ISSN 2949-2483

Volume 2 Number 2

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2024

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Том 2, № 2
2024

DOI: 10.21202/2949-2483.2024.2

ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

eISSN 2949-2483

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

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

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

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 2, № 2
2024
DOI: 10.21202/2949-2483.2024.2
ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
eISSN 2949-2483

Содержание

От редакции
УДК 34:004
EDN: https://elibrary.ru/bpdcht
DOI: https://doi.org/10.21202/jdtl.2024.13

Современная зарубежная правовая мысль о новых феноменах цифровой трансформации

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

Анна Константиновна Жарова
Национальный исследовательский университет «Высшая школа экономики», Москва, Россия

Елизавета Александровна Громова
Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, 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

Непосредственная вовлеченность в процессы цифровизации ученых-правоведов и практикующих юристов всего мира совсем недавно казалась эфемерной. Трудно было представить, что за короткое время стремительный скачок в развитии технологий начнет менять практически все сферы деятельности (включая юридическую), сделает цифровизацию настолько всеобъемлющей, что она уже будет восприниматься как обыденность. Что никого уже не будет удивлять возрастание значения на рынке труда цифровых компетенций, ставших необходимыми для эффективного использования и работы с цифровыми технологиями. Что при обучении и подготовке квалифицированных юристов, повышении их квалификации потребуется пересматривать компетентностный подход с учетом тенденции цифровой экономики, которая формирует новую регуляторную среду отношений. Что в юридический лексикон прочно войдут такие понятия, как «цифровые права», «цифровая зрелость», «технологический суверенитет» и многие другие. Что сами юристы вместе со своими коллегами из других отраслей знаний будут действовать в координатах цифровой

трансформации, критерии которой предстоит определить, учитывая, что право служит основным фактором темпа технологизации и цифровизации общественных отношений.

В своей деятельности юристы неизбежно сталкиваются с новыми феноменами, порождаемыми цифровизацией. Отношение к последней поделило юридический мир, с известной долей условности, на два лагеря (группы): одни воспринимают ее как благо, которое дает развитие научно-технического прогресса, влекущее появление новых возможностей для человека, общества и государства, другие же относятся к ней настороженно, видя появление ранее неизвестных рисков, вызовов, угроз для человечества, вплоть до экзистенциальных. Но как бы мы ни относились к цифровизации и ее феноменам, точно можно сказать, что она стала глобальным мегатрендом, задающим новые исследовательские парадигмы и объединяющим ученых и практиков из разных уголков мира, стремящихся поделиться своим опытом и видением решения возникающих прикладных и теоретических задач, обусловленных цифровизацией, внести свой вклад в развитие юридической практики, науки и технологий. На это указывает и содержание Journal of Digital Technologies and Law, расширившего географию своих авторов, чьи научные результаты были представлены широкой общественности в первом выпуске журнала за 2024 г.

Взяв высокую планку в 2023 г., журнал продолжает развивать международное сотрудничество не только в части работы со своими амбассадорами, являющимися известными специалистами в области права и технологий и представляющими журнал в разных странах мира, но и в части опубликования новых и заслуживающих внимания исследований из разных государств. В этом смысле текущий выпуск сфокусирован на отражении различных направлений зарубежной правовой мысли, находящейся под влиянием цифровизации. На страницах номера можно ознакомиться с работами ученых из Австралии, Египта, Индии, Испании, Китая, Мали, Марокко, Нигерии, Португалии, Танзании, Уганды, Филиппин, Франции.

В представленном выпуске Journal of Digital Technologies and Law собраны научные изыскания зарубежной правовой науки, в которой осмысливаются страноведческие, региональные и международные аспекты конвергенции права и технологий, возможности и эффективность сочетания внутреннего (национального) права государств и инструментов международного права, трансформации классических концепций, доктрин, правовых институтов в современных условиях цифровизации, правовая и технологическая составляющая новых феноменов, порожденных цифровой трансформацией, такая как киберпространство, киберсуверенитет, шерентинг, лутбокс и другие, а также последствия цифровой трансформации права, правовые проблемы и перспективы цифровизации.

Номер открывает статья «Демаркация киберпространства: правовые и политические последствия применения концепции национальных интересов суверенных государств» (**Яссин Абдалла Абделькарим (Египет)**), в которой анализируются различные аспекты адаптации традиционного юридического понятия суверенитета к текущим реалиям и подчеркивается необходимость его переосмысления в киберпространстве с учетом требований безопасности и разработки дисциплинарной детерминанты киберсуверенитета. Показано применение традиционных и современных правовых концепций суверенитета в новой, цифровой, среде, раскрыто функциональное значение концепции государственных киберинтересов для демаркации киберпространства и определения границ национального суверенитета.

Проблемы суверенитета, риски кибербезопасности, подходы к регулированию и повышению эффективности управления данными в разных юрисдикциях получили отражение в статье «Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления» (**Гульбакыт Болатбеккызы (Китай)**). В работе вопросы суверенитета и локализации информации предлагается считать одними из самых сложных в области трансграничной передачи данных и формирования трансграничного пространства доверия. Последнее признается важным стимулом развития национальных цифровых экосистем и форматов обмена данными (G2G, G2C, G2B, B2B и B2C), однако важно обеспечить баланс между доступностью данных, с одной стороны, и их безопасностью, с другой.

Нельзя не отметить, что глобальные потоки данных уже стали фактором, определяющим устойчивое развитие современной международной торговли. Возникающие на этом пути преграды, сдерживающие трансграничную передачу данных, часто влекут за собой задержку и удорожание товаров и услуг. Анализу перспектив международных торговых контрактов в свете технологических новаций в торговом праве посвящено отдельное исследование – «Применение смарт-контрактов в сфере международной торговли и перспективы дальнейшей эволюции Инкотермс» (**Принс Фатер Ауду (Нигерия)**, **Шабих Фатима (Индия)**). В нем анализируются международные коммерческие условия, определяющие транзакции между импортерами и экспортерами, и делается вывод, что их синхронизация со смарт-контрактами способна положительно повлиять на перспективы международной торговли и особенно на экспортно-импортные контракты.

В контексте международной торговли все более актуальными становятся вопросы безопасности онлайн-транзакций и трансграничных платежей. Новые технологии, такие как смарт-контракты и блокчейн, должны были повысить безопасность связи и обмена трансграничной информацией. Эту задачу путем кодирования и декодирования информации решают и криптографические технологии. Вместе с тем интеграция последних в международную торговлю, а именно в сферу продуктов информационно-коммуникационных технологий, породила сложные проблемы регулирования. В номере отдельное внимание уделяется изучению специфики правового регулирования международной торговли криптографическими продуктами и технологиями документами Всемирной торговой организации и региональными торговыми соглашениями (**Сайед Кудрат Хашими (Индия)**, **Джексон Симанго Магоге (Танзания)**). В работе раскрывается сложный правовой ландшафт, меняющийся под воздействием цифрового императива, в условиях интеграции криптографических технологий в международную торговлю.

Онлайн-транзакции получают широкое распространение не только на международном, трансграничном уровне, но и в массовых многопользовательских онлайн-играх, где во внутриигровых магазинах приобретаются виртуальные товары. Развитие бизнес-моделей в этой сфере деятельности пошло по пути таких микротранзакций, когда наряду с покупкой игры целиком, как это было раньше, появляется возможность приобретать в ней отдельные предметы. Это привело к появлению новой модели получения дохода, основанной на продаже внутриигровых (виртуальных) предметов. Данное явление, получившее название лутбоксов, стремительно набрало обороты и быстро глобализировалось, что для юрисдикций ряда стран стало настоящей правовой проблемой. В этой связи интерес представляет сравнительное исследование опыта правового регулирования лутбоксов в различных странах (**Сеппи Пор (Австралия)**).

В другой статье, вошедшей в настоящий выпуск, показана эффективность электронных платежей как средства транзакций, однако вместе с тем отмечается ряд юридических проблем, которые могут мешать их дальнейшему беспрепятственному использованию (**Исмаила Озовехе Харуна (Нигерия), Пол Атагамен Айдоноджи (Уганда), Онивеху Джулиус Бейда (Нигерия)**). Так, широкий спектр вопросов, связанных с работой электронных платежных систем, раскрывается на примере одного из перспективных государств Африки – Нигерии. В условиях, когда официальными нигерийскими органами и лицами уже предприняты определенные шаги по решению обозначенных проблем, отмечается их недостаточность для эффективного регулирования системы электронных платежей в стране.

Еще одним новым феноменом, считающимся порождением цифровизации, а точнее связанным с популярностью и распространением социальных сетей и интернет-активностью детей и их родителей, является шерентинг. Суть его состоит в размещении в социальных сетях информации о несовершеннолетних (особенно их фото и видео), ставящем под угрозу основные права несовершеннолетних, подвергающем риску их частную жизнь, порождающем социально-правовые конфликты. В номере этим вопросам посвящено специальное исследование (**Франциско Хосэ Аранда Серна (Испания)**), проведенное на основе анализа основных положений законодательства Испании, Франции и США, определяющих социально-правовую природу шерентинга как деятельности, его правовые последствия.

Определению уровня защищенности прав авторов контента в социальных сетях и выработке мер профилактики правонарушений в данной области посвящена статья «Меры профилактики нарушений авторских прав на создание контента в цифровой среде: опыт Нигерии» (**Адетуту Дебора Айна-Пелемо, Итамар Басси, Глориос Океоген Акподжаро (Нигерия)**). На примере опыта Нигерии предпринимается попытка изучить права и меры защиты, предоставляемые создателям цифрового контента в соответствии с законодательством об интеллектуальной собственности.

Цифровой формат может быть использован и в интересах стандартизации, а также упрощения формулирования многих документов. На примере анализа соглашений о государственно-частном партнерстве, оценки их юридических параметров в условиях цифровизации в одной из статей номера (**Доминик Т. Молинтас (Филиппины – Австралия)**) предпринята попытка синтезировать их основные положения в общую матрицу, которая может послужить инструментом при составлении соглашений о государственно-частном партнерстве с учетом особенностей законодательства и иных обстоятельств.

В последние годы в центре всеобщего внимания науки и практики находится искусственный интеллект. Данная тематика нашла отражение и в представленном номере (**Хамза Джабир (Марокко), Камаль Лагтати (Марокко), Денис Поэ-Токпа (Франция)**). Применяя аналитический и сравнительный методы, авторы выявляют проблемы и анализируют возможности этического и правового регулирования искусственного интеллекта на примере опыта цифровых преобразований в Марокко.

Завершает выпуск журнала краткий аналитический экскурс в антропосоциогенез, в котором представлены эволюция человечества, различных социальных институтов и понимания экзистенциальной роли законов, направленных на обеспечение совместной жизни социума в контексте технологических новаций (**Дженеба Траоре (Мали – Кабо-Верде)**).

Представленные исследования показывают, что цифровая трансформация сопряжена с проблемой неравномерного развития цифровых технологий в разных странах. Проблема эта не новая, обознается она в исследованиях по-разному, как

проблема цифрового разрыва, цифрового раскола, цифрового неравенства. Вместе с тем по-прежнему актуальность ее сохраняется и находится в фокусе внимания зарубежной доктрины.

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

В этом году Journal of Digital Technologies and Law был одобрен для индексации в **HeinOnline** – крупнейшей в мире базе данных правовых исследований и юридических периодических изданий. Это дополнительно подчеркивает соответствие журнала принятым издательским стандартам, предпринятые усилия для обеспечения прозрачности и воспроизводимости результатов исследований.

Востребованность научного поиска и новых результатов в этом направлении подтверждается высоким интересом к Journal of Digital Technologies and Law и представленным на его страницах публикациям, охватывающим проблематику цифровых технологий и права (рис. 1).

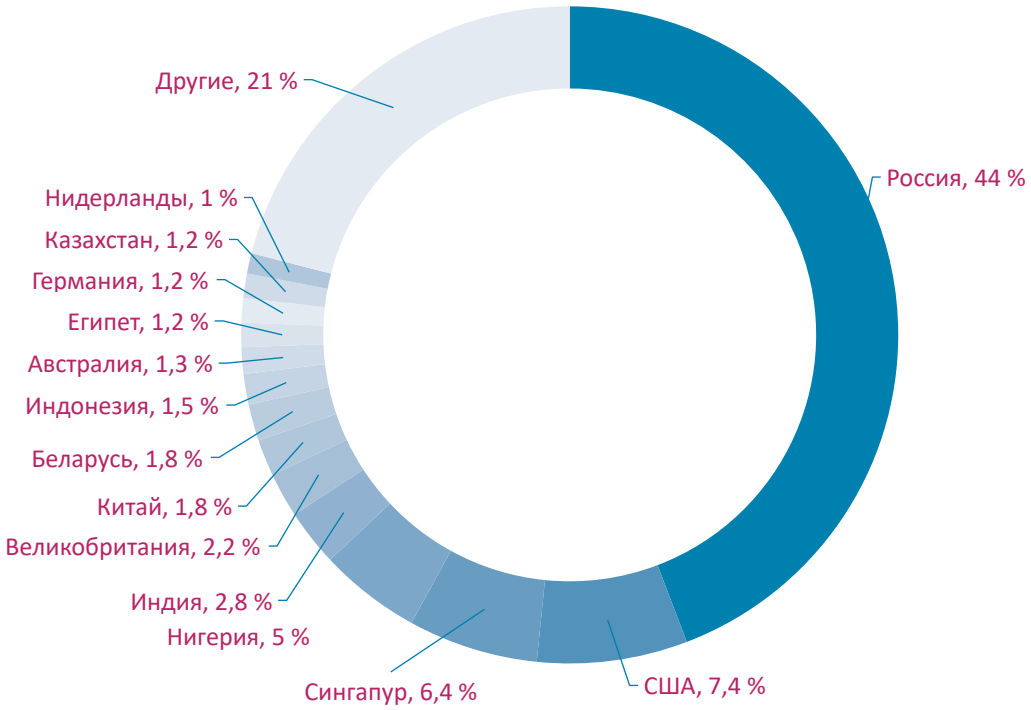


Рис. 1. Статистика посещаемости сайта журнала Journal of Digital Technologies and Law (по состоянию на 30 июня 2024 г.)

В целях дальнейшего формирования международного диалога мы открыты для сотрудничества с ведущими и молодыми отечественными и зарубежными учеными, экспертами, практикующими юристами для публикации их идей по вопросам совершенствования существующих и выработки новых подходов к решению проблем правового регулирования и охраны общественных отношений, связанных с цифровыми технологиями.

Благодарим авторов, рецензентов, сотрудников редакции, амбассадоров журнала, членов редакционной коллегии и читателей за сотрудничество и растущий интерес к нашему периодическому изданию.

