навыков не

[37] МИД РФ. (2023, 24 августа). Йоханнесбургская декларация-II. БРИКС и Африка: партнерство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности. https://clck.ru/3EYqaG

[38] Там же.

самый значительный, так как мы видим, что технологии входят в жизнь всех людей и они к ним привыкают. С другой стороны, стоит иметь в виду и уже отмечавшийся выше применительно к «декарбонизации» экономики момент, подобный описанному в фантастическом рассказе Пола Андерсона 1963 г. «Поворотный пункт» (Poul Anderson, “Turning Point”)[39], в котором обсуждался один из возможных вариантов контакта землян с инопланетянами – с позиции «эффекта домино»[40] в развитии технологий последних. В этом рассказе, в частности, приводились размышления персонажей по вопросу развития технологий инопланетной цивилизацией: «– Да, – задумчиво сказал Балдингер. – Я всегда отдавал себе отчет, что где-то должны быть существа поумнее нас. Вот только не ожидал, что человечество встретится с ними на моем веку. Уж слишком микроскопический отрезок Галактики мы исследовали. И потом… Я всегда думал, что у них будут машины, наука, космический транспорт.

– Они у них и будут, – сказал я.

– Если мы теперь улетим… – начал Лежен.

– Поздно, – сказал я. – Мы уже дали им эту блестящую погремушку – науку. Если мы сбежим, они сами отыщут нас через пару веков. Самое большее»[41].

Вместе с тем мы не утверждаем, что вопрос о навыках использования цифровых технологий неважный. Его важность подчеркивается различными региональными инициативами на уровне Европейского союза, например, это Коалиция «Цифровые навыки и рабочие места, которая борется с дефицитом цифровых навыков, объединяя государства-члены, компании и организации»[42]; Европейская программа повышения квалификации – пятилетний план, направленный на то, чтобы помочь частным лицам и предприятиям развивать больше навыков и применять их на практике[43]; Программа стажировок «Цифровые возможности» – учебная инициатива, финансируемая ЕС, направленная на то, чтобы помочь производственным компаниям, банкам, компаниям в сфере сельского хозяйства и здравоохранения заполнить вакансии кандидатами, владеющими цифровыми технологиями для кибербезопасности, анализа данных, машинного обучения, так как компьютерно грамотная рабочая сила жизненно важна для поддержания глобальной конкурентоспособности Европы в быстро меняющемся мире[44]. При всем этом, думается, вопрос овладения определенными навыками проще и легче решаем, чем параметр (барьер) третьего уровня – многогранность цифрового неравенства или то, как люди пользуются технологиями и какие выгоды (или даже проблемы) из этого извлекают.

---

39 Андерсон, П. (1963). Поворотный пункт. Libking. https://clck.ru/3EYqbD

40 Эффект домино – политическая теория, которая заключается в том, что какое-либо изменение влечет за собой линейный ряд других изменений, аналогично тому, как падают косточки домино, выстроенные в ряд.

41 Андерсон, П. (1963). Поворотный пункт. Libking. https://clck.ru/3EYqbD

42 European Commission. The Digital Skills and Jobs Coalition. https://clck.ru/3EYqgZ

43 European Commission. The European Skills Agenda. https://clck.ru/3EYqfE

44 Digital Opportunity Traineeships. ErasmusIntern.org. https://clck.ru/3EYqhL

2.3. Препятствия к полной реализации потенциала цифровых технологий: пример Бразилии и опыт СССР

Мы знаем, что сеть Интернет открывает много возможностей, но также может разрушать жизнь людей. В сети Интернет сегодня и казино, и другие игры, на которые, может, и не нужно тратить деньги, но они могут настолько занимать время человека, что становятся вредными. Итак, третий уровень, по нашему мнению, – самый сложный момент.

Дело в том, что то, как пользователи будут пользоваться технологиями, определяется главным образом различными социологическими факторами. Например, во всеобъемлющем труде A Ralé Brasileira – Quem é e como vive бразильского исследователя Жессе де Соуза показано, что переход к среднему классу из низшего – это иллюзия, так как этот «переход» основан лишь на денежном факторе: много людей в Бразилии стали зарабатывать в денежном выражении, как средний класс или выше, но люди, происходящие из бедных (ниже среднего) классов, которые никогда не вписывались в средний класс, продолжают не вписываться в него, так как их менталитет и даже менталитет их детей – другой.

Если традиционный представитель среднего класса думает: «Я буду работать, и все будет хорошо», то представитель «нового» среднего класса жил и продолжает жить, несмотря на деньги, с менталитетом бедного человека, поэтому не происходит смешения представителей «нового» среднего класса с теми, кто традиционно был и продолжает быть его представителем, то же касается и их детей – последние не уверены в себе, подготавливаются не как лидеры, они продолжают мыслить категориями представителей ниже среднего класса. Другими словами, даже если люди получают деньги, ментально они не становятся представителями среднего класса (Souza, 2018).

Этот подход проявляется в Бразилии и в цифровой среде. Нет точных исследований по этому поводу, но некоторые данные показывают, что доступ к сети Интернет среди самых бедных жителей Бразилии увеличился, но влияние подключения на жизнь людей остается неравномерным между классами, высказывается предположение[45], что использование сети Интернет людьми ниже среднего класса не даст им шанса развиваться. И нет в инициативах на уровне международного сообщества мер для решения именно этой значительной проблемы.

Представляется, что контуры этой проблемы возможно очертить во всех обществах, где исторически большой разрыв между богатыми и бедными. По нашему мнению, это связано с получаемым людьми изначальным уровнем воспитания и последующего образования.

Понятно, что не на пустом месте появились слова «Дав человеку рыбу, ты накормишь его один раз. Научи его ловить рыбу, и он будет кормиться ею всю жизнь», приписываемые то Лао-цзы, то Конфуцию, то рассматриваемые как упоминаемые в созданном во времена ранней Хань древнекитайском философском трактате «Хуайнань-цзы»[46].

---

[45] O portal Brasil61.com conversou com o ex-coordenador do Comitê Gestor da Internet no Brasil, Márcio Migon. Reportagem: Felipe Moura. 21 de Fevereiro de 2022, 22:35h, Atualizado em: 23 de Fevereiro de 2022, 22:46h. https://clck.ru/3EYqj5

[46] «Хочешь накормить человека один раз – дай ему рыбу...». (2020, 10 июня). https://clck.ru/3EYqkP; Сегодня разберем пословицу, которая уходит корнями глубоко в китайскую историю. (2023, 10 января). ВКонтакте. https://clck.ru/3EYqn5 и др.

Описываемая проблема была решена в Советском Союзе в ходе кампании по ликвидации безграмотности (ликбеза) и массовому обучению с 1919 г. до начала 1940-х гг. грамоте взрослых и подростков – самого масштабного социального и образовательного проекта не только во всей истории России, но и Европы, которому сопутствовала упорная и трудная работа по созданию разветвленной сети общеобразовательных школ, рабфаков, техникумов и вузов (Трубилин, Золотухина, 2022); мы все помним плакат «Знание разорвет цепи рабства» (худ. А. Радаков, 1920 г., Петроград)[47].

Кроме того, когда у человека появляется мечта (возьмем, например, так называемую американскую мечту, отчасти находящую отражение в кинофильме «В погоне за счастьем» (2006, США)[48], или известный сюжет романа Дж. Лондона «Мартин Иден», или описанную в индийском эпосе «Махабхарата»[49] неодолимую тягу Карны, сына принцессы Кунти и Бога Солнца Сурьи, волею судеб воспитывавшегося в семье колесничего, стать лучником и великим воином), она является движущей силой его развития.

Вместе с тем те идеи и их воплощения, что мы описали, развивались в недрах экономики знаний (Rodríguez et al., 2021) – экономической системы, в которой производство товаров и услуг основано, главным образом, на наукоемких видах деятельности, способствующих развитию технических и научных инноваций, и в которой ключевой элемент ценности зависит от человеческого капитала и интеллектуальной собственности как источника инновационных идей, информации и практик. Сейчас же происходит переход от экономики знаний к экономике данных[50] – цифровой экосистеме, по своей сути сетевой и кастомизированной, в которой данные собираются различными субъектами, включая государство, поисковые системы, социальные сети, интернет- и обычные магазины, платежные системы, поставщиков программного обеспечения, таких как услуги (SaaS) и иных компаний, использующих подключенные устройства в интернете вещей (IoT) (Ершова и др., 2024), систематизируются и обмениваются этими данными посредством сети частных лиц (компаний) и учреждений для создания экономической ценности. В такой экономике наряду с хранением и защита собранных данных, в том числе персональных, составляет значительную ее часть и приоритет.

2.4. Неравенство данных (data inequality): новый вызов экономики данных и использование персональных данных

В этих условиях появляются новые проблемы неравенства – data inequality (Cinnamon, 2019), которые традиционно не охватываются концепцией цифрового неравенства. Поскольку современная экономика во многом зависит от данных, не только от больших, но особенно от них, персональные данные часто называют новой нефтью. С одной стороны, все пользователи с доступом к сети Интернет

47 Музей Москвы. Экспонаты. https://clck.ru/3EYqny

48 The Pursuit of Happyness, 2006, USA. https://clck.ru/3EYqpE

49 Сериал «Махабхарата», 2013, Индия. https://clck.ru/3EYqqA

50 European Commission. (2021, May 9). Results of the European Data Market study 2021–2023. https://clck.ru/3EYqru

производят такие данные, с другой – очень немногие из них имеют возможность эти данные обработать и извлечь из них выгоду.

Так, в рамках экспериментального правового режима, установленного Федеральным законом от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона «О персональных данных»[51], обезличенные персональные данные смогут обрабатываться без согласия субъекта персональных данных – идентифицируемого гражданина – в целях повышения эффективности государственного или муниципального управления. Что может пониматься под повышением такой эффективности, неясно.

Аналитики считают[52], что такие данные будут обрабатываться участниками эксперимента на основании соглашения с уполномоченным органом (определяется Правительством Москвы), которое будет содержать требования к процедурам обезличивания персональных данных, получаемых участником эксперимента и/или органами государственной власти и местного самоуправления на основе положений Приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»[53] (Приказ № 996) и в последующем передаваться участнику экспериментального правового режима на основании вышеназванного соглашения. Эти способы обработки будут применяться и к данным о состоянии здоровья (сведениям о наличии или отсутствии инвалидности, медицинском диагнозе и т. д.), тогда как ранее Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[54] не содержал положений о том, что соответствующие сведения могут обрабатываться в обезличенном виде без согласия субъекта персональных данных.

Здесь ставятся вопросы[55] о том, что за редким исключением данные невозможно обезличить полностью и остается риск обратной идентификации (например, об этом прямо говорит п. 5 Приказа № 996, согласно которому обезличенные данные должны иметь характеристику запрещенной, например, в Бразилии, обратимости – возможности преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность; для многих компаний требование по обезличиванию может оказаться

---

51 О персональных данных. № 152-ФЗ от 27 июля 2006 г. (2006, 31 июля). Собрание законодательства РФ, 31 (часть I), ст. 3451.

52 Зайцев, А., Мингазова, Л. (2020, 10 июня). #DigitalLaw. Обзор Федерального закона о проведении в Москве эксперимента в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта. Часть 1. Деловые решения и технологии. Zakon.ru. https://clck.ru/3EYquM

53 Приказ об утверждении требований и методов по обезличиванию персональных данных. (2013, 17 сентября). Российская газета, 208.

54 О персональных данных. № 152-ФЗ от 27.07.2006. (2006, 31 июля). Собрание законодательства РФ, 31 (часть I), ст. 3451.

55 Эксперимент над Москвой: Закон о внедрении искусственного интеллекта вступил в силу. (2020, 1 июля). НК – истории адвокатов! https://clck.ru/3EYqvR; (Cinnamon, 2019).

в новинку, поэтому есть сомнения, как оно будет реализовываться; если данные настолько ценные, почему только большие или избранные компании должны иметь доступ и возможность их толковать, приводя к появлению у большинства пользователей статуса «цифрового пролетариата» (a sort of 'digital proletariat')?