Научная статья
УДК 34:004:342.3:004.9
EDN: https://elibrary.ru/sywsrk
DOI: https://doi.org/10.21202/jdtl.2024.14

Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре, Сохаг, Египет

Ключевые слова

государство,
граница,
кибербезопасность,
киберинтерес,
киберпространство,
киберсуверенитет,
национальный интерес,
право,
суверенитет,
цифровые технологии

Аннотация

Цель: обосновать существование национального киберсуверенитета как юридического понятия, наряду с которым путем введения инновационной детерминанты – концепции государственных киберинтересов – переосмыслить традиционные понятия национального суверенитета и государственных границ в условиях динамичной природы киберпространства и необходимости разработки гибридного механизма защиты кибергранниц, основанного одновременно на праве и технологиях.

Методы: на основе доктринального метода выявлены принципиальные расхождения в представлениях ведущих ученых разной отраслевой принадлежности по концептуальным теоретико-методологическим и понятийно-категориальным вопросам, в том числе по вопросу обоснования единого алгоритма для установления границ в киберпространстве. Доктринальный метод дополнен анализом судебной практики разных стран, позволяющим рассмотреть распространение судами своей юрисдикции на споры, связанные с киберпространством.

Результаты: в исследовании представлено применение традиционных и современных правовых концепций суверенитета в новой, цифровой среде, результатом чего стало сочетание правовых и технологических подходов. Раскрыто функциональное значение концепции государственных киберинтересов для демаркации киберпространства и определения границ национального суверенитета. Показана адаптируемость данной концепции к технически неопределенной природе киберпространства. Делается вывод об основных направлениях формирования концепции киберинтересов в киберпространстве, ее политических и правовых последствиях, основанных в том числе на практике судов разных стран по разрешению киберспоров.

Научная новизна: концепция государственных киберинтересов рассматривается в качестве инновационного метода определения киберграниц, что обусловливает трансформацию смысла традиционного понятия суверенитета и тесно связанного с ними понятия национальных интересов применительно к киберпространству в контексте обеспечения требований безопасности и активизации национальной защиты от киберугроз.

Практическая значимость: полученные результаты устраняют имеющиеся противоречия в определении суверенитета и его пространственных пределов в условиях развития современных технологий; способствуют выработке дисциплинарного стандарта киберсуверенитета на основе надежного демаркатора, необходимого для определения государственного суверенитета и границ в киберпространстве; адаптируют традиционные юридические понятия суверенитета и национальных интересов к глобальным современным кибервызовам; способствуют трансформации традиционных правовых институтов и норм в области суверенитета и границ в условиях киберпространства.

Для цитирования

Абделькарим, Я. А. (2024). Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств. *Journal of Digital Technologies and Law*, *2*(2), 262–285. https://doi.org/10.21202/jdtl.2024.14

Содержание

Введение

С появлением Интернета перед человечеством открылась безграничная сфера взаимодействия, которая распространяется на весь мир. Сегодня киберпространство связывает самые отдаленные уголки планеты. Это позволяет обмениваться разнонаправленными потоками данных между государствами, передавая разнообразную информацию и осуществляя международное кибервзаимодействие между людьми.

Безграничность киберпространства бросает вызов традиционным правовым нормам в области суверенитета и границ. Эти нормы необходимы для установления государственного контроля над национальной территорией с целью предотвращения экстерриториального ущерба, который могут нанести многочисленные незаконные кибердействия извне. Таким образом, требования безопасности предполагают переосмысление этих понятий в киберпространстве для активизации национальной защиты против киберугроз. Разрабатывая эти понятия в киберпространстве, ученые стремятся дать им четкое определение и разработать стандарты их проявления в киберпространстве. Однако отсутствие единой методологии порождает противоречия в определении суверенитета и границ в киберпространстве. В зависимости от сферы своей деятельности ученые расходятся в представлении требуемой детерминации.

Данное исследование призвано восполнить этот пробел путем введения новой детерминанты суверенитета и границ в киберпространстве. Этой детерминантой является понятие государственных киберинтересов. В работе отмечается, что национальные интересы в киберпространстве являются основной мотивацией для вмешательства государства; именно они побуждают государства действовать для защиты своих суверенных интересов.

Для достижения цели исследования в статье рассматривается соответствующая научная литература по проблемам суверенитета и границ в киберпространстве. Автор доказывает целостную взаимосвязь между этими понятиями и их тесную связь с идеей национальных интересов. Показано отсутствие дисциплинарного стандарта демаркации в киберпространстве; это практический пробел в знаниях, который данное исследование призвано восполнить. Затем автор объясняет концепцию государственных интересов, рассматривает ее последствия и использование судами разных стран при разрешении киберспоров. Наконец, в работе с помощью юридической аргументации доказана функциональность концепции государственных киберинтересов для установления границ в киберпространстве и предложены практические основы для ее реализации.

1. Суверенитет и границы в киберпространстве: интегральное соответствие

Суверенитет как политико-правовая концепция – это неоднозначное понятие, которое юристы и политики разрабатывают с XVI в. Это важнейший фактор организации межгосударственных отношений и всех взаимодействий на глобальном, общечеловеческом, уровне. Выдающиеся западные ученые, такие как Боден[1] и Гоббс[2],

[1] Жан Боден (1530–1596), французский политический деятель и философ.

[2] Томас Гоббс (1588–1679), английский философ и историк.

представляли суверенитет как высшую власть короля принимать решения в пределах государства[3]. Согласно их взглядам, суверенитет – это политическая детерминанта государственной власти над территорией страны; ограничение национальной власти, которое налагает на государства фактическое обязательство взаимно уважать национальные суверенитеты друг друга. У Руссо эта политическая категория превратилась в понятие общественного договора[4]. Впоследствии философы и юристы разрабатывали различные теории суверенитета. Независимо от толкования понятия, суверенитет остается основным фактором, определяющим власть государства над своей территорией. Согласно Вестфальской доктрине, суверенитет означает верховную власть государства на своей территории (McLean & McMillan, 2009). Это традиционное определение суверенитета в юридических и политических науках, которое соответствует характеру межгосударственных взаимодействий в реальном мире. Таким образом, государства используют традиционные методы демаркации для установления государственных границ, регулирования полномочий и взаимодействий.

Однако появление киберпространства как современной сферы человеческих отношений и взаимодействий подразумевает распространение традиционных понятий на кибердеятельность. Этот факт потребовал от юристов и ученых переосмысления существующих понятий и теорий в контексте киберпространства. Таким образом, начала складываться концепция суверенитета в киберпространстве для организации государственной власти и отслеживания незаконной деятельности. Из-за очевидных различий между киберпространством и реальным миром необходимы значительные усилия со стороны ученых и законодателей для уточнения понятия суверенитета в условиях динамичной природы киберпространства. Этот процесс показал, что из-за особой природы киберпространства традиционные методы демаркации границ бесполезны. Необходимо разработать специальный инструментарий для установления кибергранниц, определяющих государственный суверенитет в киберпространстве.

В первом разделе исследования мы опишем эволюцию научного знания в области концепций киберсуверенитета и кибергранниц, а также изменения понятия суверенитета. Затем мы рассмотрим социальные и политические перспективы киберсуверенитета и его влияние на государственную и внутреннюю социальную политику, в частности, на законодательные аспекты этого явления. Наконец, мы проанализируем процесс демаркации в реальном мире и в киберпространстве и покажем пробелы в определении государственного суверенитета в киберпространстве.

1.1. Эволюция границ и суверенитета в киберпространстве

В 1983 г. благодаря изобретению протокола управления передачей данных (Transfer Control Protocol/Internetwork Protocol, TCP/IP) человечество обрело официальное открытое всемирное коммуникационное пространство – Интернет (ранее – онлайн-библиотека системы университетов штата Джорджия). С тех пор между пользователями Интернета – физическими, юридическими

[3] Sovereignty. (2024, Mar. 12). Encyclopedia Britannica. https://clck.ru/3A7Ttf

[4] Жан-Жак Руссо (1712–1778), французский философ.

лицами и правительствами – передаются огромные объемы данных. Развитие обмена данными требует анализа этой сферы взаимодействий с целью выявления ее особенностей.

Choucri и Clark (2013) отмечают, что в киберпространстве действительно отсутствует суверенитет; традиционное понятие суверенитета распространяется на киберпространство, но в такой форме, которая отвечает его безграничной природе. Подразумевается, что понятие суверенитета должно быть контекстуализировано в соответствии с технической сутью киберпространства. В этом решении проявляется попытка интегрировать юридическое понятие в технический контекст, чтобы преодолеть правовую неопределенность киберпространства.

Разработка понятия киберсуверенитета продолжилась, в результате чего была создана его строгая детерминанта. Исследователи сосредоточились на объяснении и уточнении того, как в киберпространстве проявляются границы. Границы являются логическим следствием суверенитета, поскольку они представляют собой его пределы. Понятия суверенитета и границ неразрывно связаны между собой; для определения суверенитета должны быть установлены и выверены границы. Эта логика распространяется и на киберпространство, поскольку точная интерпретация суверенитета требует разработки строгой детерминанты границ в киберпространстве.

Таким образом, началась научная разработка технических детерминант государственных границ в киберпространстве. Эти границы имеют те же признаки и функции, что и традиционные, поскольку позволяют государствам устанавливать свой суверенитет в киберпространстве. Соответственно, кибергранцы были определены как «функциональный эквивалент границы, где данные поступают в первую реальную контрольную точку – сетевой маршрутизатор, компьютерный сервер, ПК или другие сетевые устройства» (Osborn, 2017). Это определение основано на моделях обмена данными, представленных в указанном исследовании. Как следствие, сотрудники государственных органов, например таможенники, могут наблюдать за потоком данных в киберпространстве, отслеживая нелегальные товары или облагая налогами другие кибератериалы, находящиеся в законном обороте. Значимость этого определения состоит в том, что для объяснения юридического понятия был использован чисто технический подход, что соответствует природе киберпространства. Osborn считал, что киберсуверенитет государства распространяется на первую точку, где поток данных затрагивает государственные интересы. Аналогичным образом Фанг при определении киберсуверенитета отдавал приоритет техническому аспекту, отмечая: «Суверенитет государства в киберпространстве основан на системах ИКТ (информационно-коммуникационные технологии), находящихся под юрисдикцией государства; его границами являются порты сетевых устройств государства, непосредственно подключенных к сетевым устройствам других государств; суверенитет киберпространства реализуется с целью защиты операций с данными посредством киберролей» (Fang, 2018). Автор соотносит кибертерриторию государства с сетью устройств в нем. Таким образом, карта всех устройств сети соответствует территории государства в киберпространстве. Кроме того, он отметил, что киберсуверенитет предоставляет государству те же полномочия в отношении своей территории, что и традиционный суверенитет, в частности возможности для обороны и сохранения независимости (Fang, 2018). Определение Фанга удачно сочетает в себе аспекты права и технологии, устанавливая государственную территорию в киберпространстве в соответствии с технической картой сетевых устройств и рассматривая права государства исходя из этой правовой концепции.

В связи с этим прокуратурой Египта был принят функциональный подход к вопросу о признании кибергранниц. В официальном заявлении отмечается, что у государства есть виртуальные границы в киберпространстве; они составляют четвертую государственную границу на политической карте[5]. Таким образом, надзор в этой сфере представляет собой государственный интерес первостепенной важности. Хотя в заявлении не приводится определение кибергранниц, их существование и функции признаны официально.

Широкое проникновение Интернета в современную жизнь сделало киберпространство неотъемлемой частью человеческих взаимоотношений и различного рода взаимодействий. Непрерывное развитие коммуникационных технологий в киберпространстве ставит под сомнение полномочия государств по регулированию деятельности в Интернете. Это побуждает ученых обратить пристальное внимание на правовые вопросы, возникающие при кибервзаимодействии. Аспекты государственного суверенитета и государственной власти над кибертерриторией занимают значительное место в научных дебатах. Кроме того, в рамках судебной практики был разработан ряд инструментов, позволяющих установить политические границы в киберпространстве.

Проблема киберсуверенитета не может ограничиваться физическим расположением сетевых устройств (Omar et al., 2022). Отсутствие традиционных границ в киберпространстве предполагает концептуализацию суверенитета с учетом технической неограниченности киберпространства. Поэтому в работе Omar с соавторами был введен термин «универсальный информационный суверенитет», обозначающий полномочия государства проводить операции по кибербезопасности для защиты своих национальных интересов в виртуальной реальности (Omar et al., 2022). Авторы показали, что определение границ государственного киберсуверенитета – это скорее политический, чем правовой процесс, поскольку каждое государство по-своему оценивает поток данных и его влияние на национальные интересы (Omar et al., 2022). Они осветили также практический аспект киберсуверенитета, выяснив его прямую связь с кибербезопасностью. Суверенитет – это легитимация операций по обеспечению кибербезопасности. Таким образом, это высшее проявление государственных интересов в киберпространстве.

Zekos отмечал, что глобальная природа Интернета переносит практику суверенитета с государств на рыночные силы, поскольку заменяет традиционную интерпретацию государственного суверенитета на понимание его как власти глобализованного рынка, обеспечивающей контроль капитала над киберпространством (Zekos, 2022). В связи с непрерывным ростом экономических выгод от глобализации киберпространства государства испытывают трудности с обеспечением своего традиционного суверенитета (Zekos, 2022). Таким образом, киберглобализация породила концепцию киберсуверенитета; это адаптация традиционного юридического понятия суверенитета в киберпространстве (Zekos, 2022). Следовательно, киберсуверенитет соответствует безграничности киберсферы, где традиционные территориальные границы полностью исчезают. Автор утверждает, однако, что государственный суверенитет в его правовой концепции тесно связан с территорией, поскольку это понятие позволяет государству устанавливать свою власть

5 The Egyptian Public Prosecution. (2020). Official Statement on Hanin Hossam's Case. https://clck.ru/39rfJM

в пределах национальных границ (Zekos, 2022). Соответственно, для установления суверенитета над государственной территорией в киберпространстве необходимо признание ее наличия. В условиях отсутствия традиционных территориальных границ автор предлагает для обеспечения государственного суверенитета применять современные методы географического цифрового отслеживания потоков данных в Интернете (Zekos, 2022). Кроме того, он приходит к выводу, что для признания своей территории в киберпространстве государствам следует использовать фактор эффекта (Zekos, 2022): любая деятельность, которая имеет какие-либо последствия на традиционной территории, устанавливает на ней государственный суверенитет. При таком толковании суды различных стран распространяют свою юрисдикцию на споры в киберпространстве. Распространение национального суверенитета на киберпространство оправдано связью между кибернетическим обществом и государством, независимо от отличий киберпространства (Zekos, 2022). Следовательно, государства могут установить свой суверенитет над электронными транзакциями и взаимодействиями, которые затрагивают их интересы. Это доказывает существование киберсуверенитета как юридического понятия.

По мнению Simmons и Hulvey, установление кибергранниц облегчает организацию и управление потоками данных между национальными киберпространствами и универсальным киберпространством с помощью национальных законов (Simmons & Hulvey, 2023). Таким образом, кибергранницы отражают стремление правительств защищать национальное киберпространство от иностранного вмешательства (Simmons & Hulvey, 2023). Поэтому границы и суверенитет – это две стороны одной медали, которая представляет собой национальную безопасность в киберпространстве.

Соблюдение киберсуверенитета – главный принцип кибероперации. Он является продолжением традиционного суверенитета, который представляет собой необходимое условие мирного сосуществования (Japaridze, 2023). Киберсуверенитет дает государствам право отслеживать незаконную деятельность в Интернете и принимать соответствующие контрмеры для сохранения своей национальной целостности в виртуальном пространстве (Japaridze, 2023). Таким образом, киберсуверенитет помогает защитить граждан от киберугроз. Однако крайние взгляды на киберсуверенитет могут привести к дроблению киберпространства до мельчайших областей (Japaridze, 2023), что противоречит первоначальному предназначению этой глобальной сферы. Поэтому суверенитет необходим в киберпространстве как определяющий фактор государственной власти для организации глобального взаимодействия.

Также стоит отметить точку зрения на киберсуверенитет как «подчинение киберпространства государственным интересам и ценностям» (Zein, 2022). Это определение говорит о наличии у государства высших полномочий по контролю и надзору за киберпространством и отражает очевидную связь между суверенитетом в киберпространстве и государственной властью. Оно также подразумевает усилия по демаркации киберпространства. Автор утверждает, что киберпространство де-факто является «универсальным всеобщим», подобно открытому морю и культурному наследию человечества (Zein, 2022). Поэтому сложно установить над ним суверенитет конкретной страны. Однако государства могут формировать свой национальный киберсуверенитет путем введения технических мер для ограничения потока данных, наблюдения за подозрительной деятельностью других государств и использования неопределенности киберпространства для противодействия этим явлениям (Zein, 2022). Кроме того, правовые последствия традиционного

суверенитета распространяются и на киберсуверенитет, поскольку государства должны обеспечивать взаимное уважение национального суверенитета при работе в киберпространстве, избегать незаконного вмешательства во внутренние дела других стран и поддерживать целостность территориального киберсуверенитета против незаконных кибератак, направленных на критическую инфраструктуру (Zein, 2022). Следует отметить, что автор подчеркивает тесную связь киберсуверенитета с безопасностью и благополучием страны, поэтому утверждает главенство политических мотивов над стремлением распространить суверенитет в его традиционной юридической интерпретации на новое инновационное киберпространство. В этом контексте A. Zhuk считает, что суверенитет в киберпространстве является чисто виртуальным и подразумевает установление государственного контроля над цифровой инфраструктурой, расположенной в пределах национальной виртуальной территории (Zhuk, 2023). Это исключительная особенность онлайн-сообществ, не имеющая связи с традиционной физической территорией.

Итак, поскольку суверенитет узаконивает действия государства по защите национальных интересов, ученые стремятся подробно описать, как эта концепция проявляется в киберпространстве. Если раньше спорили о самом существовании киберсуверенитета, то современная литература свидетельствует о его глобальном признании. Это признание проявляется в попытках интерпретировать данное понятие в техническом контексте киберпространства. Важно отметить, что при объяснении киберсуверенитета ученым удалось выделить его функциональные аспекты. Согласно определениям, суверенитет – это метод легитимизации действий государства в киберпространстве для представления своих национальных интересов. Более того, отсутствие четкого определения суверенитета может спровоцировать глобальный киберконфликт из-за пересечения полномочий между государствами. Это угрожает стабильности, необходимой для развития универсальных взаимодействий в киберпространстве. Поэтому разработка дисциплинарной детерминанты киберсуверенитета является обязательным условием для предотвращения возможных тяжелых последствий.

1.2. Тесная связь киберсуверенитета с национальными интересами

С момента своего появления в XVIII в. национальные интересы стали главным фактором, определяющим отношение государств к территориям. Государствам удавалось контролировать свои территории на основе понимания национальных интересов. Koulos утверждал, что страны, чтобы реализовать свои полномочия на определенной территории, начинают процесс ее национализации (Koulos, 2022). По мнению Cox, национальные интересы – это «совокупность убеждений, шаблонов и практик, ориентированных на народ, проживающий на ограниченной территории, и воплощенных в политических требованиях самоидентифицирующегося народа, которые могут быть или не быть реализованы в националистическом движении и самосознании» (Cox, 2021). Из этого определения можно понять, что национальные интересы некоторое время были ограничены традиционными территориальными пространствами. Однако появление Интернета устранило традиционные границы между государствами и позволило осуществлять транснациональное взаимодействие. Таким образом, национальные интересы стали завоевывать киберпространство, поскольку государства начали реализовывать планы по национализации киберпространства. В этом

аспекте необходимо изучить тесную связь между суверенитетом и национальными интересами в киберпространстве как рубеж, доказывающий необходимость демаркации киберсуверенитета государств и поиска детерминант кибергранниц государств. Кроме того, необходимо исследовать некоторые государственные правила кибербезопасности, чтобы выявить отношение государства к демаркации киберпространства.

Понимание национальных интересов не препятствует применению этого понятия в реальном мире; в Интернете некоторые взаимодействия также мотивированы национальными интересами. Неограниченная универсальная природа киберпространства породила ряд областей цифрового соперничества, управляющим фактором которого являются национальные интересы. Поэтому, несмотря на двойственную природу киберпространства, государства стремились включить его в свои национальные концепции (Koulos, 2023). Иными словами, режимы разных стран пытались подчинить киберпространство своим политическим амбициям. Например, конечный адрес URL обычно указывает на государство, в котором находится владелец домена, например, .fr для Франции, .us для США и .eg для Египта. Koulos приводит этот пример в доказательство национализации киберпространства. Глобальное изменение ценностей привело к космополитическому пониманию национальных интересов (Cox, 2021). Глобализация пробудила политические амбиции стран на доминирование в киберпространстве. Отныне, указывает Cox, безграничная сфера Интернета разжигает бурную конкуренцию между странами под флагом национальных интересов (Cox, 2021). Более того, границы в киберпространстве формируются для защиты суверенитета на национальной территории. При этом для установления национальных кибергранниц государства используют соответствующие методы. Эти механизмы отвечают специфической технической неопределенности киберпространства, что отличает их от традиционных методов демаркации границ. Интенсивная глобализация киберпространства заставляет государства концентрироваться на его территориализации, чтобы защитить свои национальные интересы от политической напряженности[6]. Национальные интересы являются главным оправданием их политики.

Поскольку киберпространство – это богатый источник информации, сверхдержавы стремятся установить над ним контроль, руководствуясь понятием киберсуверенитета[7]. Государства используют специальные технологии, чтобы укрепить контроль над национальной кибертерриторией. Они устанавливают национальный суверенитет в киберпространстве с помощью механизмов наблюдения и сбора данных, чтобы сохранить киберпревосходство для обеспечения целей экономики и безопасности (St-Hilaire, 2020). Государства могут осуществлять политическое давление на интернет-гигантов, чтобы использовать их технические возможности в политических конфликтах[8].

---

6 Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. https://clck.ru/3A7YMR

7 Там же.

8 Blenkinsop, Ph. (2022, March 3). EU bars 7 Russian banks from SWIFT, but spares those in energy. Reuters. https://clck.ru/3A7Yt8

Более того, киберпространство стало значительным полем межгосударственного противостояния из-за разнообразных противоречивых интересов, на которые влияют потоки данных (Manshu & Chuanying, 2021). Если не урегулировать эти киберконфликты, они могут вызвать тяжелые политические последствия. На практике мы видим, что такие государства, как Китай и Россия, вкладывают огромные средства в технологии для установления своего суверенитета в киберпространстве, чтобы укрепить свою кибербезопасность против доминирования западных стран. Хотя их политика может привести к дроблению киберпространства, что противоречит принципу свободной передачи данных, эти государства ставят во главу угла свои национальные интересы (St-Hilaire, 2020). Именно национальные интересы выступают двигателем этой политики, что свидетельствует об их тесной связи с киберсуверенитетом. Ярким примером связи между киберсуверенитетом и национальными интересами является обещание Хиллари Клинтон ликвидировать цифровой железный занавес, установленный Китаем для контроля потока данных в Интернете (St-Hilaire, 2020). Это соревнование между странами за господство в киберпространстве мотивировано национальными интересами и направлено на обеспечение киберпревосходства страны. Кроме того, в США был создан Штаб кибероперaций – рабочая группа для защиты национальных интересов США в киберпространстве от иностранных угроз[9]. После этого, в 2014 г., руководство Китая объявило об активизации работы по завоеванию господства в киберпространстве (Segal, 2014). Соревнования между странами за доминирование в киберпространстве представляют собой гонку вооружений между сверхдержавами за обладание этим важным ресурсом.

Следует отметить, что значимость киберпространства побуждает государства стремиться к доминированию в этой сфере. При этом они руководствуются идеями национального превосходства в киберпространстве. Этот факт подразумевает, что государства стремятся установить границы в киберпространстве для обеспечения национальных интересов и защиты суверенитета. Благодаря этому в киберпространстве представлена концепция национальных интересов, что доказывает ее тесную связь с понятием киберсуверенитета. Действительно, защита национальных кибергранниц предполагает разработку механизма установления этих границ в киберпространстве.

1.3. Демаркация киберпространства: необходимость в детерминанте

Как следует из сказанного, судебная практика признает, что установление границ в киберпространстве необходимо для определения пределов национального суверенитета с целью предотвратить возможные конфронтации. Существование кибергранниц является основой киберсуверенитета, что придает особую важность их демаркации. В реальном мире демаркация межгосударственных границ не является препятствием, поскольку государства используют традиционные инструменты, принятые и утвержденные международным правом. Более того, национальные интересы подразумевают установление четких государственных границ для обеспечения национальной обороны в киберпространстве. Однако из-за технически неоднозначной природы киберпространства процесс установления государственных границ существенно усложняется.

[9] Command (2010), Our Mission and Vision. https://clck.ru/3A7XsQ

Общеизвестно, что территория государства является пространством его исключительной власти, которое ограничено признанными и четкими границами, представляющими собой государственные политические границы (Ahmed, 2021). Традиционно границы указывают на пределы, в которых государство может использовать свою власть. Таким образом, демаркация видимых границ между странами и территориями имеет решающее значение для стабильности и мирного сосуществования; она предотвращает незаконные вмешательства между государствами. Поскольку невозможно представить себе государство без территории, то и территория без границ существовать не может, так как целостность и признание территории зависят от установления ее очевидных и стабильных границ. На традиционных границах работают разрешительные правовые механизмы, обеспечивающие надзор за физическим перемещением людей и товаров, например, въездные и выездные визы, таможни, пограничные и береговые службы (Simmons & Hulvey, 2023).

Аналогичным образом, демаркация киберпространства занимает важное место в политике защиты государственных интересов. Страны имеют законное право устанавливать свой суверенитет против кибератак, направленных на национальную инфраструктуру. Кроме того, киберсуверенитет является одной из главных проблем уголовного правосудия, поскольку национальные судебные органы обязаны уважать суверенитет других стран при сборе доказательств в Интернете (Sallavaci, 2020). В целях сохранения киберсуверенитета трансграничное судопроизводство должно быть организовано на основе многосторонних или двусторонних договоров. Таким образом, ученые признают, что киберсуверенитет необходим для уголовного правосудия. Этот факт требует разработки соответствующего механизма установления границ в киберпространстве. Однако стремительная динамика киберпространства, обусловленная огромными потоками данных, затрудняет установление четких политических границ (Abdelrahman & Mekhiemer, 2022). В отличие от традиционных границ в киберпространстве ограничить территорию государства крайне сложно из-за отсутствия дисциплинирующей детерминанты. Следование традиционным межгосударственным границам стало нереалистичным из-за глобального характера киберпространства (Ahmed, 2021).

Чтобы маркировать свою кибертерриторию, государства используют традиционные метафоры для реагирования на иностранные киберугрозы (Simmons & Hulvey, 2023). Этот подход обусловлен территориальным мышлением государств в отношении киберпространства. Они рассматривают киберпространство как территорию, на которой можно доминировать и осуществлять суверенный контроль. Такие методы, как локализация данных, блокировка сайтов и судебные запросы о сотрудничестве, символизируют сочетание технологий и права для демаркации киберпространства. Это же отношение отражает определение кибергранич, данное Osborn. Однако опора на техническую составляющую для установления четких границ в киберпространстве может оказаться недостаточной из-за быстрого развития интернет-технологий, которое может столкнуться с медленным процессом внесения изменений в законодательство. Таким образом, становится актуальной разработка устойчивой детерминанты кибергранич. В данном исследовании представлена концепция государственных интересов как детерминанты кибергранич.

2. Использование концепции государственных интересов для демаркации киберпространства

2.1. Сущность концепции

Понятие «человеческий интерес» относится к потребностям, которые люди стремятся удовлетворить для своего благополучия. Эти потребности не являются чисто индивидуальными, они имеют социальные характеристики, обусловленные их вкладом в общественные отношения. Кроме того, они не являются абсолютными из-за ограничений производственных возможностей (Wang, 2022). Через свои основания интересы демонстрируют социальную трансформацию человеческих потребностей и тесную связь между людьми в определенном поле взаимодействий. Они являются детерминантами человеческих отношений, которые объединяют их в одних ситуациях и разделяют в других. Из-за разнообразия факторов интересы могут создавать противоречия между социальными группами, т. е. государствами (Wang, 2022). Интересы являются отправной точкой для создания политических, экономических и социальных связей внутри сообщества (Wang, 2022). Cox утверждал, что интересы стали главной осью общественных наук благодаря их вкладу в концепцию коллективных эмоций в сообществе (Cox, 2021). Таким образом, интересы – это эффективное выражение коллективной мотивации группы, которая побуждает государственную власть реагировать для их защиты.

Что касается государств, то их интересы как социальное явление означают национальные требования, которые удовлетворяют внутренние потребности в противовес интересам других государств. Поскольку страны могут различаться в установлении своих интересов, возникает конфликт интересов. Таким образом, интересы определяют, как ведут себя государства, чтобы обеспечить свои потребности. В приложении к киберпространству это означает, что каждое государство будет вести себя в Интернете так, чтобы удовлетворить свои национальные потребности; киберповедение государств будет соответствовать их интересам.

Государственные интересы – это общие интересы, поскольку они формируются на основе групповых потребностей (Wang, 2022). В киберпространстве понятие государственного интереса как общего интереса имеет следующие основные характеристики: публичность, реализация через цепочку поставок продукции, единство, включение фундаментальных ценностей и независимость (Wang, 2022). Это основные детерминанты государственных интересов как концепции.