В Бразилии ситуация несколько иная, но вопросы те же. Так, правила об осведомлении субъектов персональных данных о целях обработки их данных закреплены в Законе о защите персональных данных 2018 г.[56] (Закон 2018 г.), но они неэффективны. Например, согласно п. I ст. 6 этого Закона оператор должен обрабатывать персональные данные согласно законным, легитимным и заранее определенным и сообщенным субъекту персональных данных целям, а согласно п. VI ст. 6 оператор должен гарантировать такому субъекту качество его данных в части гарантии их точности, ясности, релевантности и актуальности в соответствии с необходимостью, обусловившей их сбор, и целью их обработки; ст. 7 устанавливает случаи, в которых допустима обработка персональных данных, в их числе выполнение юридических обязанностей или регулирующих функций контролирующего органа (напр., п. II), при этом согласно ст. 18 субъект персональных данных имеет право на получение от контролирующего органа в любое время и по запросу в отношении обрабатываемых им данных субъект: I – подтверждения наличия обработки; II – доступа к данным; III – исправления неполных, неточных или устаревших данных; IV – анонимизации, блокировки или удаления ненужных, чрезмерных данных или данных, обрабатываемых не в соответствии с положениями Закона 2018 г.; V – переноса данных другому поставщику услуг или продуктов по прямому запросу и с соблюдением коммерческой и промышленной тайны в соответствии с правилами, действующими в отношении контролирующего органа; VI – удаления персональных данных, обрабатываемых с согласия владельца, за исключением случаев, предусмотренных ст. 16 Закона 2018 г.; VII – информации о государственных и частных лицах, с которыми контролирующий орган осуществлял совместное использование данных; VIII – информации о возможности не давать согласие на обработку данных и о последствиях отказа; IX – отзыве согласия в соответствии с § 5 ст. 8 Закона 2018 г.

Но эти формулировки часто не описывают и не передают субъекту, предоставившему свои данные, правильное представление пути его персональных данных на рынке данных. Тогда как сегодня часто бывает, что, если пользователь не хочет предоставить свои данные, он не может пользоваться сервисами. Кроме того, производство данных в мире неравномерно, и одна из причин в том, что в мире насчитывается около 1,1 млрд человек без официального документа, удостоверяющего личность; часто не производится фиксация основных данных, таких как рождение, смерть и т. п., что создает массу информационно бедных людей (Cinnamon, 2019).

Как в таких случаях вообще создать метрику развития? Если развитие – это цель международных усилий, как же оценить результаты мер, направленных на достижение этой цели?

---

[56] Lei Geral de Proteção de Dados Pessoais (LGPD) Nº 13.709, de 14 de Agosto de 2018 (Redação dada pela Lei nº 13.853, de 2019 para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências). https://goo.su/tUZhUwC

Представляется, что международные усилия должны сосредоточиваться на 1) создании принудительных правил, для того чтобы компании, работающие с данными, правильно осведомляли пользователей о своих целях таким образом, чтобы пользователь точно знал, что будет сделано с его данными, и 2) создании принудительных правил для более гибкого выбора целей обработки персональных данных (и данных вообще) и их использования на стороне предоставляющих их для обработки и т. п. лиц.

Заключение

Изложенное позволяет заключить следующее.

1. Будущее цифрового общества зависит от совместных усилий мирового сообщества по созданию справедливых и равноправных условий доступа к информационным ресурсам и технологиям. Поэтому доступ к сети Интернет и цифровым технологиям должен стать основным правом человека, чтобы обеспечить равные возможности для всех слоев общества, поскольку изначально кристаллизация отчетливо выраженных цифровых различий основывается на существующих офлайн социальных различиях.

2. Развитие цифровых навыков и грамотности среди населения является важнейшей задачей для успешного преодоления цифрового неравенства наряду со стимулированием рационального использования технологий, чтобы достичь всех предлагаемых ими потенциальных выгод и обеспечить понимание людьми работы с большими данными и использования их персональных данных.

3. Необходимо расширить и углубить сотрудничество развитых стран с менее развитыми, чтобы последние могли производить больше данных, которые будут служить метрикой развития и основой для создания стратегий развития. При этом следует обеспечить большую прозрачность, предоставляя эффективные и доступные средства, чтобы владелец данных мог ясно понять, кем и с какой целью обрабатывались его персональные данные.

4. Переход от экономики знаний к экономике данных требует адаптации стратегий международного сотрудничества для обеспечения справедливого доступа к данным и их обработки. Вследствие чего информация, полученная в результате обработки больших данных, должна быть более доступна исследователям и широкой общественности, что позволит ускорить научные открытия и поддержать инклюзивное экономическое развитие, в том числе на основе политики транснационального доступа к исследовательской инфраструктуре, совместной эксплуатации объектов исследовательской инфраструктуры, например, стран БРИКС.

5. Для достижения всего этого всем странам следует озаботиться развитием образовательной системы в плане совершенствования способов приобретения населением мыслительных способностей и развития его мировоззрения, учитывая возможности использования социальных и культурных ресурсов стран БРИКС, например, таких как языковое разнообразие и традиции образования, для создания качественного и справедливого образования, рассматривая открытое образование как модель образования будущего.

Список литературы

Гладкова, А. А., Гарифуллин, В. З., Рагнедда, М. (2019). Модель трех уровней цифрового неравенства: современные возможности и ограничения (на примере исследования Республики Татарстан). *Вестник Московского университета (Серия 10. Журналистика)*, *4*, 41–72. https://doi.org/10.30547/vestnik.journ.4.2019.4172

Ершова, И. В., Лаптев, В. А., Андреева, Л. В., Ахрем, Т. П., Беликова, К. М., Беседин, А. Н., Габов, А. В., Галкин, С. С., Друева, А. А., Ельникова, Е. В., Енькова, Е. Е., Кантор, Н. Е., Короткова, О. В., Лебедев, А. В., Микрюков, В. А., Микрюкова, Г. А., Петраков, А. Ю., Сайдашева, М. В., Свит, Ю. П. … Щербакова, М. А. (2024). *Право и реальный сектор экономики России*. Москва: Проспект. EDN: https://elibrary.ru/awgyzd. DOI: https://doi.org/10.31085/9785392407354-2024-480

Перфильева, О. В. (2007). Проблема цифрового разрыва и международные инициативы по ее преодолению. *Вестник международных организаций: образование, наука, новая экономика*, *2*(2), 34–49. https://elibrary.ru/jwnzzp

Поляков, Л. В., Анкудинов, И. А., Егоров, В. Ю., Ляцос, А. Д., Рыжкин, Е. Н. (2022). Зеленая Россия будущего: экономические проблемы и политические перспективы. *Бизнес. Общество. Власть*, 46, 87–116. https://www.elibrary.ru/wjuvwn

Трубилин, А. Г., Золотухина, А. Д. (2022). Ликвидация безграмотности – самый масштабный социальный и образовательный проект в истории России. *Международный журнал гуманитарных и естественных наук*, *12-5*(75), 16–21.

Cinnamon, J. (2019). Data inequalities and why they matter for development. *Information Technology for Development*, *26*(2), 214–233. https://doi.org/10.1080/02681102.2019.1650244

Du, Z., & Wang, Q. (2024). Digital infrastructure and innovation: Digital divide or digital dividend? *Journal of Innovation & Knowledge*, *9*(3), 100542. https://doi.org/10.1016/j.jik.2024.100542

Gallardo, R., & Whitacre, B. (2024). An unexpected digital divide? A look at internet speeds and socioeconomic groups. *Telecommunications Policy*, *48*(6), 102777. https://doi.org/10.1016/j.telpol.2024.102777

Gritsenko, D. (2023). Advancing UN digital cooperation: Lessons from environmental policy and governance. *World Development*, *173*, 106392. https://doi.org/10.1016/j.worlddev.2023.106392

Johnson, D. R., & Post, D. G. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Kuo-Hsun, J., Ma. (2022). *Digital learning divide. In International Encyclopedia of Education* (4th Ed., pp. 157–164). https://doi.org/10.1016/b978-0-12-818630-5.01013-7

Li, P., Li, Q., & Li, X. (2024). The influence of three digital divide levels on financial advisor demand and engagement among Chinese residents: An investigation based on China. *Journal of Innovation & Knowledge*, *9*(2), 100488 https://doi.org/10.1016/j.jik.2024.100488

Liu, N., Qian, Y., Gu, X., & Li, G. (2024). Digital technology, e-commerce, and economic inequality: The case of China. *International Review of Economics & Finance*, *91*, 259–271. https://doi.org/10.1016/j.iref.2024.01.016

Pool, H., Schuyler, T., Senf, T. M., & Moschovitis, Ch. J. P. (1999). *History of the Internet. A Chronology, 1843 to Present*. London: ABC-CLIO.

Rabbani, M. (2024). Internet price, speed, and disparity: The case of rural healthcare providers in the United States. *Telecommunications Policy*, *48*(2), 102674 https://doi.org/10.1016/j.telpol.2023.102674

Reidenberg, J. R. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, *76*, 553.

Ren, W., & Zhu, X. (2024). The age-based digital divides in China: Trends and socioeconomic differentials (2010–2020). *Telecommunications Policy*, *48*(3), 102716. https://doi.org/10.1016/j.telpol.2024.102716

Rodríguez, A., Abraham, A., Voxi, O., & Amavilah H. (2021). Using deep learning neural networks to predict the knowledge economy index for developing and emerging economies. *Expert Systems with Applications*, *184*, 115514 https://doi.org/10.1016/j.eswa.2021.115514

Souza, J. (2018). *Ralé brasileira: quem é e como vive*. Belo Horizonte: Editora UFMG.

Wang, Q., Hu, S., & Li, R. (2024). Could information and communication technology (ICT) reduce carbon emissions? The role of trade openness and financial development. *Telecommunications Policy*, *48*(3), 102699. https://doi.org/10.1016/j.telpol.2023.102699

Wang, S., & Zhang, H. (2024). Inter-Organizational cooperation in digital green supply chains: a catalyst for Eco-Innovations and sustainable business practices. *Journal of Cleaner Production*, *472*, 143383. https://doi.org/10.1016/j.jclepro.2024.143383

Информация об авторах



Беликова Ксения Михайловна – доктор юридических наук, профессор, профессор кафедры предпринимательского и корпоративного права, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
Адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, 9
E-mail: BelikovaKsenia@yandex.ru
ORCID ID: https://orcid.org/0000-0001-8068-1616
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57193239710
WoS Researcher ID: https://www.webofscience.com/wos/author/record/N-3126-2016
Google Scholar ID: https://scholar.google.ru/citations?user=H58vKS4AAAAJ&hl=ru
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=497601



Диас Мартинс Рафаэл – кандидат юридических наук, разработчик программного обеспечения Интерсистемас, адвокат (OAB/RN 15.923)
Адрес: 9067-400, Бразилия, Натал/РН, 2885 – Питимбу, просп. Каиапос, 5
E-mail: martins.rafael@mail.ru
ORCID ID: https://orcid.org/0009-0001-9397-8694



Казанба Евгений Тенгизович – аспирант, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА); главный юрисконсульт, ФГКУ «Центральное территориальное управление имущественных отношений» Министерства обороны России
Адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, 9
E-mail: ekazanba@gmail.com
ORCID ID: https://orcid.org/0009-0006-6242-5735

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: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 8 июля 2024 г.
Дата одобрения после рецензирования – 22 июля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:341:004.4
EDN: https://elibrary.ru/ocdmla
DOI: https://doi.org/10.21202/jdtl.2024.47

International Cooperation in Overcoming Digital Inequality: Legal Frameworks, Barriers and Development Parameters

Ksenia M. Belikova
Kutafin Moscow State Law University, Moscow, Russia

Rafael Dias Martins
Intersystemas, Natal, Brazil

Evgeniy T. Kazanba
Kutafin Moscow State Law University, Moscow, Russia

Keywords

availability of technologies,
digital divide,
digital inequality,
digital space,
digital technologies,
international cooperation,
international law,
Internet,
law,
legislation

Abstract

Objective: based on a systematic analysis of the actual level of international cooperation in overcoming digital inequality, to determine the parameters of its further development, taking into account modern legal and other barriers and global challenges caused by the transition from the knowledge economy to the data economy.

Methods: the methodological basis of the research is represented by dialectics, comparative legal and historical legal approaches, and the method of system analysis.

Results: the problem of digital inequality was considered in the following key aspects: access to the Internet; differences in the level of digital literacy; features of technology use and the versatility of digital inequality. It is noted that access to the Internet and digital technologies should become one of the fundamental human rights in order to ensure equal opportunities for all segments of society, since initially the crystallization of clearly expressed digital differences is based on the existing offline social differences. It was established that, in order to successfully overcome digital inequality, the key global task is to develop digital skills and literacy among the population. It is also important to stimulate the rational use

Corresponding author
© Belikova K. M., Dias Martins R., Kazanba E. T., 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.

of technologies and ensure people's understanding of working with both the technologies and the data obtained through them. The authors propose to expand and deepen cooperation between developed and developing countries so that the latter can produce more data that may serve as a metric and a basis for creating development strategies. At the same time, greater transparency should be ensured by providing effective and accessible means so that the data owner can clearly understand who and why processes their personal data. The article argues that the transition from the knowledge economy to the data economy requires the adaptation of international cooperation strategies to ensure equitable access to both data and their processing. This may accelerate scientific discoveries and support inclusive economic development. The issues of fragmentation and defragmentation of international law are analyzed.

Scientific novelty: it is due to the current lack of scientific results concerning the level of international cooperation achieved so far in overcoming digital inequality given the parameters of its systemic development and the main (legal and other) barriers.

Practical significance: the study results can be used to improve the legal framework and strategies for international cooperation in overcoming digital inequality to ensure equitable access to data and their processing.

For citation

Belikova, K. M., Dias Martins, R., Kazanba, E. T. (2024). International Cooperation in Overcoming Digital Inequality: Legal Frameworks, Barriers and Development Parameters. *Journal of Digital Technologies and Law, 2*(4), 1003–1030. https://doi.org/10.21202/jdtl.2024.47

References

Cinnamon, J. (2019). Data inequalities and why they matter for development. *Information Technology for Development*, *26*(2), 214–233. https://doi.org/10.1080/02681102.2019.1650244

Du, Z., & Wang, Q. (2024). Digital infrastructure and innovation: Digital divide or digital dividend? *Journal of Innovation & Knowledge*, *9*(3), 100542. https://doi.org/10.1016/j.jik.2024.100542

Ershova, I. V., Laptev, V. A., Andreeva, L. V., Akhrem, T. P., Besedin, A. N., Belikova, K. M., Gabov, A. V., Galkin, S. S., Drueva, A. A., Elnikova, | E. V., Enkova, E. E., Kantor, N. E., Korotkova, O. V., Lebedev, A. V., Mikryukov, V. A., Petrakov, A. Yu., Sajdasheva, M. V., Svit, Yu. P. … Shherbakova, M. A. (2024). *Law and the real sector of the Russian economy*. Moscow: Prospekt. (In Russ.). https://doi.org/10.31085/9785392407354-2024-480

Gallardo, R., & Whitacre, B. (2024). An unexpected digital divide? A look at internet speeds and socioeconomic groups. *Telecommunications Policy*, *48*(6), 102777. https://doi.org/10.1016/j.telpol.2024.102777

Gladkova, A. A., Garifullin, V. Z., Ragnedda, M. (2019). Model of Three Levels of the Digital Divide: Current Advantages and Limitations (Exemplified by the Republic of Tatarstan). *Moscow University Journalism Bulletin*, *4*, 41–72. (In Russ.). https://doi.org/10.30547/vestnik.journ.4.2019.4172

Gritsenko, D. (2023). Advancing UN digital cooperation: Lessons from environmental policy and governance. *World Development*, *173*, 106392. https://doi.org/10.1016/j.worlddev.2023.106392

Johnson, D. R., & Post, D. G. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Kuo-Hsun, J., Ma. (2022). *Digital learning divide. In International Encyclopedia of Education* (4th Ed., pp. 157–164). https://doi.org/10.1016/b978-0-12-818630-5.01013-7

Li, P., Li, Q., & Li, X. (2024). The influence of three digital divide levels on financial advisor demand and engagement among Chinese residents: An investigation based on China. *Journal of Innovation & Knowledge*, *9*(2), 100488 https://doi.org/10.1016/j.jik.2024.100488

Liu, N., Qian, Y., Gu, X., & Li, G. (2024). Digital technology, e-commerce, and economic inequality: The case of China. *International Review of Economics & Finance*, *91*, 259–271. https://doi.org/10.1016/j.iref.2024.01.016

Perfilieva, O. V. (2007). Getting over Digital Divide: the international organizations contribution. *International Organisations Research Journal*, *2*(2), 34–49. (In Russ.).

Polyakov, L. V., Ankudinov, I. A., Egorov, V. Yu., Lyatsos, A. D., & Ryzhkin, E. N. (2022). Green Russia of the future: economic problems and political prospects. *Biznes. Obshhestvo. Vlast*, 46, 87–116. (In Russ.).

Pool, H., Schuyler, T., Senf, T. M., & Moschovitis, Ch. J. P. (1999). *History of the Internet. A Chronology, 1843 to Present*. London: ABC-CLIO.

Rabbani, M. (2024). Internet price, speed, and disparity: The case of rural healthcare providers in the United States. *Telecommunications Policy*, *48*(2), 102674. https://doi.org/10.1016/j.telpol.2023.102674

Reidenberg, J. R. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, *76*, 553.

Ren, W., & Zhu, X. (2024). The age-based digital divides in China: Trends and socioeconomic differentials (2010–2020). *Telecommunications Policy*, *48*(3), 102716. https://doi.org/10.1016/j.telpol.2024.102716

Rodríguez, A., Abraham, A., Voxi, O., & Amavilah H. (2021). Using deep learning neural networks to predict the knowledge economy index for developing and emerging economies. *Expert Systems with Applications*, *184*, 115514 https://doi.org/10.1016/j.eswa.2021.115514

Souza, J. (2018). *Ralé brasileira: quem é e como vive*. Belo Horizonte: Editora UFMG. (in Portuguese).

Trubilin, A. G., & Zolotukhina, A. D. (2022). The elimination of illiteracy is the largest social and educational project in the history of Russia. *International Journal of Humanities and Natural Sciences*, *12-5*(75), 16–21. (In Russ.).

Wang, Q., Hu, S., & Li, R. (2024). Could information and communication technology (ICT) reduce carbon emissions? The role of trade openness and financial development. *Telecommunications Policy*, *48*(3), 102699. https://doi.org/10.1016/j.telpol.2023.102699

Wang, S., & Zhang, H. (2024). Inter-Organizational cooperation in digital green supply chains: a catalyst for Eco-Innovations and sustainable business practices. *Journal of Cleaner Production*, *472*, 143383. https://doi.org/10.1016/j.jclepro.2024.143383

Authors information



Ksenia M. Belikova – Dr. Sci. (Law), Professor, Department of Entrepreneurial and Corporate Law, Kutafin Moscow State Law University
Address: 9 Sadovo-Kudrinskaya Str., 125993 Moscow, Russia
E-mail: BelikovaKsenia@yandex.ru
ORCID ID: https://orcid.org/0000-0001-8068-1616
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57193239710
WoS Researcher ID: https://www.webofscience.com/wos/author/record/N-3126-2016
Google Scholar ID: https://scholar.google.ru/citations?user=H58vKS4AAAAJ&hl=ru
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=497601



Rafael Dias Martins– PhD (Law), software developer, Intersystemas, lawyer (OAB/RN 15.923)
Address: ave. Caiapos, 2885 - Pitimbu, Natal/PH, 59067-400, Brazil
E-mail: martins.rafael@mail.ru
ORCID ID: https://orcid.org/0009-0001-9397-8694



Evgeniy T. Kazanba – post-graduate student, Kutafin Moscow State Law University; Chief Legal Adviser of the Federal State Budgetary Institution “Central Territorial Administration of Property Relations” of the Ministry of Defense of the Russian Federation
Address: 9 Sadovo-Kudrinskaya Str., 125993 Moscow, Russia
E-mail: ekazanba@gmail.com
ORCID ID: https://orcid.org/0009-0006-6242-5735

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 – July 8, 2024
Date of approval – July 22, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:346.6:004.8
EDN: https://elibrary.ru/gnqswz
DOI: https://doi.org/10.21202/jdtl.2024.48

Правовые аспекты защиты персональных данных и проблемы конкуренции на цифровых рынках

Афувапе Колаволе

Глобальный университет имени О. П. Джиндала, Сонипат, Индия

Ключевые слова

антимонопольное законодательство,
защита персональных данных,
злоупотребление данными,
конкурентное право,
конфиденциальность,
права потребителей,
право,
цифровые платформы,
цифровые рынки,
цифровые технологии

Аннотация

Цель: разработка подходов и предложений по совершенствованию правовых механизмов защиты персональных данных в условиях развивающегося характера цифровых рынков и роста цифровой конкуренции.

Методы: статья подготовлена на основе формально-юридического и сравнительно-правового методов исследования.

Результаты: показаны уникальные особенности цифровых рынков, которые необходимо учитывать для достижения целей антимонопольного законодательства. Отмечается, что основополагающими элементами цифрового рынка являются концепция больших данных и аналитики больших данных, которые на основе цифровых платформ способны производить многие прямые и косвенные сетевые эффекты, требующие понимания для эффективного антимонопольного реагирования и применения соответствующего законодательства. Рост цифровых платформ как бизнес-модели и жизненно важной инфраструктуры цифровой экономики рассмотрен как фактор совершенствования мер правового регулирования отношений, связанных с защитой данных и конфиденциальностью. Определен потенциал в сфере цифровых платформ показателей оценки сложившейся рыночной силы и влияния потенциальной конкуренции на ограничение этой силы. Данные рассмотрены как неотъемлемый компонент общего конкурентного ландшафта на рынке. Анализу подвергнуто действующее в Европейском союзе правовое регулирование в сфере функционирования цифровых платформ и защиты персональных данных. Выявлены трудности, связанные с созданием и применением эффективных нормативных актов, регулирующих деятельность цифровых платформ. Обоснована необходимость изменения антимонопольными органами подходов к аналитике с тем, чтобы учесть

© Колаволе 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.

отличительные особенности цифровых платформ. Отмечено, что такие изменения могут потребовать законодательных реформ и пересмотра процедур, чтобы соответствовать быстрому развитию этих рынков и обеспечить тщательное изучение любого потенциально антиконкурентного поведения.

Научная новизна: проведенное исследование вносит вклад в разработку подходов к определению показателей обеспечения конфиденциальности персональных данных в условиях цифровизации рынков и оценке эффективности антимонопольного законодательства и практики его применения в новой конкурентной среде.

Практическая значимость: полученные результаты могут быть положены в основу совершенствования антимонопольного законодательства и законодательства в сфере защиты персональных данных, а также правового регулирования деятельности цифровых платформ в целом.

Для цитирования

Колаволе, А. (2024). Правовые аспекты защиты персональных данных и проблемы конкуренции на цифровых рынках. *Journal of Digital Technologies and Law*, *2*(4), 1031–1053. https://doi.org/10.21202/jdtl.2024.48

Содержание

Введение
1. Данные как неотъемлемый компонент общего конкурентного ландшафта на рынке
2. Цифровая трансформация экономики и появление «релевантного рынка» в цифровой среде
3. Концептуальные основы рыночной силы и доминирования
4. Эволюция европейского антимонопольного законодательства
5. Управление цифровыми технологиями и данными: этические и нормативные меры
   5.1. Закон о цифровых рынках
   5.2. Закон о цифровых услугах
   5.3. Закон об управлении данными
6. Проблемы регулирования в сфере цифрового рынка
Заключение
Список литературы

Введение

Цифровизация существенно трансформировала конкурентную среду в мировой экономике, создав новые рынки и изменив существующие (Knudsen et al., 2021). В результате такого развития событий перед антимонопольными органами стоит сложная задача. Они вынуждены бороться с новыми формами правонарушений, исследовать рынки с неясными границами и преодолевать неопределенность,

присущую быстро меняющимся рынкам[1]. Ситуация на цифровых рынках и показатели роста рыночной силы побуждают как создавать новые, так и более активно применять уже существующие инструменты регулирования конкуренции (Budzinski & Stöhr, 2019).