2.2. Политические и правовые последствия концепции государственных киберинтересов

По мнению Fang, национальный суверенитет в киберпространстве – это политический интерес государства (Fang, 2018), и когда государство устанавливает свою власть над кибертерриторией, оно защищает национальные киберинтересы. Иными словами, установление политических границ в киберпространстве и утверждение национального суверенитета в их пределах отражает использование концепции государственных интересов для определения и поддержания кибергранниц. Еще одним примером подчинения кибердипломатии государственным интересам является противоречие между США и Китаем. В то время как США борются за неограниченное киберпространство, поскольку достижение их национальных интересов требует

свободного потока данных, Китай стремится установить строгие кибергранницы, чтобы защитить свою кибернезависимость (Fang, 2018). Этот пример подчеркивает критическое влияние концепции национальных интересов на киберполитику государств. Государство может ввести принудительную обработку данных, чтобы обеспечить легитимность обмена данными в пределах своих кибергранниц и отслеживать незаконную кибердеятельность (Paice & McKeown, 2023). Такая практика способствует укреплению целостности национальной кибертерритории и реализации концепции киберсуверенитета. В этом выражается важнейшая роль концепции государственных интересов в обеспечении безопасности кибергранниц. В частности, государственные интересы являются главной мотивацией в киберпространстве (Cox, 2021); когда киберинтересы страны оказываются под угрозой, вмешательство государства становится обязательным для защиты целостности национальных благ. Этот вывод соответствует сути суверенитета и национальных интересов в киберпространстве. Более того, угроза киберинтересам государств провоцирует кибервойну, которая включает в себя взаимные кибератаки через кибергранницы для защиты своих экономических и военных объектов (Fang, 2018). Угрозы киберинтересам требуют срочной реакции государства, а противостояние им направлено на защиту национальных интересов.

В докладе Счетной палаты США от 2024 г. указывалось на острую необходимость разработки четких механизмов кибердипломатии для защиты государственных интересов в киберпространстве[10]. Тем самым правительство официально признало концепцию государственных киберинтересов и ее использование для планирования национальной дипломатии в киберпространстве. Таким образом, концепция государственных киберинтересов утвердилась в политике и дипломатии. Аналогичным образом ЕС использует совместную кибердипломатию, которая поддерживает совместные киберинтересы Евросоюза (Reiterer, 2022). Звучат призывы внедрять в ЕС самые передовые технологии для защиты киберинтересов Союза в условиях непрерывного развития конкурирующих кибердержав (Reiterer, 2022). Киберинтересы стали заметным элементом при разработке крупных национальных стратегий.

С юридической точки зрения общепризнано, что киберпространство – это виртуальная сфера глобальных взаимодействий, которая порождает реальные отношения между государствами. Кибервзаимодействие оказывает влияние на человеческие отношения в реальном мире. Этот факт вызывает необходимость регулирования киберпространства, обеспечивая правовые рамки для таких взаимодействий (Fang, 2018). Таким образом, государства внедряют свое законодательство в киберпространстве, чтобы защитить свои национальные интересы.

2.3. Судебные интерпретации концепции государственных киберинтересов

Контекстуализация концепции государственных киберинтересов представляет не только научный интерес. Изучение судебной практики, в том числе киберсудебных процессов, позволяет выяснить, как национальные судебные органы использовали эту концепцию для разрешения киберспоров.

[10] 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

В деле State v. Hunt (2020) судебная система США занималась проблемой детской порнографии в Интернете. Важность решений по этому делу обусловлена угрозой эксплуатации несовершеннолетних. Так, по утверждению суда, в соответствии с 18 U.S.C. § 2252A, хранение порнографических материалов выражает преступное намерение обвиняемого просмотреть их. В решении отражено, что введение национального законодательства в киберпространстве стало следствием реализации государственных киберинтересов, а именно искоренения детской порнографии в Интернете. Аналогичным образом, в деле People v. Jacobo (2019) суд применил определение онлайн-торговли людьми и разрешение на преследование по составу этого преступления, установленное Законом штата Калифорния против сексуальной эксплуатации (Californians Against Sexual Exploitation Act, CASE) от 2012 г. таким образом, чтобы правоохранительные органы могли преследовать эту деятельность, если в нее вовлечен гражданин США. Это очевидное расширение кибергранespecially США, поскольку этого требуют государственные интересы. В деле Democratic Nat'l Comm. v. Russian Fed'n (2019) американский суд также встал на защиту целостности избирательного режима от зарубежных кибератак, которые угрожали демократической системе США. Кроме того, судебное разбирательство может быть возбуждено в экономических киберинтересах государства, как в деле Regina v Cory Aguilar (2018); суд Великобритании счел, что вред, нанесенный истцу мошеннической деятельностью ответчика в Интернете, достаточен для признания его виновным и заключения в тюрьму. Дело Regina v Stephen Brownlee (2020) было посвящено противодействию контрабанде через Интернет. Судебные органы Великобритании одобрили преследование неназванных веб-сайтов, которые использовались контрабандистами в качестве платформ для обмена нелегальными товарами. Эти сайты были признаны точками нарушения государственных границ и приговорены к уничтожению для защиты национальных интересов.

В делах Lifestyle Equities CV v Amazon UK Services Ltd. (2021) и Tunein Inc v Warner Music UK Limited, Sony Music Entertainment UK Limited (2021) судебные органы Великобритании встали на защиту творческой сферы своей страны, противостоя незаконной онлайн-торговле нелицензионными материалами и произведениями искусства. Несомненно, такие материалы наносят моральный и финансовый ущерб владельцам авторских прав, защита которых представляет собой важнейший государственный интерес в соответствии с Законом Великобритании об авторском праве, промышленных образцах и патентах от 1988 г.

Американский судья О'Сканлиан в деле Robins v. Spokeo (2017) счел, что неверный отчет о бизнесе в Интернете нарушает Закон США об объективной кредитной отчетности (US Fair Credit Reporting Act), давая истцу право на компенсацию. Аналогичным образом суд Великобритании признал то же право в деле Ghannouchi v Middle East Online Ltd & Anor. Таким образом, суд борется с распространением неверной информации на веб-сайтах и защищает достоверность национальных СМИ.

В заключение отметим, что, согласно рассмотренным решениям, судебные органы признают существование концепции кибергранic и связывают ее с концепцией государственных интересов. Такая функциональная интерпретация означает, что государственные кибергранicы устанавливаются в соответствии с государственными интересами в киберпространстве; если имеется интерес, то государство может расширять свой киберсуверенитет для его защиты. Однако судебные решения не содержат нормативного определения кибергранic; защищаемые интересы – это государственные кибергранicы в соответствии с функциональной интерпретацией, которая согласуется с определением Osborn (2017) и Zein (2022).

3. Пригодность концепции государственных интересов для демаркации киберпространства

3.1. Основания пригодности

Нет нужды говорить о том, что в киберпространстве до сих пор нет четкого определения концепции границ. Государства используют различные механизмы для защиты своих национальных интересов. Разнообразие внутренней киберполитики противоречит универсальности киберпространства, стабильность которого требует единых норм. Отсутствие многосторонних конвенций о демаркации киберпространства, конкуренция политических киберинтересов, разнообразие национальных интерпретаций правовых понятий, проблемы установления авторства и ответственности в киберпространстве – вот главные препятствия на пути принятия концепции глобальной детерминанты кибергранич[11]. В связи с отсутствием механизма правовой демаркации мы вводим понятие государственного интереса как необходимой детерминанты.

В качестве глобального всеобщего киберпространство требует введения общепризнанного стандарта для определения политических границ. Следует помнить, что чисто техническая природа киберпространства не препятствует контекстуализации правовых понятий в этой сфере. Традиционная концепция суверенитета распространяется на киберпространство, но в форме, соответствующей его технической природе (Choucri & Clark, 2013). Сочетание права и технологии стало основной проблемой, которая стояла перед учеными, пытавшимися разработать нормы для демаркации киберпространства. Эта проблема, как было показано ранее, побудила Osborn использовать чисто технический подход к определению кибергранич. Однако развитие науки дает нам возможность увязать концепции границ и суверенитета в киберпространстве с концепцией государственных интересов.

Ключом к успешной интеграции правового понятия в цифровую среду является адаптивность (Akhmatova & Akhmatova, 2020). Это вызов, который стоит перед легализацией киберпространства и управлением им. Адаптивность концепции государственных интересов к технически неопределенной природе киберпространства очевидна. Поскольку киберпространство удовлетворяет самые разные человеческие потребности, концепция интересов формируется через методы, принятые государствами для удовлетворения этих потребностей. Как указывает Wang (2022), интересы – это истинное выражение социальной жизни сообществ; они являются двигателем социальных взаимодействий между людьми. Поэтому они должны быть приоритетом при установлении границ между группами. Таким образом, концепция государственных интересов в киберпространстве эволюционирует, достигая пределов государственной киберполитики. Адаптивность ее компонентов к кибервзаимодействию позволяет использовать эту концепцию в качестве детерминанты государственной власти в киберпространстве.

[11] Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. https://clck.ru/3A7ZPU

Кроме того, главными мотивами вмешательства государств в киберпространство являются национальные интересы. Изучение китайского и западного подходов демонстрирует их поспешные попытки сформировать свой киберсуверенитет в соответствии с национальными интересами, которые они стремятся защищать в киберпространстве. В частности, четкое присутствие национальных интересов в киберпространстве побуждает государства использовать свои внутренние правовые инструменты для защиты своих киберинтересов. Согласно анализу Benabid[12] и Paice и McKeown (2023), интересы государств являются активными двигателями национальной политики в киберпространстве. Эти факты доказывают приоритетность государственных киберинтересов на национальном уровне, что находит отражение в реализации этой концепции на политической арене.

С точки зрения судебной практики, решения национальных судов по киберспорам позволяют квалифицировать концепцию государственных интересов для определения кибергранич. Судебные органы США и Великобритании распространили свою юрисдикцию на киберпространство в тех случаях, когда существует угроза национальным интересам. Поскольку юрисдикция отражает суверенитет, национальные суды устанавливают национальный суверенитет в той степени, в которой затрагиваются государственные интересы. В этой интерпретации концепция государственных интересов используется в качестве детерминанты киберсуверенитета государства и, как следствие, его кибергранич.

3.2. Практические основы демаркации

После создания правовой основы для использования концепции государственных киберинтересов для определения кибергранич необходимо разработать практическую базу для этого процесса. В статье представлено несколько методов использования этой концепции в качестве детерминанты границ.

Ввиду универсальности киберпространства предлагается через использование конвенций и других механизмов развивать обычное международное право, поддерживая адаптивность правовых понятий к технической природе киберпространства[13]. При этом государства должны вступать в соглашения о принятии концепции государственных интересов для установления кибергранич. Регулирование киберпространства требует универсальных механизмов, поскольку односторонняя политика может поставить под угрозу глобальные усилия по регулированию. Кроме того, многосторонние договоренности обеспечивают международный консенсус в отношении принятия государственных киберинтересов для демаркации киберпространства. Как следствие, концепция государственных киберинтересов приобретет дисциплинарный характер, что повысит ее вклад в управление киберпространством.

---

12 Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. https://clck.ru/3A7YMR

13 Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. https://clck.ru/3A7ZPU

Ключом к преодолению технико-юридических дилемм должны стать инновации (Linden & Shirazi, 2023). Ученым необходимо углублять традиционное понимание правовых понятий, адаптируя их к техническим контекстам, таким как киберпространство. Кроме того, инновации являются основой современных кибероперaций, поскольку они предоставляют государствам выгодные возможности в киберпространстве (Soare, 2023). Что касается судебной сферы, то в попытке преодолеть техническую природу киберспоров суды разных стран используют технические инструменты наряду с традиционными правовыми понятиями. Этот уникальный механизм защиты кибергранниц основан одновременно на праве и технологиях. Такая гибридная структура обеспечивает этому механизму гибкость, позволяющую адаптировать правовые концепции к техническому киберпространству. Кроме того, гибкость повышает возможности национальных судов противостоять киберугрозам. Инновации – это ключ, который позволяет судам преодолеть технические трудности киберспоров и застой в законодательстве, объединив право и технологии.

Стремительные, скачкообразные изменения дискурса предполагают преодоление препятствий за счет выхода за пределы существующей реальности. Опора исключительно на реалистичные логические рассуждения при разрешении технико-правовой дилеммы ставит юристов в тупик. В этом случае важнейший вклад в развитие правовой доктрины вносит воображение. В правовом аспекте именно воображение предоставляет ученым впечатляющие, убедительные и инновационные возможности для преодоления традиционных трудностей (d'Aspremont, 2022). Правовое воображение представляет собой мощный инструмент против юридической бюрократии; это «мышление о невозможном ради преодоления» (d'Aspremont, 2022). Кроме того, воображение, с точки зрения права, расширяет возможности юристов по переосмыслению существующих норм в гибких технологических средах, где изменения происходят быстро и неупорядоченно (Pollicino, 2020). Таким образом, воображение юриста позволяет изменять традиционные правовые понятия в соответствии с быстро развивающимися техническими сферами, такими как киберпространство. Следует отметить, что концепции границ и суверенитета также родились когда-то в воображении, а затем успешно интерпретированы и включены в реалистичные правовые контексты с помощью инновационных технико-правовых принципов, заложенных в эти решения и интерпретации. Аналогичным образом, концепция государственных киберинтересов, благодаря правовому воображению, может быть эффективно контекстуализирована в киберпространстве для установления границ и суверенитета. В вышеупомянутых судебных решениях эта концепция использовалась для определения объема национальной юрисдикции, что прямо подразумевает государственный суверенитет в пределах национальных границ. Следовательно, можно сделать вывод, что государственные кибергранницы распространяются на каждую точку киберпространства, где затрагиваются государственные интересы. Такая интерпретация отражает гибкость концепции государственных интересов, соответствуя неопределенной природе киберпространства, где технически сложно соблюсти жесткие нормы. Таким образом, воображение позволяет воссоздать традиционные правовые понятия в киберпространстве, наделив их эффективным свойством адаптации к киберпространству – гибкостью.

Заключение

Суммируя вышесказанное, следует отметить, что киберпространство оказалось неспособным противостоять установлению границ с помощью традиционных методов демаркации, принятых для обозначения границ в реальном мире. Попытки ученых описать суверенитет и границы в киберпространстве с разных точек зрения породили противоречивое понимание этих понятий. Указанные противоречия дестабилизируют универсальные отношения в киберсфере. Для преодоления этой дилеммы нами предпринята попытка разработать современный правовой механизм определения суверенитета и границ в киберпространстве.