Деловые практики управления данными стали объектом повышенного внимания со стороны антимонопольных органов и организаций, регулирующих защиту данных (Lancieri, 2019). Динамика развития цифровых рынков оказывает значительное влияние на конфиденциальность данных, поскольку многие бизнес-модели основаны на массовом получении персональных данных (Bandara et al., 2021). На основе этих данных создаются индивидуальные профили, содержащие конфиденциальные сведения о личной жизни. Поэтому органы по защите данных уделяют особое внимание оценке эффективности и достаточности законодательной базы, регулирующей обработку таких персональных данных (Buckley et al., 2024).

Несколько десятилетий цифровые платформы бурно развивались как важнейший элемент инфраструктуры цифровой экономики и ее ключевая бизнес-модель. Однако теперь ученые и регуляторы конкурентной политики начинают рассматривать их как угрозу (Nuccio & Guerzoni, 2019). Некогда господствовавший консенсус о том, что традиционные законы не должны сдерживать развитие цифровой экономики, быстро уступил место новой стратегии, характеризующейся более активным вмешательством (Manne, 2020).

Данная статья вносит теоретический и эмпирический вклад в поиск методов количественной оценки рыночной силы. Автор рассматривает ряд вопросов, связанных с разработкой масштабных планов по защите и улучшению конкуренции на цифровых рынках. Оценка рыночной силы в современных цифровых контекстах является одной из основных областей, представляющих интерес для исследования эффективного антимонопольного реагирования и применения антимонопольного законодательства в этой области.

1. Данные как неотъемлемый компонент общего конкурентного ландшафта на рынке

Цифровые платформы способны использовать данные таким образом, что это может быть расценено как злоупотребление; однако данные также оказывают влияние на доминирование компании на рынке (Robertson, 2020). В современных бизнес-моделях на основе платформ данные стали важнейшим ресурсом, а умение использовать их для создания новых и инновационных товаров и услуг служит значительным конкурентным преимуществом (Mariani & Wamba, 2020). Основная проблема, связанная с данными в контексте оценки доминирования компании на рынке, заключается в их применении и неоднозначном характере их ценности, что создает проблемы для ценовых инструментов, используемых для такой оценки (Sznajder, 2021). Ценность данных не является фиксированной. Напротив, истинный потенциал кроется в знаниях, которые можно извлечь из набора данных, и для компании крайне важно эффективно использовать этот потенциал. Простого

[1] Popiel, P. (2020). Emergent Governance: The Politics of Competition in Digital Markets: Doctoral dissertation. University of Pennsylvania.

накопления или сохранения массивов данных со временем будет недостаточно, поскольку они устаревают. Необходим постоянный сбор данных и доступ к ним, а также алгоритмы, способные использовать информацию, заложенную в данных (Adadi, 2021). Следовательно, платформы заинтересованы в том, чтобы удерживать пользователей на своих сервисах. Однако крупные сборщики данных редко занимаются продажей баз данных; отсюда отсутствие реального спроса и предложения на данные, которые можно было бы использовать в анализе рынка. Растущая зависимость от данных в рамках бизнес-моделей на основе платформ и создания платформенных товаров и услуг привела к отходу от традиционных стратегий ценообразования (Kretschmer et al., 2022). Таким образом, данные стали важным элементом, который необходимо учитывать при анализе рыночного доминирования на разных этапах. Влияние данных на конкуренцию и рыночную силу может проявляться по-разному, в зависимости от их применения; однако их необходимо рассматривать как неотъемлемый компонент общего конкурентного ландшафта на рынке.

Применение данных существенно влияет на поведение на рынках, поскольку усиливает такие характеристики, как сетевые эффекты, удержание клиентов и издержки переключения, особенно на платформенных рынках (Cen & Li, 2020). Например, как только платформа на основе социальной сети набирает значительную пользовательскую базу, она становится привлекательной для потенциальных индивидуальных пользователей, стремящихся взаимодействовать с существующими членами (прямые сетевые эффекты), и для коммерческих организаций (приносящих доход), которые могут рекламировать товары и услуги с помощью контента или целевых объявлений на платформе (косвенные сетевые эффекты). Пользователи могут столкнуться с проблемами при переключении между платформами, взаимодействии с несколькими социальными сетями (мультихоминг) или с отсутствием совместимости между сервисами в рамках экосистемы, что может привести к эффекту удержания (Pervin et al., 2019). Следовательно, присущие этим рынкам особенности могут быть использованы для удержания пользователей на платформе, что облегчает непрерывный сбор данных. Эти показатели влияют как на способность компаний налагать конкурентные ограничения друг на друга, так и на размер соответствующих долей рынка.

2. Цифровая трансформация экономики и появление «релевантного рынка» в цифровой среде

В соответствии со ст. 102 Договора о функционировании Европейского союза (Treaty on the Functioning of the European Union, TFEU) целью определения границ рынка, а также последующего исследования рыночной силы являются установление и определение пределов конкуренции между компаниями (Andriychuk, 2023a). Это подразумевает определение того, есть ли у потенциально доминирующего субъекта реальные конкуренты, которые могут ограничить его поведение на рынке, учитывая, что субъект не сможет работать без существенного конкурентного давления, что может негативно сказаться на потребителях. В рамках антимонопольного законодательства ЕС для оценки пороговых значений доли рынка и рыночной силы используется понятие релевантного рынка, что создает экономический контекст для конкретных судебных дел и определяет теоретическое понимание конкурентного вреда. Определение рынка опирается на оценки замещаемости, которые играют важную роль в выявлении соответствующего антимонопольного товарного

рынка (Parker et al., 2020). Эти оценки были разработаны в контексте статичных рынков. Хотя определение рынка представляет собой лишь один из этапов анализа доминирующего положения, оно играет решающую роль в оценке рыночной силы, поскольку определяет широту рынка. От этого определения впоследствии зависит легкость или трудность достижения доминирующего положения на этом рынке. Основная цель определения рынка заключается в том, чтобы сделать выводы о степени рыночной силы.

Однако развивающийся характер цифровых рынков значительно усложняет процесс определения соответствующего рынка. Цифровые рынки обладают рядом особых характеристик, которые отличают их от обычных статичных рынков. Эти уникальные особенности необходимо учитывать при определении соответствующих товарных рынков для целей антимонопольного законодательства. К числу ключевых характеристик относятся быстрая эволюция цифровых рынков, наличие рынков или сегментов рынка с нулевыми ценами, динамика «победитель получает все», наблюдаемая в некоторых цифровых секторах, тенденция к перелому рынка на основе цифровой платформы из-за сетевых эффектов, что может привести к удержанию пользователей, и конкуренция за сам рынок, которая является заметным аспектом конкуренции в цифровой среде.

Концепции больших данных и аналитики больших данных служат основополагающими элементами цифрового рынка, что приводит к необходимости глубоких знаний в этой сфере (Perera & Iqbal, 2021). Кроме того, платформы часто называют многосторонними рынками, и соответствующая превалирующая бизнес-модель требует глубокого понимания прямых и косвенных сетевых эффектов, лежащих в основе таких платформ (Dunne, 2021). Вместе с платформами развиваются цифровые экосистемы, что может удержать потребителей и снизить конкуренцию (Jenny, 2021). Это явление тесно связано с растущей тенденцией к созданию конгломератных корпоративных структур. Цифровая трансформация экономики привела к появлению рынков, на которых идентичные или сопоставимые товары можно приобрести как офлайн, так и онлайн, например, напечатанные книги в реальном магазине или электронные книги в онлайн-магазине (Ratchford et al., 2022). Такая ситуация заставляет задуматься о том, происходит ли слияние онлайн- и офлайн-рынков или их следует рассматривать как отдельные релевантные рынки. В сценариях, когда одна из сторон рынка приобретает услуги в обмен на данные, а не напрямую за деньги, обычные экономические методики определения рынков оказываются неприменимыми. Следует подчеркнуть, что цифровые платформы широко распространены в цифровом ландшафте. Эти платформы функционируют как посредники, облегчая взаимодействие между несколькими участниками рынка, что характеризует их как «многосторонние рынки». Альтернативная точка зрения заключается в том, чтобы рассматривать каждую сторону рынка как отдельный релевантный антимонопольный рынок. Однако экономисты утверждают, что изолированная оценка сторон платформенного рынка не позволяет отразить всю динамику цифровых платформ. Такая точка зрения упускает из виду важнейшие моменты, необходимые для эффективного антимонопольного анализа. И наоборот, определение релевантного рынка как включающего всю платформу, может оказаться чрезмерно широким для обычной антимонопольной оценки, потенциально охватывая рынки, которые не являются взаимозаменяемыми (Bietti, 2024). Такой подход потребует существенных изменений в применении антимонопольного законодательства в отношении определения рынка.

3. Концептуальные основы рыночной силы и доминирования

Значительные колебания рыночной капитализации доказывают огромный потенциал, заложенный в компаниях на основе экосистем. Крупнейшие технологические компании, известные как GAFAM (Google (Alphabet), Apple, Facebook[2], Amazon и Microsoft), стратегически использовали платформы и экосистемы для установления своего доминирования на рынке, о чем свидетельствует их значительная рыночная капитализация (Lianos & McLean, 2021). Примечательно, что эти компании не только вытеснили традиционных лидеров, таких как крупные нефтяные компании, промышленные конгломераты и финансовые институты, но и укрепили свои позиции, продемонстрировав значительный рост как в абсолютных, так и в относительных показателях. Их суммарная рыночная капитализация, еще более возросшая вследствие пандемии COVID-19, сейчас превышает 1 трлн долларов (Liang & Whalen, 2022).

Обширный рынок капитала имел значительные последствия, среди которых подрыв важнейшего преимущества устоявшихся компаний в период быстрых преобразований, а именно инертности. Ранее запасы наличности и капитала, которыми располагали действующие компании, ограничивали потенциал роста их конкурентов. Затем ситуация существенно изменилась, поскольку доминирующим механизмом распределения капитала стали фондовые рынки. На этот сдвиг в значительной степени повлияли условия низких процентных ставок в начале XXI в., появившиеся в результате нетрадиционной монетарной политики и последствий мирового финансового кризиса. Как следствие, излишки капитала требовали возможностей для инвестиций, поэтому любое предприятие с потенциалом роста могло быстро получить финансирование. Таким образом, инвестиции в новые платформы и экосистемы, такие как цифровая экономика, привлекли значительные финансовые ресурсы. Новые предприятия стали востребованы теми самыми действующими компаниями, которых они стремились вытеснить, и смогли переломить традиционную динамику рыночной силы в рамках сложившихся секторов экономики.

Учитывая, что рост является приоритетным показателем для рынков капитала, эти компании ориентируются на расширение, а не на быстрое получение прибыли, тем самым нарушая привычную динамику развития соответствующих секторов. Развивающийся ландшафт производящей экономики приобретает свои характерные черты, особенно по мере того, как все большее значение придается программному обеспечению. Примечательным аспектом является непропорционально высокое соотношение постоянных и переменных затрат. Процесс кодирования составляет значительную часть инноваций, а после разработки стоимость тиражирования минимальна. Такая динамика способствует возникновению конкурентной среды, в которой на рынке может доминировать один субъект. Взаимодействие тенденций глобализации и цифровизации значительно расширило понятие «релевантный рынок», тем самым подчеркнув важность этих явлений. Это расширение еще более усиливается за счет экономии на масштабе и обучении, поскольку данные пользователей могут применяться в различных контекстах, а не ограничиваться одним приложением.