В отличие от других научных работ в данном исследовании для определения технического понятия используется чисто юридическая концепция. В качестве инструмента демаркации киберпространства в нем представлена концепция государственных киберинтересов. Эта концепция подразумевает установление связи между национальным суверенитетом в киберпространстве и любым воздействием на национальные интересы. Что касается функциональности концепции государственных интересов, в исследовании показана ее адаптируемость к технической природе киберпространства, что позволяет преодолеть традиционные препятствия на пути интеграции юридического понятия в техническую среду. Кроме того, в работе предложены механизмы, обеспечивающие применимость данной гипотезы.

Список литературы

Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, *16*(15), 423–443. (In Arabic). https://doi.org/10.21608/jocu.2022.134235.1172

Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, *2*(6), 632–646. (In Arabic).

Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, *5*, 6. https://doi.org/10.1186/s41018-020-00076-2

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

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

d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, *35*(4), 1017–1027. https://doi.org/10.1017/s0922156521000637

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

Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13

Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, *1*, 119. https://doi.org/10.12688/openreseurope.14010.2

Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, *9*, 22. https://doi.org/10.1186/s40854-022-00432-8

Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, *3*, 97–114. https://doi.org/10.1007/s42533-021-00079-7

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

Omar, M. O., AlDajani, I. M., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.

Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity, Springer, Singapore*. https://doi.org/10.1007/978-981-19-6414-5_1

Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online. Edward Elgar Publishing*. https://doi.org/10.4337/9781788976688.00009

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. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1

Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.

Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship, 3158*.

Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. https://doi.org/10.4324/9781003284093-6

St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-61386-0

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

Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, *3*(3), 679–738. https://doi.org/10.21608/ijdjl.2022.138565.1159 (In Arabic).

Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*, 45. https://doi.org/10.1007/s44206-023-00067-x

Сведения об авторе

Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре, Министерство юстиции Египта
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел
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: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 21 сентября 2023 г.
Дата одобрения после рецензирования – 12 октября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:342.3:004.9
EDN: https://elibrary.ru/sywsrk
DOI: https://doi.org/10.21202/jdtl.2024.14

Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests

Yassin Abdalla Abdelkarim
Luxor Elementary Court, Sohag, Egypt

Keywords

border,
cyber interest,
cyber security,
cyber sovereignty,
cyberspace,
digital technologies,
law,
national interest,
sovereignty,
state

Abstract

Objective: to substantiate the existence of national cyber sovereignty as a legal concept; by introducing the concept of state cyber interests as an innovative determinant, to review the traditional concepts of national sovereignty and state borders in the context of the dynamic nature of cyberspace and the need to develop a hybrid mechanism for cyber borders protection, based simultaneously on law and technology.

Methods: the doctrinal method was used to identify the basic discrepancies in the views of leading scientists in different fields on fundamental theoretical-methodological, conceptual and categorical issues, including the justification of a single algorithm for establishing borders in cyberspace. The doctrinal method is supplemented by the analysis of judicial practice of different countries, which allows considering the courts extending their jurisdiction to disputes related to cyberspace.

Results: the study presents the application of traditional and modern legal concepts of sovereignty in the new digital environment, resulting in a combination of legal and technological approaches. The author reveals functional significance of the concept of state cyber interests for demarcating cyberspace and defining the boundaries of national sovereignty. The adaptability of this concept to the technically uncertain nature of cyberspace is shown. The conclusion is made about the main directions in forming the concept of cyber interests in cyberspace and its political and legal implications, based, among other things, on the practice of courts of different countries in resolving cyber disputes.

Scientific novelty: the concept of state cyber interests is considered as an innovative method of defining cyber borders. It leads to the transformation of the traditional sovereignty concept and the close national interest concept in relation to cyberspace in the context of fulfilling security requirements and intensifying national defense against cyber threats.

Practical significance: the obtained results eliminate existing contradictions in the definition of sovereignty and its spatial limits under the modern technology development; contribute to the elaboration of a disciplinary standard of cyber sovereignty based on a reliable demarcator necessary for the definition of state sovereignty and borders in cyberspace; adapt traditional legal concepts of sovereignty and national interests to the global modern cyber challenges; contribute to the transformation of traditional legal concepts of sovereignty and national interests in cyberspace.

For citation

Abdelkarim, Y. A. (2024). Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests. *Journal of Digital Technologies and Law, 2*(2), 376–399. https://doi.org/10.21202/jdtl.2024.20

References

Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, *16*(15), 423–443. (In Arabic). https://doi.org/10.21608/jocu.2022.134235.1172

Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, *2*(6), 632–646. (In Arabic).

Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, *5*, 6. https://doi.org/10.1186/s41018-020-00076-2

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

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

d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, *35*(4), 1017–1027. https://doi.org/10.1017/s0922156521000637

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

Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13

Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, *1*, 119. https://doi.org/10.12688/openreseurope.14010.2

Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, *9*, 22. https://doi.org/10.1186/s40854-022-00432-8

Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, *3*, 97–114. https://doi.org/10.1007/s42533-021-00079-7

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

Omar, M. O., AlDajani, I. M., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.

Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity, Springer, Singapore*. https://doi.org/10.1007/978-981-19-6414-5_1

Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online. Edward Elgar Publishing*. https://doi.org/10.4337/9781788976688.00009

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. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1

Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.

Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship, 3158*.

Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. https://doi.org/10.4324/9781003284093-6

St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-61386-0

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

Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, *3*(3), 679–738. https://doi.org/10.21608/ijdjl.2022.138565.1159 (In Arabic).

Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*, 45. https://doi.org/10.1007/s44206-023-00067-x

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – September 21, 2023
Date of approval – October 12, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.15

Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления

Гульбакыт Болатбеккызы

Уханьский университет, Ухань, Китай

Ключевые слова

государственное управление,
защита данных,
кибербезопасность,
конфиденциальность,
персональные данные,
права человека,
право,
трансграничность,
цифровизация,
цифровые технологии

Аннотация

Цель: определить основные юридические факторы трансграничного обмена данными в контексте распространения цифровых технологий и цифровизации государственного управления, включая правовые гарантии, проблемы безопасности, риски кибербезопасности, подходы к регулированию и повышению эффективности управления данными в разных юрисдикциях.

Методы: исследование опирается на синтез и критический анализ различных аспектов заявленной проблемы, в том числе на анализ как первичных, так и вторичных источников. На примере сравнения политики регулирования Китая, США, ЕС и государств-членов ЕАЭС сопоставляются различные подходы относительно ограничения или поощрения свободной трансграничной передачи данных. Комплексный мета-анализ и оценка литературы позволили сформировать представление о методах, используемых для защиты данных в разных юрисдикциях, а также обозначить рамки и направления государственной политики, необходимые для эффективной передачи данных между юрисдикциями.

Результаты: выявлены основные проблемы, связанные с трансграничной передачей данных в контексте распространения цифровых технологий и цифровизации управления, такие как растущее неравенство в развитии цифровых технологий, правовая неопределенность, обеспечение конфиденциальности и кибербезопасности и др. Проанализированы правовые основы трансграничной передачи данных в контексте цифровизации государственного управления и практика их реализации, что способствовало поиску путей повышения эффективности управления в условиях транснациональной передачи данных, включая предоставление услуг, развитие открытости и участия общественности.

Научная новизна: на основе проведенного анализа подходов различных юрисдикций к проблемам юридического характера, вопросам обеспечения безопасности и суверенитета, обусловленным трансграничной передачей данных, выявлены роль и применимость международного права, а также уникальные вызовы, возникающие в государствах-членах Евразийского экономического союза на пути формирования трансграничного пространства доверия.

Практическая значимость: исследование указанных вопросов имеет значение для выработки и принятия взвешенных политико-правовых решений государственными структурами, прежде всего правительственными и законодательными органами, направленных на достижение баланса между доступностью данных и их безопасностью, между эффективностью государственного управления и соблюдением прав граждан. Полученные результаты будут иметь значение также для иных субъектов отношений, связанных с трансграничной передачей данных и вопросами регулирования указанных отношений.

Для цитирования

Болатбеккызы, Г. (2024). Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления. *Journal of Digital Technologies and Law*, *2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Содержание

Введение

Трансграничная передача данных в контексте цифровизации управления подразумевает передачу персональных или конфиденциальных данных через государственные границы для достижения различных целей, включая оказание государственных услуг, развитие международных партнерских отношений и обмен данными между государственными учреждениями и частным сектором. Передача данных через границы в рамках цифровизации управления необходима для повышения качества государственных услуг и развития международного сотрудничества. Эта практика играет важную роль в развитии как государственных услуг, так и глобального сотрудничества.

Однако при этом возникают проблемы юридического характера, вопросы безопасности и суверенитета, которые необходимо решать на основе международных соглашений и надежных мер в области защиты данных. Достижение баланса между доступностью и безопасностью данных – сложная задача, требующая от правительств тщательной работы по соблюдению прав граждан и международных правовых рамок.

Кроме того, в настоящее время не существует ни одного закона или нормативного акта, касающегося трансграничной передачи или регулирования данных, который мог бы быть согласован на глобальном уровне и единогласно одобрен членами международного сообщества. Ситуация усугубляется из-за растущего неравенства в распространении цифровых технологий, которые до сих пор не доступны в равной степени для всех стран, независимо от их ВВП.

1. Трансграничная передача данных и ее значение для цифровизации государственного управления

1.1. Категоризация трансграничной передачи данных

Выделяют четыре основные категории трансграничной передачи данных. Во-первых, это межправительственный обмен данными (Government to Government, G2G), то есть обмен данными между государственными структурами отдельных стран, служащий таким целям, как дипломатическое сотрудничество, координация действий правоохранительных органов и реагирование на стихийные бедствия. Это общепринятая практика, когда международные правоохранительные органы обмениваются данными для борьбы с глобальной преступностью. Например, Европол призван способствовать обмену информацией между европейскими правоохранительными органами для борьбы с организованной преступностью и терроризмом (De Moor & Vermeulen, 2010). Во время международных кризисов правительства сотрудничают друг с другом, обмениваясь данными для управления мероприятиями по ликвидации последствий стихийных бедствий и оказанию гуманитарной помощи. Например, Управление ООН по координации гуманитарных вопросов (Office for the Coordination of Humanitarian Affairs, OCHA) способствует обмену данными во время чрезвычайных гуманитарных ситуаций (Bennett, 2002).

Вторая категория – это обмен данными между правительством и бизнесом (Government to Business, G2B), в ходе которого государственные структуры передают данные организациям частного сектора для содействия сотрудничеству между государственным и частным секторами или в целях приватизации государственных

функций (например, передача налогового администрирования частным компаниям). Для обеспечения беспрепятственного транзита товаров через международные границы государственные структуры и таможенные органы обмениваются данными, относящимися к международной торговле и таможне, включая данные об отправлениях и грузовых декларациях. Чтобы исключить двойное налогообложение компаний и частных лиц, налоговые органы разных стран могут обмениваться информацией о налогоплательщиках в рамках соглашений о предупреждении двойного налогообложения (Niu et al., 2021).

Третье направление – обмен данными между правительством и частными лицами (Government to Citizen, G2C). Это трансграничная передача данных граждан для получения международных услуг (например, доступа к медицинскому обслуживанию за рубежом). Когда граждане одной страны выезжают за границу, их медицинские карты могут быть доступны на международном уровне для обеспечения соответствующего медицинского обслуживания. Например, инфраструктура цифровых услуг электронного здравоохранения Европейского союза (eHealth Digital Service Infrastructure, eHDSI) позволяет гражданам ЕС получать доступ к медицинским данным во время поездок по территории ЕС (Bruthans & Jiráková, 2023).

Правовая база и соответствующая практика играют важную роль при трансграничной передаче данных в цифровом управлении; сюда включаются законы о защите данных и международные соглашения в этой области. Согласно законам о защите данных их передача должна осуществляться в соответствии с правилами защиты данных как страны происхождения, так и страны-получателя. В качестве примера можно привести Общий регламент Европейского союза по защите данных, который устанавливает строгие требования к трансграничной передаче данных, уделяя особое внимание определению соответствия стандартным условиям договора и обязательным корпоративным правилам. Стоит упомянуть и Китайский закон о защите личной информации (Personal Information Protection Law, PIPL), который также имеет экстерриториальное действие и устанавливает требования как для государственного, так и для негосударственного сектора. Что касается международных соглашений, то между некоторыми странами заключены двусторонние соглашения, регулирующие передачу данных. В частности, таковой являлась Программа по защите конфиденциальности ЕС–США (EU-U.S. Privacy Shield), которая способствовала обмену данными между ЕС и США, пока не была отменена в результате рассмотрения дела Schrems II.

Вопросы суверенитета и локализации данных становятся одними из самых сложных в области трансграничной передачи данных. Некоторые страны вводят требования по локализации данных, согласно которым определенные категории данных должны храниться на их территории. Например, согласно российским нормам, персональные данные российских граждан должны храниться на серверах, расположенных на территории России (Gurkov, 2021). Другой пример – недавняя ситуация с российским филиалом Yandex.kz в Казахстане[1], когда министерства и представители компании Yandex приняли решение о физическом переносе серверов в Казахстан после инцидента с блокировкой сайта на территории Казахстана из-за нежелания компании соблюдать условия соглашения.

[1] «Яндекс» переносит свою инфраструктуру в Казахстан под угрозой блокировки. (2023, 21 августа). CNews. https://clck.ru/39o7xf

При передаче данных через границы стран одинаково важны безопасность и кибербезопасность. Данные должны быть защищены от нежелательного доступа или утечки. Чтобы гарантировать конфиденциальность и безопасность передаваемых данных, необходимо использовать шифрование, безопасные протоколы и надежные меры кибербезопасности.

Повышение качества государственных услуг и развитие международного сотрудничества в рамках цифровизации государственного управления требуют трансграничного обмена данными. Однако при этом возникают проблемы, связанные с суверенитетом, безопасностью и правом, которые должны быть решены с помощью международных соглашений и надежных протоколов защиты данных. Поиск баланса между доступностью и безопасностью данных – сложный процесс, требующий от правительств осторожности при соблюдении прав своих граждан и следовании международным правовым нормам.

1.2. Проблемы конфиденциальности и безопасности данных при их трансграничной передаче

Трансграничная передача данных в контексте цифровизации управления вызывает серьезные опасения в отношении конфиденциальности и безопасности данных. Эти опасения обусловлены различными факторами, включая правовые гарантии, проблемы безопасности, риски кибербезопасности, сложности юрисдикции, сложность законодательных решений и необходимость надежного управления данными. Эффективное решение этих проблем требует внедрения правовых протоколов, тактик кибербезопасности и процедур управления данными, направленных на защиту частной информации граждан в условиях все большего распространения цифровых технологий.

По мере развития новых передовых технологий граждане ожидают все более продвинутых услуг и улучшения различных аспектов жизни. Технологический прогресс позволяет находить более эффективные решения существующих проблем, но при этом возникают новые проблемы, связанные с безопасностью и неприкосновенностью частной жизни. Цифровизация информационных ресурсов создает дополнительные проблемы в области цифровых данных и инфраструктуры. В то время как развитые страны внедряют надежные меры безопасности и методы оптимизации, развивающиеся страны по-прежнему сталкиваются с трудностями в решении этих вопросов[2].

Трансграничная передача данных предполагает соблюдение правовых норм и требований, необходимых для беспрепятственного перемещения данных. Эти нормы распространяются как на передачу данных внутри организации, работающей вне национальных границ, так и на передачу данных между организациями в разных странах. Например, во многих юрисдикциях, включая ЕС, Великобританию и Китай, установлено требование, согласно которому для обеспечения безопасной и законной передачи данных из одной страны в другую страна-получатель должна обеспечивать стандарты конфиденциальности личной информации, как минимум, эквивалентные

[2] UNGA. Nearly Half of the World's Population is Excluded from 'Benefits of Digitalization', the Speaker stresses as the Second Committee Debates Information Technology for Development. https://clck.ru/39o86M

стандартам страны-отправителя. Только в этом случае орган регулирования конфиденциальности данных или иной орган управления (в ЕС это Европейская комиссия) может вынести решение, позволяющее беспрепятственно передавать данные через границы.

2. Обеспечение безопасности и эффективности при трансграничной передаче данных

2.1. Механизмы обеспечения безопасности трансграничной передачи данных

Для того чтобы всесторонне осветить современную ситуацию с безопасностью при трансграничной передаче данных, рассмотрим практику применения различных норм. Хотя глобальной системы сертификации адекватности защиты данных при их трансграничной передаче не существует, многие страны и региональные группы стран внедрили свои собственные правила и положения для контроля в этой области. Выделяют пять самых распространенных подходов:

1. Заключения о признании адекватности защиты: передача данных разрешена в регионы, в которых, согласно заключению государственных органов, стандарты защиты данных соответствуют или превосходят стандарты страны происхождения. Общий регламент ЕС по защите данных гласит, что за выдачу заключений об адекватности защиты отвечает Европейская комиссия. Исследование, проведенное Международной ассоциацией специалистов в области защиты информации (International Association of Privacy Professionals, IAPP), показало, что в 74 юрисдикциях принята норма, по которой государственные организации, такие как регуляторы конфиденциальности данных или иные правительственные структуры, уполномочены выдавать заключения об адекватности защиты при передаче данных[3]. Важно понимать, что эти заключения не всегда являются окончательными и могут быть пересмотрены в связи с изменением обстоятельств или модификацией законов о защите данных.

2. Договорные соглашения: договоры о передаче данных используются для авторизации передачи данных за пределы юрисдикции, в которой находится организация. Такие договоры гарантируют строгое соблюдение соответствующих стандартов соответствия, например, в области обработки и хранения данных. На практике наиболее часто используются стандартные договорные положения (Standard Contractual Clauses, SCC). Это заранее составленные положения, которые включаются в договоры между импортерами и экспортерами данных для их трансграничной передачи. Они были одобрены Европейской комиссией как соответствующие Общему регламенту ЕС по защите данных. По оценке IAPP, в настоящее время 71 страна мира использует стандартизированные договорные положения[4].

3. Правила передачи данных внутри организации, или обязательные корпоративные правила (Binding Corporate Rules, BCR), представляют собой совокупность внутренних политик и соглашений, регулирующих защиту данных и авторизующих трансграничную передачу данных в рамках одной организации. BCR признаются в различных юрисдикциях, включая ЕС, Великобританию, Бразилию, Сингапур и Южную Африку.

---

3 International Association of Privacy Professionals. Infographic: Global Adequacy Capabilities. https://clck.ru/39o88u

4 Там же.

Многие организации отдают предпочтение BCR Евросоюза, чтобы структурировать свои глобальные проекты при соблюдении конфиденциальности данных. Однако внедрение BCR может быть сложным и трудоемким процессом, поскольку для этого необходимо получить разрешение соответствующих органов по защите данных.

4. Механизмы сертификации: несколько юрисдикций признают сертификаты по передаче данных, выданные соответствующими органами. Чтобы получить сертификат, компания должна пройти проверку со стороны независимого контролирующего органа (Accountability Agent, AA), который может быть как государственной структурой, так и частной организацией. В настоящее время единственным таким механизмом является система трансграничных правил конфиденциальности АТЭС (Cross-Border Privacy Rules, CBPR), признанная в восьми странах: Австралии, Канаде, Китае, Японии, Южной Корее, Мексике, Сингапуре и США.

5. Согласие пользователя: несмотря на сложности масштабирования, получение согласия пользователя традиционно служит основным подходом к трансграничной передаче данных. Оно особенно широко применяется в сложных правовых средах, где является центральным элементом различных режимов передачи данных. Согласие пользователя должно соответствовать определенным критериям, в том числе быть информированным, явным и недвусмысленным, при этом стандарты получения согласия в разных юрисдикциях различны. Согласно Общему регламенту ЕС по защите данных, согласие пользователя может служить механизмом обеспечения передачи данных только в том случае, если не имеется Заключения о признании адекватности защиты или других гарантий, таких как стандартные договорные положения или обязательные корпоративные правила. Отсутствие общепринятых норм сертификации адекватной защиты данных затрудняет для организаций навигацию по сложному ландшафту нормативных актов в этой области.

В связи с этим правительства многих стран активно пытаются решить проблему трансграничной передачи данных. Совместными усилиями они стремятся создать благоприятные условия для законных трансграничных потоков данных, обеспечивая при этом защиту конфиденциальности личной информации и безопасности данных.

2.2. Правительственные инициативы для повышения эффективности трансграничной передачи данных

Рассмотрим ряд недавних инициатив, предпринятых правительствами отдельных стран для повышения эффективности трансграничной передачи данных.

Европейский союз и Соединенные Штаты совместно представили новый рамочный документ ЕС–США о конфиденциальности данных Data Privacy Framework (DPF)[5]. Он заменяет прежнюю Программу по защите конфиденциальности ЕС–США (EU-U.S. Privacy Shield), которая была отменена в результате решения по делу Schrems II в 2020 г. Европейской комиссии было дано указание не утверждать рамочный документ до тех пор, пока в нем не будут адекватно устранены опасения, высказанные в деле Schrems II как Парламентом ЕС, так и Советом ЕС по защите данных (Gao & Chen, 2022).

[5] International Association of Privacy Professionals. (n.d.). EU-U.S. Data Privacy Framework: Guidance and Resources. https://clck.ru/39o8Dg

По инициативе Японии правительства стран Большой семерки активно развивают институциональное партнерство (Institutional Arrangement for Partnership, IAP)[6]. Оно призвано восполнить пробел в создании эффективного и надежного механизма международного сотрудничества для введения в действие системы «Свободный поток данных на основе доверия» (Data Free Flow with Trust, DFFT).

С 1 июня 2023 года в Китае введены в действие Правила заключения стандартного договора о трансграничной передаче персональных данных. Они обязывают организации, обрабатывающие персональные данные (даже те, что обрабатывают данные менее 1 миллиона человек), заключать договоры с зарубежными получателями данных перед их передачей за границу. Законодательство Китая по обеспечению безопасности данных включает в себя три ключевых закона: Закон о кибербезопасности, Закон о безопасности данных и Закон о защите персональной информации. Эти законы подкреплены целым рядом правительственных постановлений. В соответствии с этими актами центральное правительство сформировало систему регулирования экспорта персональных данных.

Кроме того, был проведен форум, посвященный системе трансграничных правил конфиденциальности (Global Cross-Border Privacy Rules, CBPR) (Joel, 2023). Страны-члены Азиатско-Тихоокеанского экономического сотрудничества (АТЭС), включая США, Канаду, Японию, Сингапур и другие государства, инициировали этот форум с целью создания международной системы сертификации на основе CBPR и соответствующих систем признания конфиденциальности при обработке информации (Privacy Recognition for Processors, PRP).

В условиях стремительной трансформации цифровой экономики организации должны сохранять гибкость и активно обновлять свои методы и протоколы в соответствии с постоянно меняющейся нормативно-правовой базой. Это особенно важно для крупных организаций, ведущих обширную деятельность во всем мире, поскольку несоблюдение требований может привести к значительным штрафам. Например, в 2021 г. европейские органы надзора за защитой данных наложили штрафы на сумму около 1,2 млрд долларов США, причем самый крупный штраф выплатил американский онлайн-ритейлер[7]. В 2022 г. Управление по киберпространству Китая (China's Cyberspace Administration, CAC) оштрафовало известную компанию Didi Global (сервис по заказу такси) на 8 млрд юаней (1,2 млрд долларов) за нарушение правил национальной безопасности и защиты персональных данных. Китайские компании, расположенные на территории страны и планирующие первичное размещение акций на международном рынке, до сих пор сталкиваются с последствиями этого решения[8].

При наличии различных механизмов для облегчения трансграничной передачи данных каждая организация должна самостоятельно оценивать и выбирать наиболее подходящие варианты, исходя из своих конкретных потребностей. Универсального

---

6 World Economic Forum. (2023, April 26). How and why data must flow freely and responsibly across borders. https://clck.ru/39o8Gf

7 EDPB. (2023, May 22). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. https://clck.ru/39o8HK

8 Webster, G. (2022, July 21). Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. DigiChina. https://clck.ru/39o8KA

решения не существует. В зависимости от ситуации правительства могут использовать одновременно несколько систем. Также важно, чтобы меры по авторизации передачи данных были органично интегрированы в существующие рабочие процессы. Отсутствие эффективных мер может привести к необходимости длительных и дорогостоящих согласований в различных инстанциях.

3. Применимость международного права для регулирования трансграничной передачи данных

3.1. Подходы различных юрисдикций к проблеме трансграничной передачи данных

Очевидно, что роль международного права в регулировании трансграничной передачи данных весьма велика; оно служит краеугольным камнем в деле защиты частной жизни, соблюдения прав человека, обеспечения кибербезопасности, содействия торговле, урегулирования конфликтов и создания индивидуальных соглашений. Оно закладывает основу и определяет стандарты надлежащего управления данными на международном уровне, способствует ответственной реализации такого управления и укрепляет доверие к цифровым взаимодействиям.

Как отмечалось, интернет «не поддается регулированию». Однако в Интернете стираются границы между национальными государствами, но не законы (Chuanying, 2020). В совместном исследовании, проведенном по заказу Министерства обороны в 1998 г., отмечается следующее.

Возможно, реальная проблема, с которой сталкиваются правительства в связи с развитием Интернета (и других средств коммуникации с использованием информационных технологий), заключается не столько в распространении информации, сколько в увеличении числа участников на уровне правительств и дипломатии. Организованные группы и отдельные лица могут создавать (и фактически создают) коалиции как внутри страны, так и на международном уровне, которые оказывают беспрецедентное давление на национальные правительства в отношении практически любой деятельности или сферы интересов. Эти группы могут фактически создавать то, что правительствам остается только признать. В связи с этим возникает вопрос, изменилась ли природа суверенитета после возникновения возможности мгновенных и повсеместных коммуникаций, и если да, то как (Press et al., 1998).

Иного мнения придерживается доцент Мэрилендского университета в Колледж-Парке, доктор Вирджиния Хауфлер (Virginia Haufler): «Разработку и внедрение эффективных норм на основе директивных, правительственных подходов затрудняет децентрализованный, открытый, глобальный характер… Интернета» (Haufler, 2013).

Разрушительные террористические атаки 11 сентября и использование террористами Интернета для коммуникации послужили толчком к принятию развитыми странами мер по ограничению контента. По данным общественной организации, выступающей за свободу журналистики, еще в сентябре 2002 г. США, Великобритания, Франция, Германия, Испания, Италия, Дания, Европейский парламент, Совет Европы и страны Большой восьмерки выражали обеспокоенность по поводу своих прав и свобод в Интернете (Nijboer, 2004).

Международные правительственные организации столкнулись с серьезными проблемами в связи с тем, что цели государств при ограничении контента существенно

различаются. Эти разногласия стали очевидными на открытии Всемирной встречи на высшем уровне по вопросам информационного общества (World Summit for the Information Society, WSIS) в декабре 2003 г. Одними из ключевых разногласий в ходе переговоров на этом форуме стали формулировки, используемые для рассмотрения последствий высказываний в Интернете. Китай, что немаловажно, выразил свое отрицательное отношение к тексту о свободе прессы, который отражал американскую точку зрения. В результате в Декларации принципов свобода прессы все же была упомянута, но в более сдержанной форме и с добавлением формулировки, подчеркивающей важность национального суверенитета (Berleur, 2007)[9]. Принятый План действий гласил, что правительства должны принять необходимые меры для борьбы с вредным и незаконным медиаконтентом, соблюдая при этом право на свободу слова (Jensen, 2006). Внешние наблюдатели сошлись во мнении, что План действий игнорирует непримиримые разногласия по регулированию контента и дает мало указаний на будущее (Souter, 2004).

К примеру, Соединенные Штаты и Евросоюз по-разному относятся к конфиденциальности данных. Американская позиция в отношении личных прав базируется в основном на идее невмешательства государства. В результате в США не получили особой поддержки законы штатов, касающиеся конфиденциальности данных. Как отмечают Bessette and Haufler (2001), в США предпочитают скорее рыночный метод сбора данных. «Если на международном уровне будут приняты законы о неприкосновенности частной жизни, то они, естественно, станут преобладающим методом ее обеспечения», – заявил представитель администрации президента Айра Магазинер (Farrell, 2003).

В Европе, напротив, тайна частной жизни рассматривается как одно из фундаментальных прав, которое должно находиться под защитой государства. Bessette and Haufler отмечают, что «европейские страны, в частности, ввели надежные гарантии неприкосновенности частной жизни, определив ее как одно из основных прав человека» в результате случаев нарушения неприкосновенности частной жизни со стороны правительства (Mai'a, 2023). В 1995 г. Европейский союз принял всеобъемлющую Директиву о защите данных, которая установила для европейских компаний четкие правила и механизмы их соблюдения. Директива была направлена на предотвращение деятельности компаний за пределами юрисдикции ЕС в целях обхода закона. Она запрещала передавать личные данные граждан ЕС странам, не обеспечивающим надлежащую безопасность. Директива должна была вступить в силу в конце 1998 г. (Long & Quek, 2002).

Учитывая масштабы этого запрета, Австралия, Канада и страны Восточной Европы были вынуждены изменить свои собственные правовые системы, чтобы соответствовать стандартам ЕС. США, однако, предприняли ответные меры, вынудив американские транснациональные корпорации создать системы саморегулирования, соответствующие законам ЕС.