---

[2] Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Концепция социальной рыночной экономики и возможности регулирующего вмешательства

Рыночная сила служит важнейшим критерием для регулятивного вмешательства в рамках европейской социальной рыночной экономики. Чтобы полностью понять значение рыночной силы в этом контексте, необходимо сначала определить концепцию социальной рыночной экономики. Основной задачей Европейского союза является создание внутреннего рынка, функционирующего на принципах высококонкурентной социальной рыночной экономики, как это сформулировано в ст. 3(3) Договора о функционировании Европейского союза (TFEU) (Gerstenberg, 2020).

Концепция социальной рыночной экономики понимается как интеграция экономических принципов свободного рынка в рамках подхода, который ставит во главу угла социальное благосостояние. В условиях свободного рынка фирма, получающая максимальную прибыль, обычно стремится установить цены на максимально возможном уровне (Mascarenhas et al., 2024). Однако наличие конкурентных сил не позволяет компании устанавливать цены, превышающие цены их конкурентов, поскольку потребители, скорее всего, предпочтут покупать товары у компаний, предлагающих более низкие цены. Следовательно, фирмы будут либо поддерживать цены на уровне конкурентного порога, либо стремиться к повышению качества своих товаров и услуг по сравнению с конкурентами. В условиях свободной рыночной экономики вмешательство регулирующих органов в торговлю считается излишним, поскольку присущая свободному рынку динамика способствует эффективной конкуренции. Эта конкуренция функционирует как естественный саморегулирующийся механизм, который поддерживает рыночное равновесие (Texocotitla et al., 2017).

Критика свободной рыночной экономики привела к появлению концепции социальной рыночной экономики. В основном социальная рыночная экономика признает основные постулаты системы свободного рынка. Однако, по нашему мнению, она также подчеркивает необходимость регулирующего вмешательства для поддержания социального равновесия. Это может быть достигнуто, например, путем обеспечения доступности основных услуг или регулирования антиконкурентного поведения фирм, которые могут действовать независимо как от конкурентов, так и от потребителей. В этом контексте регулирующее вмешательство в социальную рыночную экономику служит защитным механизмом, обеспечивающим функционирование рынка с ожидаемой эффективностью.

Важно также определить надлежащий уровень вмешательства государственных органов. Чрезмерное регулирование может препятствовать автономии личности в обществе и потенциально нарушать рыночную конкуренцию. И наоборот, недостаточные меры регулирования могут способствовать антиконкурентному поведению и привести к несправедливому распределению основных услуг, как уже говорилось ранее. Следовательно, определение надлежащего уровня регулирующего вмешательства имеет решающее значение для эффективного функционирования рынка. В связи с этим при рассмотрении вопроса о необходимости экономического вмешательства государственные органы устанавливают конкретные меры, включая защиту услуг, представляющих общеэкономический интерес, защиту прав интеллектуальной собственности и поддержание конкурентной среды, не позволяющей предприятиям злоупотреблять своей рыночной силой. Рыночная сила существует в диапазоне от совершенной конкуренции, характеризующейся отсутствием

рыночной силы, до монопольной власти, где критическая точка для доминирования компании определяется как «значительная рыночная сила». Такое доминирование подразумевает, что организация может действовать в значительной степени независимо от своих конкурентов, клиентов и в конечном счете потребителей. Хотя многосторонние цифровые платформы могут столкнуться с реальной конкуренцией, динамика рынка часто существенно ограничена угрозой потенциальной конкуренции. Обладание обширными массивами данных и возможностью их сбора могут увеличить рыночную силу, создавая барьеры для входа конкурентов, не имеющих доступа или возможности собирать сопоставимые данные. Кроме того, эти платформы могут получать преимущества за счет сопутствующих экономических элементов, таких как сетевые эффекты и издержки переключения.

4. Эволюция европейского антимонопольного законодательства

В международном регулировании рынка цифровых платформ прослеживаются общие темы, особенно в вопросах, касающихся контента, данных и концентрации рыночной силы (Cammaerts & Mansell, 2020). На эту согласованность во многом влияет глобальный охват крупнейших компаний-платформ и постоянные совместные дискуссии между регулирующими органами разных стран. Каждый субъект, занимающийся экономической деятельностью, подпадает под действие антимонопольного законодательства. Основная цель этой законодательной базы – поддержание и развитие конкурентных процессов, которые позволят наиболее эффективно распределять ресурсы и защищать экономические свободы различных участников рынка. Методы правоприменения, которые варьируются в зависимости от юрисдикции, призваны защитить от экономического ущерба (который может проявляться в виде негативного воздействия на такие элементы, как ценообразование, качество, выбор потребителя или инновации) и гарантировать, что компании конкурируют на основе своих естественных преимуществ.

Основная цель конкурентной политики – гарантировать, что действия компаний, безотносительно к тому, являются ли они независимыми, совместными или результатом слияния, не будут препятствовать какому-либо экономическому аспекту благосостояния потребителей или общего экономического благосостояния, а также конкурентной среды. Следовательно, конкурентная политика служит для защиты «общественных интересов» на конкурентных рынках, затрагивая права личности косвенным образом, в отличие от политики конфиденциальности данных.

Во многих странах мира были предложены или приняты законодательные изменения, направленные на решение проблем, связанных с цифровой конкуренцией. Эти изменения предполагают введение новых норм априори, призванных усилить меры по обеспечению соблюдения законодательства на цифровых рынках постфактум. Наряду с предложениями, направленными на совершенствование существующих основ конкурентной политики, было выдвинуто несколько рекомендаций по созданию новых законодательных и регулирующих органов априори.

Европейский союз, опираясь на развитую нормативно-правовую базу, стал лидером в области регулирования цифровых платформ. Существует ряд важных реформ, которые необходимо внимательно изучить с точки зрения их реализации и последствий. Среди них готовящийся к принятию Закон о цифровых услугах (Digital Services Act, DSA), направленный на повышение безопасности в Интернете

и борьбу с нелегальным контентом, а также Закон о цифровых рынках (Digital Markets Act, DMA), призванный стимулировать конкуренцию на концентрированных платформенных рынках. Попытки регулирования интернет-платформ имеют многогранный и стратегический характер. В них в первую очередь воплощаются нормативные и идеологические постулаты, лежащие в основе нормативно-правовой базы, контролирующей экономику платформ. Кроме того, эта деятельность часто является результатом противоречивых политических интересов, в частности интересов крупных компаний-платформ. В результате такая динамика приводит к напряженности и компромиссам, которые неизбежны при регулировании цифровых рынков. В Соединенных Штатах Америки выдвигается ряд законодательных инициатив, направленных на обеспечение конфиденциальности данных и развитие конкуренции. Среди них следует отметить Американский закон об инновациях и выборе в Интернете (American Innovation and Choice Online Act, AICOA), Закон об открытых рынках приложений и Американский закон о конфиденциальности и защите данных (American Data Privacy and Protection Act, ADPPA). Соединенное Королевство после выхода из ЕС продолжает реализовывать независимую политику, внедряя новое законодательство и инициируя расследования в области безопасности в Интернете, защиты потребителей и конкуренции. Эту инициативу возглавляют совместно Управление по конкуренции и рынкам (Competition and Markets Authority, CMA), Управление комиссара по информации (Information Commissioner's Office, ICO), а также другие значимые регулирующие органы.

Понимание нюансов и практических последствий этих развивающихся правовых подходов становится все более важным. Эскалация регулятивных мер создает возможность дублирования и конфликта правоприменительных действий. Ожидается, что по мере того, как корпорации и регулирующие органы будут пытаться адаптироваться к этим новым требованиям, число судебных разбирательств будет расти.

5. Управление цифровыми технологиями и данными: этические и нормативные меры

Дискуссия об управлении в цифровой сфере обширна и охватывает множество аспектов, которые еще предстоит понять и теоретически осмыслить. Ключевым моментом является то, что управление, этические соображения и регулятивные меры, относящиеся к цифровой среде, регулируются отдельными нормативными актами. Эти системы дополняют друг друга, и их не следует путать, напротив, необходимо их четко разделять.

Управление цифровыми технологиями включает в себя организацию разработки и внедрения законодательства, процедур и стандартов, призванных способствовать эффективному развитию, использованию и управлению информационной средой. Эта практика включает в себя установленные конвенции и эффективную координацию, функционируя в сфере, которая не поддается прямой классификации на моральную или аморальную, а также законную или незаконную. Цифровое управление – это система принципов и предположений, которые могут пересекаться с цифровым регулированием; однако они не идентичны. Это понятие можно интерпретировать как обсуждение соответствующих правовых рамок, которые состоят из набора нормативных актов, установленных и внедренных общественными или

государственными органами для регулирования поведения соответствующих субъектов в инфосфере. Важно отметить, что не все аспекты цифрового регулирования охватываются цифровым управлением и, наоборот, не все элементы цифрового управления связаны с цифровым регулированием. Примером такого разграничения может служить Общий регламент по защите данных. Отношения соответствия служат основополагающим механизмом, с помощью которого цифровое регулирование влияет на цифровое управление.

Цифровая этика – это область этики, которая изучает и оценивает моральные дилеммы, связанные с данными и информацией, охватывая такие аспекты, как их создание, запись, хранение, обработка, распространение, обмен и использование. Она также включает изучение алгоритмов, в том числе искусственного интеллекта, искусственных агентов, машинного обучения и робототехники, а также соответствующих практик и инфраструктур, таких как ответственные инновации, программирование, хакерство, профессиональные кодексы и стандарты. Цель состоит в том, чтобы разрабатывать и отстаивать морально обоснованные решения. Цифровая этика влияет на рамки цифрового регулирования и управления, оценивая моральные нормы, определяющие то, что считается социально приемлемым или желательным. Основная проблема современного общества заключается в управлении цифровыми технологиями. Это включает в себя не только рамки цифрового управления, но и принципы цифровой этики и механизмы цифрового регулирования, что позволяет охватить весь спектр соображений в нормативной сфере.

Цифровое регулирование очерчивает границы допустимых и недопустимых действий в цифровом ландшафте, однако оно не дает указаний относительно оптимальных или наиболее полезных действий, которые можно предпринять в рамках правового поля для достижения общественного прогресса. Эта ответственность лежит на цифровой этике, которая фокусируется на моральных ценностях и предпочтениях, а также на эффективном цифровом управлении, которое делает акцент на практике управления. На этом подходе основано создание в 2015 г. независимого органа ЕС по защите данных – Консультативной группы по этике Европейского надзорного органа по защите данных (Ethics Advisory Group by the European Data Protection Supervisor, EDPS). Задача группы – изучать возникающие этические проблемы, связанные с развитием цифровых технологий и существующими правовыми рамками, в частности с GDPR.

Законодательные меры в области защиты данных предлагают ограниченный подход к решению проблем, связанных с неправомерным использованием конфиденциальности и данных пользователей. Это ограничение обусловлено тем, что в нем не учитываются возможные долгосрочные последствия для пользователей цифровых платформ, значительная рыночная сила, которой обладают конкретные платформы, и особые обязательства, которые вытекают из такой силы. В этой связи законодательство о защите данных может выиграть от добавления понятий эксплуатации и исключения, которые встречаются в антимонопольном законодательстве.