Тоталитарные режимы использовали простые, но эффективные методы регулирования интернет-контента. Предпринимались такие меры, как ограничение использования персональных компьютеров, контроль и запрет нежелательного контента

[9] McCarthy, K. (2003, December 8). Internet Showdown Side-stepped in Geneva. The Register Newsletter, 8. https://clck.ru/39o8LW

(порнографических материалов, аморальных сайтов, религиозного и политического контента), что в конечном итоге привело к цензурированию Интернета и широкому использованию систем фильтрации контента (Drezner, 2004).

В научной литературе, посвященной глобализации, часто чрезмерно упрощают сложную систему управленческих взаимодействий в международной политике, фокусируясь исключительно на бинарной оппозиции между государственной и негосударственной властью. Более верное представление о последствиях глобализации можно получить, признав возможность существования различных механизмов глобального управления. Изучение управления Интернетом показывает, что правительства могут вмешиваться в ситуацию, когда это необходимо для достижения их собственных целей, даже если ранее они возложили управленческие обязанности на коммерческие организации.

Если крупные державы не могут наладить сотрудничество, а другие международные игроки поддерживают какую-либо из влиятельных стран, то возникают так называемые «конкурирующие стандарты». В ходе исследований были выявлены два примера таких стандартов: это защита конфиденциальности данных и регулирование генетически модифицированных организмов (Trump et al., 2023). В обоих случаях США и ЕС продвигают свои системы норм для регулирования этих вопросов. Обеим сторонам удалось заручиться определенной поддержкой, однако ни один из стандартов не достиг всеобщего признания.

Наконец, предполагается, что если крупные державы придут к согласию, но их интересы не совпадут с интересами других международных игроков, то в результате появятся «клубные стандарты». Эти стандарты представляют собой одну из самых захватывающих сторон регулирования. В этом сценарии влияние крупных держав становится очевидным, поскольку они оказывают давление на другие государства и ведут с ними переговоры о создании стандарта. Часто все начинается с небольшой, но влиятельной группы, такой как ОЭСР или Целевая группа по борьбе с отмыванием преступных доходов. Эти коалиции государств-единомышленников могут выработать системы норм и впоследствии убедить другие государства принять их.

3.2. Программа по защите конфиденциальности ЕС–США и ее влияние на трансграничную передачу данных между ЕС и США

Программа по защите конфиденциальности ЕС–США – это система, призванная регулировать передачу персональных данных из Евросоюза в Соединенные Штаты. Ее основной целью было обеспечить соблюдение европейских правил защиты данных при их передаче. После того как Европейский суд отменил концепцию «Безопасной гавани» в результате решения по делу Schrems I, принятого в 2015 г., в 2016 г. была введена новая структура. Ее главной целью было создание правовой базы для передачи персональных данных из ЕС в США и обеспечение соблюдения американскими организациями стандартов защиты данных, сопоставимых с теми, что действуют в ЕС.

По мнению Европейской комиссии, Программа по защите конфиденциальности ЕС–США обеспечивает приемлемый уровень защиты данных в США, поэтому система защиты данных ЕС получила «заключение об адекватности». При определении уровня защиты должны были учитываться все соответствующие аспекты операции по передаче данных или серии связанных между собой действий.

При этом учитывалось множество переменных, в том числе «правовые нормы, как общие, так и специфические для третьей страны, а также профессиональные стандарты и меры безопасности, принятые в этой стране» (Hijmans, 2006).

Чтобы предотвратить обработку данных компаниями за пределами ЕС с целью обойти Директиву 1995 г., было введено ограничение на передачу данных (Drezner, 2008). Ряд стран изменили свое законодательство в попытке достичь стандартов адекватности. Однако вместо того, чтобы поддерживать законодательные меры, имеющие обязательную силу, Соединенные Штаты поддержали варианты саморегулирования, которые соответствовали саморегулируемому характеру федеральной политики в области конфиденциальности данных (Voss, 2019).

Сравнению подходов США и ЕС к разработке политики регулирования Интернета посвящены многочисленные исследования. Результаты показывают, что ЕС обычно разрабатывает широкое и всеобъемлющее законодательство. Однако эта законодательная процедура часто продвигается медленнее, что представляет проблему, особенно когда речь идет о быстрой эволюции Интернета и новых технологиях. В США, напротив, разработана более децентрализованная нормативная база с множеством агентств и иногда несовместимыми между собой нормативными актами (Reidenberg, 1996).

Существенные разногласия между ними усугубляются различиями между данными и метаданными. Федеральное законодательство США предоставляет правоохранительным органам значительные полномочия по доступу к метаданным (Schneider, 2009).

Однако в отношении Программы по защите конфиденциальности ЕС–США Европейский суд признал решение Европейской комиссии № 2016/1250 незаконным. По мнению суда, это решение не гарантировало степень защиты персональных данных, эквивалентную той, которая требуется согласно европейскому законодательству (Furramani, 2023).

В 2016 г. было принято решение Европейской комиссии № 2016/1250, которое разрешило передачу персональных данных из ЕС в США. В результате компании из ЕС и Европейской экономической зоны отправляли персональные данные американским организациям, включенным в список Программы по защите конфиденциальности ЕС–США, с особыми гарантиями защиты данных (Furramani, 2023).

Указанное дело было инициировано гражданином Австрии, пользователем Facebook[10], который возражал против передачи своих данных в США, заявляя, что США не обеспечивают такого же уровня защиты, как требуется по законодательству ЕС. В 2013 г. он подал иск, который комиссар по защите данных первоначально принял к рассмотрению[11]. После повторного изучения материалов комиссар пришел к выводу, что передача персональных данных в США не соответствует статьям 7, 8 и 47 Европейской хартии о правах человека[12]. Это послужило поводом для передачи дела в Верховный суд.

[10] Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

[11] CJEU, Schrems II, 2020, July 16, paras 50, 51 and 52.

[12] CJEU, Schrems II, 2020, July 16, paras 55 and 56.

По мнению Верховного суда, США не обеспечили адекватную защиту личной информации в соответствии со статьями 7 и 8 Хартии ЕС о правах человека. Суд выявил несколько проблем, включая применение Четвертой поправки к гражданам Европы, сомнения по поводу деятельности Агентства национальной безопасности без судебного надзора, а также несоответствия между положением об омбудсмене Программы по защите конфиденциальности ЕС–США и статьей 47 Хартии. В связи с этим Верховный суд передал дело в Европейский суд[13].

Согласно статье 45 Общего регламента по защите данных, Европейский суд постановил, что передача личной информации из ЕС или ЕАЭС в третьи страны должна быть основана на адекватном решении, принятом Комиссией. Если такое решение не принято, данные могут быть переданы при условии «надлежащих гарантий» согласно статье 46 Общего регламента по защите данных, которая определяет права субъектов и средства правовой защиты[14].

Суд подчеркнул роль национальных надзорных органов в отношении защиты личной информации в соответствии со статьями 51(1) и 57(1) Общего регламента по защите данных. Он указал, что национальные органы власти отвечают за соблюдение норм, установленных нормативными актами ЕС, при передаче персональных данных из ЕС или Европейской экономической зоны в другие страны или международные организации[15, 16].

Национальные надзорные органы должны иметь возможность рассматривать иски и оценивать соответствие переданных данных положениям Общего регламента даже в тех случаях, когда Европейская комиссия утвердила заключение об адекватности защиты, разрешающее передачу личной информации[17, 18].

По мнению Европейского суда, Программа по защите конфиденциальности ЕС–США не гарантирует прав субъектов данных, как требует Хартия Евросоюза о правах человека. Право на справедливое судебное разбирательство и эффективные средства правовой защиты гарантируются Хартией. Кроме того, Европейский суд постановил, что в соответствии со статьей 47 Хартии омбудсмен по вопросам Программы по защите конфиденциальности ЕС–США, назначаемый государственным секретарем, не относится к категории автономной организации или судебного органа[19].

По сути, Европейский суд пришел к выводу, что США не обеспечивают уровень защиты данных, эффективно сопоставимый с уровнем защиты Европейского союза, как того требует статья 45(1) Общего регламента по защите данных с учетом статей 7, 8 и 47 Хартии. Эти статьи гарантируют право на эффективную правовую защиту, уважение частной и семейной жизни, а также защиту персональных данных. В результате заключение об адекватности защиты было отозвано. В связи с этим при передаче

13 CJEU, Schrems II, 2020, July 16, para. 65.

14 CJEU, Schrems II, 2020, July 16, paras. 91 and 92.

15 CJEU, Schrems II, 2020, July 16, para. 107 and case C-362/14, 2015, October 6, Schrems I, para. 47.

16 15 Эта точка зрения согласуется с выводами Суда по делу Schrems II от 2020 года и по делу Schrems I от 2015 года, а также с мнением таких ученых, как Piroddi (2021) и De Mozzi (2022).

17 CJEU, Schrems II, 2020, July 16, para. 120.

18 Этот принцип был применен в деле Schrems II от 2020 года.

19 CJEU, Schrems II, 2020, July 16, para. 168.

данных между США и ЕС должны применяться дополнительные меры безопасности, предусмотренные главой V Регламента ЕС, а именно статьей 46(2), в которой говорится о соответствующих гарантиях.

4 июня 2021 года Европейская комиссия утвердила два набора стандартных договорных соглашений в ответ на отмену Программы по защите конфиденциальности ЕС–США[20]. Цель этого решения – упростить передачу персональных данных из ЕС в третьи страны. Эти коммерческие соглашения отражают требования к передаче персональных данных в соответствии с решением Европейского суда по делу Schrems II, а также содержат положения, позволяющие учесть различное количество сторон, заключающих договор (De Mozzi, 2021).

3.3. Трансграничная передача данных внутри Евразийского экономического союза

Цифровые технологии открывают перед таможенными органами новые возможности для повышения скорости и качества процесса принятия решений. Следующий этап развития цифрового государственного управления тесно связан с централизацией данных. Это предполагает структурирование государственного управления, при котором решения все больше опираются на объективные данные (Vovchenko et al., 2019).

Еще один важный компонент цифровизации системы таможенного регулирования в ЕАЭС – это создание общей платформы для обмена и передачи цифровых данных, что подчеркивается в Положении о трансграничном пространстве доверия, а также в статье 23 соответствующего Соглашения.

Кроме того, Евразийская экономическая комиссия заложила основу для развития транснационального характера цифровой экономики. Это стало возможным благодаря решению Высшего Евразийского экономического совета № 12 от 11 октября 2017 года, утвердившему первоочередные планы реализации цифровой повестки ЕАЭС до 2025 г. (Колодняя, 2018).

Хотя большая часть вышеупомянутых законов была принята в рамках ЕАЭС, все еще имеется ряд барьеров, которые затрудняют плавное вхождение в союз всех его членов. Так, сохраняется проблема регулирования оборота данных на всей территории союза, представляя собой серьезное препятствие для реализации цифровой повестки. Многие цифровые экосистемы, планируемые к внедрению, предполагают трансграничный обмен данными в различных форматах взаимодействия, включая G2G, G2C, G2B, B 2B и B 2C. При этом многие аспекты обращения данных в ЕАЭС остаются недостаточно развитыми. Как следствие, отсутствует терминологическая согласованность ключевых понятий, связанных с данными, недостаточно развито регулирование в сфере данных, отсутствуют единые подходы к правовой категоризации данных и управлению рисками в этой сфере. Не решены правовые вопросы, связанные с трансграничным обменом данными. В результате нормативные меры отстают от практики, препятствуя прогрессу в реализации цифровой повестки. Ситуация еще более осложняется требованиями национальных законодательств государств-членов ЕАЭС, в частности, в области локализации персональных данных. Крайне важно создать и внедрить соответствующее законодательство и механизмы,

[20] Commission implementing decision of 4 June, Nos. 2021/914/UE and No. 2021/915/UE.

направленные на защиту данных при их трансграничном обращении внутри ЕАЭС, включая как неперсональные, так и персональные данные (Mikhaliova, 2022).

ЕАЭС давно участвует в дискуссиях о разработке международного соглашения, касающегося оборота и защиты данных. Однако процесс согласования подходов и разработки такого соглашения по-прежнему остается сложным и длительным.

Кроме того, сохраняются проблемы в сфере электронного документооборота. Следовательно, существует необходимость в совершенствовании законодательства и выработке общих подходов в области электронных подписей. Проблема взаимного признания электронных подписей является серьезным препятствием для торговли, существенно осложняя взаимодействие с поставщиками на внутреннем рынке ЕАЭС и процесс закупок. Эффективное использование цифровой инфраструктуры Союза невозможно без устранения этих правовых пробелов.

Еще более сложным препятствием на пути реализации цифровой повестки является проблема неравномерного развития цифровых технологий в государствах-членах Союза (Filatova et al., 2018). Чтобы продемонстрировать эту проблему, мы можем изучить показатели этих государств-членов в рамках Индекса сетевой готовности[21].

Индекс сетевой готовности был предложен в 2002 г. на Всемирном экономическом форуме и в настоящее время выпускается организацией Институт Портуланс (Portulans Institute). Индекс позволяет оценить степень развития информационно-коммуникационных технологий в разных странах. Он играет ключевую роль в оценке технологического и инновационного потенциала страны и является важным показателем для проведения сравнительных исследований в области ИКТ в разных государствах.

Что касается развития информационно-коммуникационных технологий в регионе ЕАЭС, то здесь наблюдается заметная диспропорция. Например, в 2022 г. разрыв в развитии ИКТ между Россией и Кыргызстаном составлял 45 пунктов. Армения, Беларусь и Казахстан достигли сопоставимого уровня развития ИКТ, но их отставание от России также значительно. В настоящее время основное внимание уделяется расширению связей между государственными органами государств-членов ЕАЭС, обновлению интегрированной информационной системы и внедрению безопасного и непрерывного электронного документооборота, что в определенной степени смягчает эту проблему.

Однако в будущем, когда цифровые инициативы Союза будут напрямую затрагивать интересы населения, это цифровое неравенство может существенно снизить эффективность реализации проектов. Кроме того, текущие цифровые инициативы опираются на уже существующие национальные сервисы, а разный уровень развития этих сервисов усложняет реализацию совместных проектов (Bolgov & Karachay, 2016). Чтобы ускорить цифровую трансформацию государств-членов ЕАЭС, необходимо активизировать международный обмен опытом в области цифровых технологий и распространение лучших технологических практик.

Важным фактором является то, что цифровая инфраструктура внутри Союза, в частности интегрированная информационная система, еще не полностью оформлена. Кроме того, задержки наблюдаются в реализации ряда важнейших проектов

[21] Network Readiness Index Homepage. https://networkreadinessindex.org

в рамках цифровой повестки. Основными препятствиями на пути развития цифровой экосистемы Союза являются недостатки нормативно-правовой базы, отсутствие последовательной концептуальной согласованности в реализации национальных стратегий развития цифровой экономики, а также диспропорции в развитии ИКТ в разных странах региона.