Платформа может намеренно снижать интенсивность положительных сетевых эффектов или ухудшать качество услуг, которые она предоставляет пользователям, по крайней мере, с одной стороны. Такое поведение может быть истолковано как признак рыночной силы. В отсутствие такой рыночной силы платформа, как правило, добивается большего успеха, когда сетевые эффекты устойчивы,

а качество услуг высокое. В ситуациях злоупотребления намеренные нарушения – особенно манипуляции с алгоритмами поиска или подбора – могут служить барометром рыночного доминирования. Эта идея поддерживает основную идею рыночной силы, которая была рассмотрена ранее, т. е. предполагает, что определенное поведение на рынке может указывать на существование рыночной силы или даже рыночного доминирования. Изначально может показаться неожиданным начать этот дискурс с концепции согласия, а не адекватности, однако на сегодняшний день эта методология доказала свою применимость в международных инициативах в области геномики. Прежде всего, исследователи, как правило, обязаны получать согласие участников на проведение биомедицинских исследований, что позволяет без особых усилий распространить это согласие на передачу данных участников в международном масштабе. Кроме того, широкое согласие для целей исследований признается европейским законодательством и подкрепляется Общим положением о защите данных (General Data Protection Regulation, GDPR) (пункт 33 Преамбулы). Наконец, формула согласия предлагает последовательную структуру, тем самым снижая уровень непоследовательности при принятии таких мер, как решения об адекватности. Подобные меры вряд ли смогут охватить все исследовательские проекты в рамках консорциума, поскольку он расширяется, включая инициативы в странах, не имеющих адекватной системы защиты данных.

Основания для передачи данных, изложенные в статье 49(1), в частности, те, которые относятся к общественным и законным интересам, значительно более ограничены по сравнению с законными основаниями для обработки данных, содержащимися в статье 6(1). Например, в статье 49(1)(d) прямо указано, что передача данных должна быть необходима по важным причинам, связанным с общественными интересами. Концепция адекватности служит фундаментальным обоснованием для передачи данных в рамках законодательства ЕС о защите данных с момента введения в действие Директивы о защите данных в 1995 г. Хотя решение об адекватности часто рассматривается как наиболее благоприятное и обнадеживающее основание для такой передачи, важно признать три существенных ограничения, связанных с этим подходом. Во-первых, не все страны одобрили это положение[3]. Во-вторых, даже в юрисдикциях, где оно было одобрено, например, в Канаде и США, механизмы определения адекватности ограничены конкретными организациями, управляемыми этими механизмами. Наконец, после основополагающего судебного решения по делу Schrems, которое аннулировало предыдущее положение об адекватности, и в свете требования GDPR о регулярной переоценке этих решений заинтересованные стороны больше не могут считать, что утвержденное решение об адекватности будет действовать бесконечно. В связи с этим австрийский студент Макс Шремс оспорил предыдущее решение Европейской комиссии о том, что рамочная программа Safe Harbour между США и ЕС обеспечивает достаточную защиту данных. Европейский суд прямо указал, что неизбирательное наблюдение является существенным основанием для отмены предыдущего решения об адекватности в деле Schrems[4].

[3] European Commission 2018. https://clck.ru/3FDEBs

[4] European Court of Justice 2015. https://clck.ru/3FDEML

Другой метод соблюдения положений GDPR, касающихся передачи данных, предполагает включение стандартных «типовых положений», получивших предварительное одобрение Комиссии ЕС, в юридически обязательные соглашения между отправителем и получателем данных (статья 45(2)(c)-(d) Общего положения о защите данных). После того как Европейский суд в 2016 г. отменил решение об адекватности системы Safe Harbour между США и ЕС, принятое по делу Schrems, эти оговорки стали важным альтернативным механизмом передачи данных, что было отмечено различными заинтересованными сторонами (Galehr, 2023). Юридически обязательные корпоративные правила (Binding Corporate Rules, BCR), хотя и признаются в качестве предпочтительного обоснования передачи данных в соответствии с Общим положением о защите данных, редко оказываются применимыми в контексте исследований в области геномики (Phillips, 2018). Эти правила предназначены в первую очередь для крупных транснациональных организаций или групп, которые занимаются передачей персональных данных между странами, оставаясь при этом в рамках своих внутренних организационных структур (статья 47 GDPR). Чтобы использовать BCR, организация должна разработать набор правил, соответствующих положениям статьи 47 GDPR, которые затем должны быть утверждены соответствующим органом по защите данных. Такой подход требует значительных первоначальных инвестиций, что зачастую связано со сложностью, временными затратами и высокой стоимостью. Кроме того, этот подход может оказаться не самым удобным механизмом передачи данных, особенно в рамках международных исследовательских проектов в области геномики, в частности тех, в которых участвуют партнерства или консорциумы с отдельными инициативами стран-участниц.

Согласно Общему положению о защите данных, соблюдение организацией отраслевого кодекса поведения, получившего одобрение Европейской комиссии в соответствии с процедурами, изложенными в GDPR (Schütz, 2022), может служить веским основанием для передачи персональных данных этой организации при условии наличия действительных, юридически обязывающих и могущих быть исполненными обязательств по реализации необходимых гарантий. Однако существенным ограничением данного подхода является отсутствие в настоящее время какого-либо кодекса поведения, отвечающего этим критериям.

5.1. Закон о цифровых рынках

Основными правовыми документами, относящимися к Закону о цифровых рынках (Digital Markets Act, DMA), являются Регламент (ЕС) 2022/1925, принятый Европейским парламентом и Советом 14 сентября 2022 г. и направленный на создание конкурентных и справедливых рынков в цифровой сфере, а также Процедурный регламент по его реализации.

Закон о цифровых рынках представляет собой важнейшее достижение в развитии конкурентного права Европейского союза (Petit, 2021). Он опирается на обширный опыт, накопленный Европейской комиссией и Судом Европейского союза, и одновременно постулирует отход от предыдущих методологий. Этот документ знаменует собой новый подход к регулированию цифровых рынков, одновременно точный и ориентированный на соблюдение требований. Важным аспектом этой эволюции являются критические отношения и взаимодействие между Еврокомиссией и Судом Евросоюза. Комиссия отвечает за принятие решений, которые впоследствии подвергаются проверке со стороны Суда, тем самым формируя систему

конкуренции и иллюстрируя концепцию значимости выбора пути развития. Иногда эти изменения происходят фрагментарно, нарушая устоявшуюся практику, а иногда объединяют преемственность и реформы. Закон не следует относить к инициативам в области конкурентного права. Он был принят исключительно в соответствии со статьей 114 Договора о функционировании Европейского союза с целью повышения эффективности функционирования внутреннего рынка. Такое повышение должно быть достигнуто с помощью нормативных актов, способствующих развитию конкуренции и справедливости на цифровых рынках, особенно в отношении основных платформ, управляемых крупнейшими компаниями, как определено в этом Законе. Следовательно, Закон носит регулятивный характер и призван влиять на действия основных платформ с целью способствовать справедливости и конкурентности, дополняя тем самым различные другие нормативно-правовые акты, включая Закон о цифровых услугах.

Одним из основополагающих принципов Закона о цифровых рынках является установление особых обязанностей для доминирующих на рынке платформ. Эти обязанности направлены на развитие справедливой конкуренции и создание сбалансированной среды на цифровом рынке. Например, такие платформы должны разрешить бизнес-пользователям на своих платформах рекламировать свою продукцию и проводить сделки с клиентами за пределами ограничений платформы. Кроме того, Закон о цифровых рынках запрещает доминирующим платформам отдавать предпочтение собственным услугам и продуктам перед услугами и продуктами, предлагаемыми третьими сторонами на их платформах, обеспечивая тем самым более беспристрастную систему ранжирования.

Для того чтобы гарантировать соблюдение указанного закона, были разработаны комплексные стратегии по его обеспечению. Цифровые компании, которые не выполняют установленные обязательства, могут столкнуться с серьезными последствиями. Финансовые штрафы могут достигать 10 % от общемировой годовой выручки компании, а в случае повторных нарушений этот процент может удвоиться, что является сильным сдерживающим фактором. Кроме того, власти могут налагать периодические штрафы в размере 5 % от средней суточной выручки. В тех случаях, когда по результатам рыночных исследований выявляются постоянные нарушения, Закон наделяет регулирующие органы полномочиями по принудительному принятию дополнительных мер по исправлению ситуации. Закон о цифровых рынках служит важнейшим инструментом регулирования, призванным контролировать влияние, оказываемое крупными цифровыми компаниями. Этот закон направлен на создание более справедливого, прозрачного и конкурентного ландшафта на цифровых рынках путем установления и внедрения конкретных стандартов и ограничений для выявленных доминирующих платформ. Закон следует понимать как дополнительный механизм, который не изменяет существующие законы о конкуренции в Европейском союзе. Вместо этого он призван решить уникальные проблемы, возникающие при работе цифровых рынков.

5.2. Закон о цифровых услугах

Закон о цифровых услугах (Digital Services Act, DSA), вступивший в силу 19 октября 2022 г., предусматривает поэтапный подход к его реализации. Обширные онлайн-платформы, находящиеся под непосредственным контролем Комиссии, должны предоставлять статистику пользователей в течение трех месяцев. После

присвоения статуса платформы получают четырехмесячный срок для соблюдения положений, установленных данным законом. Начиная с 17 февраля 2024 г. его нормы распространяются и на более мелкие платформы, а государства-члены уполномочены обеспечивать соблюдение этих норм.

Указанный закон знаменует собой существенный сдвиг в нормативно-правовой базе, возвещая о наступлении новой эры в управлении цифровыми технологиями в Европейском союзе. Положения закона подчеркиваются его основной законодательной базой, а именно Регламентом (ЕС) 2022/2065, который был принят Европейским парламентом и Советом 19 октября 2022 г. Закон о цифровых услугах призван модернизировать и усовершенствовать существующую Директиву об электронной торговле, которая действует уже два десятилетия. Он создает всеобъемлющий набор единообразных правил, в первую очередь подчеркивая обязательства по соблюдению должной осмотрительности и условные освобождения от ответственности для услуг онлайн-посредников.

Закон о цифровых услугах укрепляет автономию пользователей, облегчая информирование о незаконном контенте и позволяя пользователям оспаривать решения платформ о модерации контента. В нем содержатся также меры по обеспечению прозрачности, которые обязывают онлайн-платформы раскрывать информацию об используемых алгоритмах, соглашениях об оказании услуг и рекламных практиках. Кроме того, он устанавливает особые обязательства для очень крупных платформ, которые должны внедрять стратегии, основанные на оценке рисков, и проходить независимую оценку своих систем управления рисками.

Закон обеспечен надежными механизмами правоприменения. Он предусматривает финансовые санкции, периодические штрафы и корректирующие действия для организаций, которые не соблюдают требования (Eifert et al., 2021). Система управления требует от стран – членов ЕС назначать координатора цифровых услуг, который действует совместно с Европейским советом по цифровым услугам. Кроме того, Комиссия осуществляет непосредственный надзор за очень крупными платформами, обладая правоприменительными полномочиями, аналогичными антимонопольному регулированию.

5.3. Закон об управлении данными

Закон об управлении данными (Data Governance Act, DGA) представляет собой уникальную правовую структуру для услуг посредничества в передаче данных (Data Intermediation Services, DIS). Хотя в Положении о регулировании дается определение «услуги посредничества в передаче данных», оно не содержит определения посредника в передаче данных, который предлагает эти услуги (Carovano & Finck, 2023). Услуги посредничества в передаче данных призваны облегчить создание коммерческих партнерств, обеспечивающих обмен данными между неопределенным числом субъектов данных и держателей данных, а также пользователей данных. Это достигается различными техническими, юридическими или иными методами, включая продвижение прав субъектов данных в отношении их персональных данных.

Статья 2(11) Закона об управлении данными определяет четыре критерия, которым должна соответствовать услуга, чтобы быть классифицированной как услуга посредничества в работе с данными: (i) основной целью услуги должен быть обмен данными; (ii) процесс обмена должен либо устанавливать, либо стремиться

к установлению коммерческих отношений; (iii) в обмене данными должно участвовать неопределенное количество держателей данных или субъектов, а также пользователей данных. Кроме того, это положение охватывает широкую материальную сферу, устанавливая, что (iv) посредничество может осуществляться с помощью технических, юридических или альтернативных методов. Закон относится к субъектам, которые создают или стремятся создать коммерческие партнерства с целью обмена данными. Совместное использование данных характеризуется как акт предоставления данных субъектом или держателем данных пользователю данных для коллективного или индивидуального использования этих данных. Этот процесс регулируется добровольными соглашениями или применимым законодательством Евросоюза или отдельной страны и может происходить напрямую или через посредника, например, посредством открытых или коммерческих лицензий, которые могут быть платными или предоставляться бесплатно.

Закон об управлении данными разграничивает сферу действия, а именно исключает услуги, которые способствуют посредничеству в передаче контента, защищенного авторским правом, а также поставщиков консолидированной системы информации о курсах акций и поставщиков услуг по предоставлению информации о счетах. Эти организации не занимаются исключительно обменом данными; скорее, они преследуют иные цели. Кроме того, из сферы действия указанного закона исключены брокеры данных, консультанты и поставщики продуктов, которые извлекают дополнительную ценность из данных.

Статья 2(11), с другой стороны, охватывает деятельность по посредничеству в передаче данных, которая осуществляется «с целью реализации прав субъектов данных в отношении персональных данных»[5]. Здесь особо упоминаются услуги по управлению персональной информацией (personal information management services, PIMS), поскольку они классифицируются как «отдельная категория» услуг по посредничеству в передаче данных.

6. Проблемы регулирования в сфере цифрового рынка

По оптимистичному мнению, доминирование экосистемных компаний отражает их исключительные динамические способности. Более обоснованной представляется прагматическая точка зрения (Andriychuk, 2023b). Ряд авторов обращают внимание на тревожные действия этих недавно получивших большое влияние корпораций, а также на неспособность регулирующих органов принять законодательные и другие меры, которые могли бы эффективно пресечь неэтичную деятельность (Richter et al., 2021). Требование благосостояния потребителей предполагает, что отсутствие явного вреда для потребителей от повышения цен свидетельствует об отсутствии антимонопольной проблемы, т. е. что монополия является просто следствием превосходства инноваций (Newman, 2021). Однако такая точка зрения упускает из виду проблемы, с которыми сталкиваются поставщики, сотрудники и особенно в контексте платформ и экосистем сопутствующие предприятия.

[5] European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). https://clck.ru/3EoySV

Регулирующие органы часто не имеют достаточного количества персонала и ресурсов для эффективного решения этих проблем, что приводит к потенциальным просчетам в правоприменении. Однако ожидания общества продолжают расти. В некоторых случаях серьезность ситуации говорит о том, что технологические компании выиграют, если будут активно и убедительно ограничивать свои действия путем саморегулирования. В противном случае ситуация спровоцирует пристальное внимание к легитимности их деятельности в обществе, что может привести к более жесткому внешнему регулированию.

Концентрация рыночной силы у ограниченного числа компаний часто рассматривается как серьезная проблема, которая может поставить под угрозу не только экономические операции, но и сами основы демократии и управления, особенно в результате эрозии традиционной прессы и растущего влияния социальных медиаплатформ (Davola & Malgieri, 2023). Возникла необходимость полностью пересмотреть нормативно-правовую базу. Этому сопутствовали существенные меры регулирования, такие как судебные иски, инициированные Соединенными Штатами против Google и других крупных технологических компаний, а также введение Европейским союзом Закона о цифровых услугах и Закона о цифровых рынках (Jacobides, 2020). Несмотря на то, что многие регулирующие органы все еще не имеют достаточно опыта, ресурсов и концентрации, чтобы адекватно реагировать на всемирный призыв к реформам, такие страны, как Великобритания и Индия, активно продвигают создание нового подразделения по цифровой конкуренции (Moreno Belloso & Petit, 2023). Существует настоятельная необходимость в разработке новых инструментов регулирования, направленных на усиление конкуренции как между платформами, так и внутри них. Кроме того, важно пересмотреть существующие рамки, теоретические конструкции и общие методологии, чтобы решить современные проблемы регулирования, особенно те, которые возникают в связи с платформами и экосистемами.

Заключение

В данной статье рассматриваются вопросы разработки и реализации решений в области цифровых рынков. Появление цифровых платформ и растущие опасения относительно их влияния как на рынки, так и на общество стремительно трансформирует регуляторную среду. Эти изменения расширяют возможности взаимодействия между аспектами конкуренции и нормативно-правовой базой. Чтобы эффективно решать эти задачи, наши теоретические взгляды на эту динамику также должны адаптироваться и развиваться.

Выбор подходящего средства правовой защиты – это сложная задача, и ошибки могут привести к дорогостоящему чрезмерному или недостаточному правоприменению. Как правило, власти должны быть готовы применять более жесткие средства защиты по мере того, как растет очевидность пагубных последствий конкретных действий. Необходимо также тщательно подходить к изучению новых теорий вреда. Любое сложное средство защиты должно рассматриваться как динамичный процесс, который периодически оценивается и изменяется по мере поступления дополнительной информации о его влиянии на реальное поведение.

Постоянный процесс изучения и адаптации требует от различных органов власти использования своих институциональных преимуществ. Эффективная координация

различных правоприменительных действий, осуществляемых национальными органами по вопросам конкуренции и национальными регулирующими органами, может стать более гибкой, если определить три важнейших, но различных вида деятельности: (i) выявление поведения или определенных рыночных структур, которые негативно влияют на благосостояние, (ii) формулирование соответствующих средств правовой защиты и (iii) контроль и корректировка их применения с течением времени.

Необходимо более полное научное исследование средств правовой защиты, особенно в связи с их применением в цифровой сфере. Средства правовой защиты должны выходить за рамки простых выводов, содержащихся в решениях о нарушении; они должны давать четко определенные и существенные рамки. Учитывая сложный характер вопросов, связанных со средствами правовой защиты, существует необходимость в более совершенных разработках и адаптируемых институциональных структурах, чем те, которые существуют в настоящее время.

Список литературы

Adadi, A. (2021). A survey on data-efficient algorithms in big data era. *Journal of Big Data*, *8*(1), 24. https://doi.org/10.1186/s40537-021-00419-9

Andriychuk, O. (Ed.) (2023a). *Antitrust and the Bounds of Power: 25 Years On*. Bloomsbury Publishing.

Andriychuk, O. (2023b). EU Digital Competition Law: The Socio-legal Foundations. *Cambridge Yearbook of European Legal Studies*, *25*, 81–104. https://doi.org/10.1017/cel.2023.12

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219–246. https://doi.org/10.1108/ejm-06-2019-0515

Bietti, E. (2024). Structuring Digital Platform Markets: Antitrust and Utilities' Convergence. *University of Illinois Law Review*, *2024*(4).

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Budzinski, O., & Stöhr, A. (2019). Competition policy reform in Europe and Germany – institutional change in the light of digitization. *European Competition Journal*, *15*(1), 15–54. https://doi.org/10.1080/17441056.2018.1555942

Cammaerts, B., & Mansell, R. (2020). Digital platform policy and regulation: Toward a radical democratic turn. *International Journal of Communication*, *14*, 135–154.

Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review*, *50*, 105830. https://doi.org/10.1016/j.clsr.2023.105830

Cen, Y., & Li, L. (2020). Effects of network externalities on user loyalty to online B2B platforms: an empirical study. *Journal of Enterprise Information Management*, *33*(2), 309–334. https://doi.org/10.1108/jeim-02-2019-0050

Davola, A., & Malgieri, G. (2023). Data, Power, and Competition Law: The (Im) possible Mission of the DMA? In *The Economics and Regulation of Digital Markets* (pp. 53–74). Emerald Publishing Limited. https://doi.org/10.1108/s0193-589520240000031003

Dunne, N. (2021). Platforms as regulators. *Journal of Antitrust Enforcement*, *9*(2), 244–269. https://doi.org/10.1093/jaenfo/jnaa052

Eifert, M., Metzger, A., Schweitzer, H., & Wagner, G. (2021). Taming the giants: The DMA/DSA package. *Common Market Law Review*, *58*(4). https://doi.org/10.54648/cola2021065

Galehr, S. (2023). *Transatlantic Data Transfers under the GDPR*. EIZ Publishing. https://doi.org/10.36862/eiz-ng001

Gerstenberg, O. (2020). Fundamental rights and democratic sovereignty in the EU: the role of the Charter of Fundamental Rights of the EU (CFREU) in regulating the European Social Market Economy. *Yearbook of European Law*, *39*, 199–227. https://doi.org/10.1093/yel/yeaa008

Jacobides, M. G. (2020). *Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference*. https://doi.org/10.2139/ssrn.3765324

Jenny, F. (2021). *Competition law enforcement and regulation for digital platforms and ecosystems: understanding the issues, facing the challenges and moving forward*. https://doi.org/10.2139/ssrn.3857507

Knudsen, E. S., Lien, L. B., Timmermans, B., Belik, I., & Pandey, S. (2021). Stability in turbulent times? The effect of digitalization on the sustainability of competitive advantage. *Journal of Business Research, 128*, 360–369. https://doi.org/10.1016/j.jbusres.2021.02.008

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, *43*(3), 405–424. https://doi.org/10.1002/smj.3250

Lancieri, F. M. (2019). Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift. *Journal of Antitrust Enforcement*, *7*(1), 27–53. https://doi.org/10.1093/jaenfo/jny012

Liang, Y., & Whalen, C. J. (2022). Money manager capitalism and the coronavirus pandemic. In *A Modern Guide to Post-Keynesian Institutional Economics* (pp. 89–120). Edward Elgar Publishing. https://doi.org/10.4337/9781800885752.00012

Lianos, I., & McLean, A. (2021). *Competition law, big tech and financialisation: The dark side of the moon*. https://doi.org/10.2139/ssrn.3930565

Manne, G. A. (2020). Error Costs in Digital Markets. *The Global Antitrust Institute Report on the Digital Economy*, *3*. https://doi.org/10.2139/ssrn.3733662

Mariani, M. M., & Wamba, S. F. (2020). Exploring how consumer goods companies innovate in the digital age: The role of big data analytics companies. *Journal of Business Research*, *121*, 338–352. https://doi.org/10.1016/j.jbusres.2020.09.012

Mascarenhas, O. A., Thakur, M., & Kumar, P. (2024). Critical Thinking Applied to Profit Maximization and Its Presumptive Capitalist Models. In *A Primer on Critical Thinking and Business Ethics* (pp. 31–64). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-312-120231002

Moreno Belloso, N., & Petit, N. (2023). *The EU digital markets act (DMA): a competition hand in a regulatory glove*. https://doi.org/10.2139/ssrn.4358589

Newman, J. M. (2021). The Output-Welfare Fallacy: A Modern Antitrust Paradox. *Iowa L. Rev.*, *107*, 563. https://doi.org/10.2139/ssrn.3866725

Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

Parker, G., Petropoulos, G., & Van Alstyne, M. W. (2020). *Digital platforms and antitrust*. https://doi.org/10.2139/ssrn.3608397

Perera, A., & Iqbal, K. (2021). Big data and emerging markets: Transforming economies through data-driven innovation and market dynamics. *Journal of Computational Social Dynamics*, *6*(3), 1–18.

Pervin, N., Ramasubbu, N., & Dutta, K. (2019). Habitat traps in mobile platform ecosystems. *Production and Operations Management*, *28*(10), 2594–2608. https://doi.org/10.1111/poms.13072

Petit, N. (2021). The proposed digital markets act (DMA): a legal and policy review. *Journal of European Competition Law & Practice*, *12*(7), 529–541. https://doi.org/10.1093/jeclap/lpab062

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*, 575–582. https://doi.org/10.1007/s00439-018-1919-7

Ratchford, B., Soysal, G., Zentner, A., & Gauri, D. K. (2022). Online and offline retailing: What we know and directions for future research. *Journal of Retailing*, *98*(1), 152–177. https://doi.org/10.1016/j.jretai.2022.02.007

Richter, H., Straub, M., Tuchtfeld, E., Buri, I., van Hoboken, J., De Gregorio, G., Pollicino, O., Peukert, A., Appelman, N., Quintais, J. P., Fahy, R., Zech, H., Goanta, C., Ruschemeier, H., Leerssen, P., Janal, R., Rodríguez, H. B. T., Graef, I., Franck, J.-U. ... & Vergnolle, D. S. (2021). To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package. *Max Planck Institute for Innovation & Competition Research Paper*, 21–25. https://doi.org/10.2139/ssrn.3932809

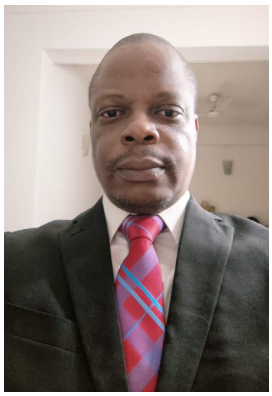
Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1). https://doi.org/10.54648/cola2020006

Schütz, P. (2022). Data protection authorities under the EU General Data Protection Regulation-a new global benchmark. In *Handbook of Regulatory Authorities* (pp. 128–145). Edward Elgar Publishing. https://doi.org/10.4337/9781839108990.00018

Sznajder, M. (2021). No Strings Attached? Zero-Price Practices on Social Media Markets under EU Abuse of Dominance Assessment. *Yearbook of Antitrust and Regulatory Studies (YARS)*, *14*(24), 33–62.

Texocotitla, M. A., Hernandez, M. D. A., & Hernandez, S. A. (2017). *The Doctrine of Free Markets: Origin, Nature and Implications*.

Сведения об авторе



Колаволе Афувапе – магистр права, ассистент преподавателя, Школа права, Глобальный университет имени О. П. Джиндала
Адрес: 131001 Нарьяна, Индия, г. Сонипат, Нир Ягдишпур Виледж, Сонипат Нарела Роуд
E-mail: kolawole.afuwape@jgu.edu.in
ORCID ID: https://orcid.org/0009-0001-5686-230X
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 4 октября 2024 г.
Дата одобрения после рецензирования – 20 октября 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.

Research article
UDC 34:004:346.6:004.8
EDN: https://elibrary.ru/gnqswz
DOI: https://doi.org/10.21202/jdtl.2024.48

Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces

Afuwape Kolawole

O. P. Jindal Global University, Sonipat, India

Keywords

antitrust law,
competition law,
confidentiality,
consumer rights,
data abuse,
digital markets,
digital platforms,
digital technologies,
law,
personal data protection

Abstract

Objective: to develop approaches and proposals to improve the legal mechanisms for the personal data protection in the context of the evolving digital markets and the growing digital competition.

Methods: the article is prepared based on formal legal and comparative legal research methods.

Results: the unique features of digital markets are shown, which must be taken into account to achieve the goals of antimonopoly legislation. It is marked that the fundamental elements of the digital market include the big data concept and big data analytics, which, based on digital platforms, are capable of producing many direct and indirect network effects. The latter require understanding for an effective antitrust response and the application of appropriate legislation. The author proves that the growth of digital platforms as a business model and vital infrastructure of the digital economy should be viewed as a factor in improving legal regulation of relations in the sphere of data protection and confidentiality. The paper identifies the potential of digital platforms for assessing the current market power and the impact of competition on limiting this power. The data are considered as an integral component of the overall competitive market landscape. The current European Union regulation in the field of digital platforms and personal data protection is analyzed. The author identifies difficulties associated with the creation and application of effective regulations governing the activities of digital platforms. The article proves that antimonopoly authorities need to change approaches to analytics in order to take into account

© Kolawole 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.

the distinctive features of digital platforms. It is noted that such changes may require legislative reforms and revision of procedures to match the rapid development of these markets and ensure that any potentially anti-competitive behavior is thoroughly investigated.

Scientific novelty: the research contributes to the development of approaches to determining indicators of ensuring the personal data confidentiality under the digitalization of markets and to evaluating the effectiveness of antimonopoly legislation and its application in a new competitive environment.

Practical significance: the results obtained can be used as a basis for improving antimonopoly and personal data protection legislation, as well as legal regulation of digital platforms in general.

For citation

Kolawole, A. (2024). Legal Aspects of Personal Data Protection and the Issues of Competition in Digital Marketplaces. *Journal of Digital Technologies and Law, 2*(4), 1031–1053. https://doi.org/10.21202/jdtl.2024.48

References

Adadi, A. (2021). A survey on data-efficient algorithms in big data era. *Journal of Big Data*, *8*(1), 24. https://doi.org/10.1186/s40537-021-00419-9

Andriychuk, O. (Ed.) (2023a). *Antitrust and the Bounds of Power: 25 Years On*. Bloomsbury Publishing.

Andriychuk, O. (2023b). EU Digital Competition Law: The Socio-legal Foundations. *Cambridge Yearbook of European Legal Studies*, *25*, 81–104. https://doi.org/10.1017/cel.2023.12

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219–246. https://doi.org/10.1108/ejm-06-2019-0515

Bietti, E. (2024). Structuring Digital Platform Markets: Antitrust and Utilities' Convergence. *University of Illinois Law Review*, *2024*(4).

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Budzinski, O., & Stöhr, A. (2019). Competition policy reform in Europe and Germany – institutional change in the light of digitization. *European Competition Journal*, *15*(1), 15–54. https://doi.org/10.1080/17441056.2018.1555942

Cammaerts, B., & Mansell, R. (2020). Digital platform policy and regulation: Toward a radical democratic turn. *International Journal of Communication*, *14*, 135–154.

Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review*, *50*, 105830. https://doi.org/10.1016/j.clsr.2023.105830

Cen, Y., & Li, L. (2020). Effects of network externalities on user loyalty to online B2B platforms: an empirical study. *Journal of Enterprise Information Management*, *33*(2), 309–334. https://doi.org/10.1108/jeim-02-2019-0050

Davola, A., & Malgieri, G. (2023). Data, Power, and Competition Law: The (Im) possible Mission of the DMA? In *The Economics and Regulation of Digital Markets* (pp. 53–74). Emerald Publishing Limited. https://doi.org/10.1108/s0193-589520240000031003

Dunne, N. (2021). Platforms as regulators. *Journal of Antitrust Enforcement*, *9*(2), 244–269. https://doi.org/10.1093/jaenfo/jnaa052

Eifert, M., Metzger, A., Schweitzer, H., & Wagner, G. (2021). Taming the giants: The DMA/DSA package. *Common Market Law Review*, *58*(4). https://doi.org/10.54648/cola2021065

Galehr, S. (2023). *Transatlantic Data Transfers under the GDPR*. EIZ Publishing. https://doi.org/10.36862/eiz-ng001

Gerstenberg, O. (2020). Fundamental rights and democratic sovereignty in the EU: the role of the Charter of Fundamental Rights of the EU (CFREU) in regulating the European Social Market Economy. *Yearbook of European Law*, *39*, 199–227. https://doi.org/10.1093/yel/yeaa008

Jacobides, M. G. (2020). *Regulating Big Tech in Europe: why, so what, and how understanding their business models and ecosystems can make a difference*. https://doi.org/10.2139/ssrn.3765324

Jenny, F. (2021). *Competition law enforcement and regulation for digital platforms and ecosystems: understanding the issues, facing the challenges and moving forward*. https://doi.org/10.2139/ssrn.3857507

Knudsen, E. S., Lien, L. B., Timmermans, B., Belik, I., & Pandey, S. (2021). Stability in turbulent times? The effect of digitalization on the sustainability of competitive advantage. *Journal of Business Research, 128*, 360–369. https://doi.org/10.1016/j.jbusres.2021.02.008

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, *43*(3), 405–424. https://doi.org/10.1002/smj.3250

Lancieri, F. M. (2019). Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift. *Journal of Antitrust Enforcement*, *7*(1), 27–53. https://doi.org/10.1093/jaenfo/jny012

Liang, Y., & Whalen, C. J. (2022). Money manager capitalism and the coronavirus pandemic. In *A Modern Guide to Post-Keynesian Institutional Economics* (pp. 89–120). Edward Elgar Publishing. https://doi.org/10.4337/9781800885752.00012

Lianos, I., & McLean, A. (2021). *Competition law, big tech and financialisation: The dark side of the moon*. https://doi.org/10.2139/ssrn.3930565

Manne, G. A. (2020). Error Costs in Digital Markets. *The Global Antitrust Institute Report on the Digital Economy*, *3*. https://doi.org/10.2139/ssrn.3733662

Mariani, M. M., & Wamba, S. F. (2020). Exploring how consumer goods companies innovate in the digital age: The role of big data analytics companies. *Journal of Business Research*, *121*, 338–352. https://doi.org/10.1016/j.jbusres.2020.09.012

Mascarenhas, O. A., Thakur, M., & Kumar, P. (2024). Critical Thinking Applied to Profit Maximization and Its Presumptive Capitalist Models. In *A Primer on Critical Thinking and Business Ethics* (pp. 31–64). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-312-120231002

Moreno Belloso, N., & Petit, N. (2023). *The EU digital markets act (DMA): a competition hand in a regulatory glove*. https://doi.org/10.2139/ssrn.4358589

Newman, J. M. (2021). The Output-Welfare Fallacy: A Modern Antitrust Paradox. *Iowa L. Rev.*, *107*, 563. https://doi.org/10.2139/ssrn.3866725

Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

Parker, G., Petropoulos, G., & Van Alstyne, M. W. (2020). *Digital platforms and antitrust*. https://doi.org/10.2139/ssrn.3608397

Perera, A., & Iqbal, K. (2021). Big data and emerging markets: Transforming economies through data-driven innovation and market dynamics. *Journal of Computational Social Dynamics*, *6*(3), 1–18.

Pervin, N., Ramasubbu, N., & Dutta, K. (2019). Habitat traps in mobile platform ecosystems. *Production and Operations Management*, *28*(10), 2594–2608. https://doi.org/10.1111/poms.13072

Petit, N. (2021). The proposed digital markets act (DMA): a legal and policy review. *Journal of European Competition Law & Practice*, *12*(7), 529–541. https://doi.org/10.1093/jeclap/lpab062

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*, 575–582. https://doi.org/10.1007/s00439-018-1919-7

Ratchford, B., Soysal, G., Zentner, A., & Gauri, D. K. (2022). Online and offline retailing: What we know and directions for future research. *Journal of Retailing*, *98*(1), 152–177. https://doi.org/10.1016/j.jretai.2022.02.007

Richter, H., Straub, M., Tuchtfeld, E., Buri, I., van Hoboken, J., De Gregorio, G., Pollicino, O., Peukert, A., Appelman, N., Quintais, J. P., Fahy, R., Zech, H., Goanta, C., Ruschemeier, H., Leerssen, P., Janal, R., Rodríguez, H. B. T., Graef, I., Franck, J.-U. ... & Vergnolle, D. S. (2021). To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package. *Max Planck Institute for Innovation & Competition Research Paper*, 21–25. https://doi.org/10.2139/ssrn.3932809

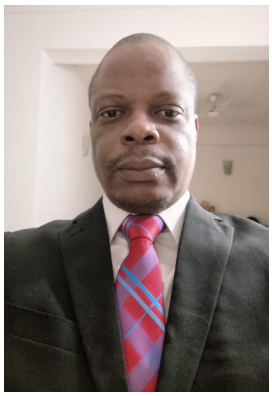
Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1). https://doi.org/10.54648/cola2020006

Schütz, P. (2022). Data protection authorities under the EU General Data Protection Regulation-a new global benchmark. In *Handbook of Regulatory Authorities* (pp. 128–145). Edward Elgar Publishing. https://doi.org/10.4337/9781839108990.00018

Sznajder, M. (2021). No Strings Attached? Zero-Price Practices on Social Media Markets under EU Abuse of Dominance Assessment. *Yearbook of Antitrust and Regulatory Studies (YARS)*, *14*(24), 33–62.

Texocotitla, M. A., Hernandez, M. D. A., & Hernandez, S. A. (2017). *The Doctrine of Free Markets: Origin, Nature and Implications*.

Author information



Afuwape Kolawole – LLM, Assistant Lecturer, Jindal Global Law School, O.P. Jindal Global University
Address: Sonipat Narela Road, Near Jagdishpur Village, Sonipat, Haryana 131001, NCR of Delhi, India
E-mail: kolawole.afuwape@jgu.edu.in
ORCID ID: https://orcid.org/0009-0001-5686-230X
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

Conflict of interest

The author declare 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 – October 4, 2024
Date of approval – October 20, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