В последние годы государства ЕАЭС активно создают свои национальные цифровые экосистемы. Эти проекты охватывают как сферу государственного управления, так и цифровую экономику этих стран. Однако темп цифровизации в регионе отстает от развития национальных цифровых систем.

Для эффективной реализации целей и задач, которые задает цифровизация, необходимо консолидировать усилия государств ЕАЭС в области цифровой трансформации экономики. Такая консолидация предполагает более активное участие национальных центров компетенций и укрепление национальных цифровых инфраструктур.

Заключение

Очевидно, что в настоящее время международное сообщество как никогда нуждается в координированной нормативной базе, касающейся трансграничной передачи данных, включая правовые гарантии и меры для выявления уязвимостей в сфере безопасности, рисков кибербезопасности и правовых проблем.

Согласованные стандарты могут быть установлены лишь при условии достижения договоренностей по основным вопросам между ведущими державами и другими международными структурами. Предполагается, что эти нормы будут регулироваться не отдельными местными организациями, но образовывать обширный «режимный комплекс» под руководством «всеобщих» межправительственных органов. Как уже отмечалось, одним из ярких примеров гармонизированных стандартов является широкое распространение интернет-протокола TCP/IP.

Список литературы

Колодняя Г. (2018). Цифровая экономика: особенности развития в России. *Экономист*, *4*, 63–69.

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society*: *Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference “Information Society: Governance, Ethics and Social Consequences”, University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union’s countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Информация об авторе

Болатбеккызы Гульбакыт – соискатель степени PhD, докторант, школа права, Уханьский университет
Адрес: 430072, Китай, провинция Хубэй, г. Ухань, Луоцзя Хилл
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313–2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

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: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 2 февраля 2024 г.
Дата одобрения после рецензирования – 1 марта 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.19

Legal Issues of Cross-Border Data Transfer in the Era of Digital Government

Gulbakyt Bolatbekkyzy
Wuhan University, Wuhan, China

Keywords

cybersecurity,
data protection,
digital government,
digital technologies,
digitalization,
human rights,
law,
personal data,
privacy,
transboundary exchange

Abstract

Objective: to identify the main legal factors of cross-border data exchange in the context of digital technology proliferation and government digitalization, including legal guarantees, security issues, cybersecurity risks, approaches to regulating and improving the efficiency of data management in various jurisdictions.

Methods: the study relies on synthesis and critical analysis of various aspects of the stated problem, including analysis of primary and secondary sources. By the example of the regulatory policies of China, the US, the EU and EAEU member states, different approaches regarding the restriction or encouragement of free cross-border data transfer are compared. A comprehensive meta-analysis and literature assessment provided insights into the methods used for data protection in different jurisdictions and allowed outlining the framework and directions of the public policy required for effective cross-jurisdictional data transfer.

Results: the main challenges associated with cross-border data transfer in the context of digital technology proliferation and government digitalization, such as growing inequalities in digital development, legal uncertainties, privacy and cybersecurity, etc., were identified. The legal framework of cross-border data transfer in the context of government digitalization and its implementation were analyzed. It contributed to the search for ways to improve the government efficiency in the context of transnational data transfer, including rendering services and promoting openness and public participation.

Scientific novelty: based on the analysis of various jurisdictions' approaches to legal, security and sovereignty issues caused by transnational data transfer, the author reveals the role and applicability of international law, as well as the unique challenges arising in the member states of the Eurasian Economic Union on the way to the formation of transboundary trust space.

Practical significance: the study of these issues may help various public agencies, first of all, governmental and legislative bodies to the elaborate well-targeted political and legal decisions, aimed at achieving a balance between data availability and data security, between the effectiveness of public administration and respect for the human rights. The results obtained will also be of importance for other subjects of relations in cross-border data transfer and regulation of these relations.

For citation

Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. *Journal of Digital Technologies and Law, 2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

References

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference "Information Society: Governance, Ethics and Social Consequences", University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union's countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Kolodnyaya, G. (2018). Digital economy: features of development in Russia. Ekonomist, 4, 63–69. (In Russ.).

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Author information

Gulbakyt Bolatbekkyzy – PhD Candidate and Doctoral Scholar, School of Law, Wuhan University
Address: Luojia Hill, Wuhan, Hubei Province, 430072, China
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313-2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – February 2, 2024
Date of approval – March 1, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:347.45/.47:339
EDN: https://elibrary.ru/zkuagz
DOI: https://doi.org/10.21202/jdtl.2024.16

Применение смарт-контрактов в сфере международной торговли и перспективы дальнейшей эволюции Инкотермс

Принс Фатер Ауду ✉

Университет Ахмаду Белло, Зария, Нигерия

Фатима Шабих

Университет Джамия-Миллия-Исламия, Нью-Дели, Индия

Ключевые слова

децентрализованные финансы (DeFi),
Инкотермс,
контракт,
международная торговля,
международное право,
право,
смарт-контракт,
технология блокчейна,
цифровизация,
цифровые технологии

Аннотация

Цель: выявить перспективы международной торговли в свете синхронизации положений Инкотермс со смарт-контрактами.

Методы: в основе исследования лежат общенаучные методы анализа, синтеза, сравнения, а также формально-юридический метод, необходимый для анализа положений Инкотермс.

Результаты: авторами проанализированы положения Инкотермс и технологические новации в торговом праве; показана связь между практикой торгового права и технологическим развитием, обусловленная включением условий договора в блокчейн. Отмечается, что интеграция технологии блокчейн со смарт-контрактами привела к разнообразию автоматизированных бизнес-транзакций и созданию платформы для торговли синтетическими активами. Раскрыты возможности безопасного и простого осуществления сделок в международной торговле с помощью технологии блокчейн. Несмотря на уникальность данной технологии, выделяются различные ее виды, а именно: публичный, частный, гибридный и консорциумный блокчейн. Обосновано, что синхронизация положений Инкотермс со смарт-контрактами может изменить перспективы международной торговли (особенно экспортно-импортных контрактов) в лучшую сторону. Подчеркивается, что на основе технологии блокчейн смарт-контракты могут произвести революцию в применении Инкотермс, и, как следствие, повысить эффективность транзакций между сторонами экспортно-импортных отношений. Одно из фундаментальных изменений, которое смарт-контракты внесут в данные торговые операции, заключается в сокращении количества ошибок и неправильного толкования правил Инкотермс.

✉ Контактное лицо

Авторы на конкретных случаях демонстрируют возникающие на этапе заключения сделки и ее исполнения споры, которые можно было бы избежать посредством использования современных технологий.

Научная новизна: показаны феномен синхронизации Инкотермс с технологией блокчейн и то, как это может повлиять на форму контрактов и способствовать их беспрепятственному исполнению. Предложенный подход к анализу феномена учитывает революционные инновации в трансграничной торговле, которые сравниваются с обычными способами применения Инкотермс в традиционных международных торговых контрактах.

Практическая значимость: проведенное исследование содержит предложения и рекомендации для дальнейшего развития инноваций в области смарт-контрактов, особенно экспортно-импортных торговых контрактов в глобальном масштабе.

Для цитирования

Ауду, П. Ф., Шабих, Ф. (2024). Применение смарт-контрактов в сфере международной торговли и перспективы дальнейшей эволюции Инкотермс. *Journal of Digital Technologies and Law*, *2*(2), 308–327. https://doi.org/10.21202/jdtl.2024.16

Содержание

Введение

Появление цифровых технологий в ходе развития науки стремительно меняет традиционные модели человеческой деятельности, разрушая при этом давно устоявшиеся условности и методы ведения дел. В сфере международной торговли революционные цифровые технологии также запустили процесс перемен. Одним из таких беспрецедентных технологических прорывов, меняющих ход событий, является технология блокчейн. Она позволила создать надежные системы, обеспечивающие безопасность, целостность данных и анонимность коммерческих сделок между сторонами, при этом свободные от контроля со стороны центрального хранилища или

органа власти. Эта децентрализованная технология управления данными, начав функционировать в 2008 г. как катализатор криптовалюты биткоин, вызвала появление целого спектра бизнес-операций. Более того, это распределенное программное обеспечение породило разнообразные автоматизированные бизнес-транзакции и создало платформу для развития смарт-контрактов. Включение условий договора в блокчейн создало связь между практикой торгового права и технологическим развитием. Интеграция технологии блокчейн со смарт-контрактами позволит воплотить в жизнь идею «однорангового рынка» (Zibin Zheng et al., 2020). Эта форма цифрового контракта основана на автоматическом выполнении условий, заложенных в блокчейн и структурированных с заранее определенными условиями, выполнение которых активирует контракт (Souei et al., 2023; Stojanović & Ivetić, 2020; Vatiero, 2022). Хотя смарт-контракты появились совсем недавно, очень высока вероятность, что они устранят ряд недостатков «бумажных» контрактов.

На международном уровне торговые операции, связанные с экспортными контрактами с участием покупателей и продавцов, регулируются нормами Международной торговой палаты (далее – МТП). Эти нормы, известные как Международные коммерческие условия (далее – Инкотермс), используются для осуществления международных торговых сделок с 1936 года (Coetzee, 2002). Чтобы соответствовать обстоятельствам, складывающимся на арене глобального бизнеса, эти условия периодически обновляются, и их текущая версия вступила в силу в 2020 году. Инкотермс определяют взаимодействие между сторонами в экспортно-импортных торговых операциях, а именно, обязанности, права и зоны ответственности договаривающихся сторон.

В данной статье мы попытаемся заглянуть в будущее и исследовать возможности для безопасного и простого осуществления сделок в международной торговле с помощью технологии блокчейн. Авторы подробно останавливаются на положениях Инкотермс и доказывают, что их синхронизация со смарт-контрактами может изменить перспективы международной торговли (особенно экспортно-импортных контрактов) в лучшую сторону.

1. Основные понятия

1.1. Инкотермс

Международные коммерческие условия, известные как «Инкотермс», – это комплекс универсальных условий, определяющих транзакции между импортерами и экспортерами. Это свод правил или регламентов, установленных Международной торговой палатой для облегчения процесса международных сделок купли-продажи между сторонами путем определения различных особенностей, связанных с торговлей, таких как сопутствующие риски, права и обязанности сторон, а также управление перевозками между экспортерами и импортерами. Инкотермс определяет формальные процедуры, а также терминологию договоров и правовых положений в экспортно-импортных торговых операциях (Davis & Vogt, 2022; Lim & En-Rong, 2021). Однако этот документ не может применяться автоматически в ходе сделки между сторонами. Это связано с тем, что указанные условия не являются обязательными и вступят в силу только если стороны включат их в договор купли-продажи[1].

[1] Incoterms in International Trade. (2020, June 18). Aceris Law LLC. https://clck.ru/3BefKf

Впервые Инкотермс были введены в нормативную базу международных договоров купли-продажи в 1936 г. Международной торговой палатой с целью минимизации несоответствий во внешнеторговых контрактах путем четкого определения прав и обязанностей продавцов и покупателей. Для того чтобы соответствовать динамичным обстоятельствам в рамках глобального делового ландшафта, Инкотермс регулярно обновляются[2]. В настоящее время действует версия Инкотермс-2020. Основной целью МТП является развитие открытого международного рынка и ускорение глобального экономического роста; достижению этой цели призваны способствовать Инкотермс благодаря их важной роли в обеспечении бесперебойного осуществления торговых операций по всему миру.

Несмотря на свой необязательный характер, Инкотермс постепенно были внедрены в сферу международной торговли для облегчения беспрепятственного выполнения экспортно-импортных контрактов между многочисленными сторонами в различных странах мира. С 1936 года, когда были опубликованы первые Инкотермс, они пересматривались несколько раз – в 1953, 1967, 1976, 1980, 1990 и 2010 гг., чтобы соответствовать требованиям изменившегося глобального делового ландшафта (Agaoglu, 2020). Инкотермс-2020, пришедший на смену Инкотермс-2020[3], вступил в силу 1 января 2020 г. и до сих пор используется во всем мире. В нем исправлены очевидные недостатки версии 2010 г., хотя значительных дополнений к общему объему положений сделано не было. Правила обновлены и сгруппированы в две категории, которые отражают режимы транспортировки. Семь из одиннадцати положений предусматривают торговлю «любым способом», а остальные четыре – продажу товаров посредством транспортировки «по суше», «по морю» или «по внутренним водным путям». Все они полностью соответствуют Конвенции ООН о международной купле-продаже товаров.

Для импортера наиболее выгодными условиями Инкотермс с точки зрения затрат являются поставки в пункт назначения (Delivered at Place, DAP), поставки с оплатой пошлины (Delivered Duty Paid, DDP) и поставки на терминал (Delivered At Terminal, DAT). Для экспортера наиболее выгодными условиями Инкотермс являются: поставка с предприятия (Ex Works, ExW), франко-перевозчик (Free Carrier, FCA), «фрахт оплачен до» (Carriage Paid To, CPT), «цена франко у борта судна» (Free Alongside Ship, FAS), франко-борт (Free On Board, FOB), «перевозка и страхование оплачены до» (Carriage and Insurance Paid To, CIP), стоимость и фрахт (Cost and Freight, CFR), стоимость, страхование и фрахт (Cost Insurance and Freight, CIF). «Выбор наиболее подходящих условий для импортера или экспортера зависит от того, хотят ли они контролировать расходы, заключить контракт на основные перевозки, снизить риски или обеспечить большую безопасность логистической цепочки»[4].

В отличие от внутренней торговой политики, Инкотермс имеют широкую применимость и могут использоваться любой страной в процессе международной торговли. По своей природе они не являются юридически обязательными, поэтому их включение в международный договор купли-продажи зависит исключительно от

2 Troy Segal. (2023, December 22). Incoterms Explained: Definition, Examples, Rules, Pros & Cons. Investopedia. https://clck.ru/3BefPS

3 Там же.

4 Incoterms: how to choose to import and export. (2022, September 11). Logisber. https://clck.ru/3BegEu

усмотрения участвующих сторон. Следовательно, включение этих условий в договор не определяет права и обязанности по договору, за исключением вопросов поставки. Они не имеют восстановительного характера и не определяют меры за нарушение какого-либо договорного обязательства.

1.2. Блокчейн

Блокчейн – это децентрализованный цифровой канал для записи транзакций между двумя сторонами. В отличие от других транзакций, где для подтверждения подлинности сделки требуется участие сторонней организации, блокчейн работает без какого-либо центрального органа или хранилища. Кроме того, неизменяемость блокчейна делает невозможным создание подделок или отслеживание хранящихся в нем транзакций. В литературе было показано, что блокчейн создает пространство для цифрового доверия, повышая как уверенность сторон в исполнении контракта, так и эффективность за счет устранения посредников и сопутствующих им затрат (Durovic & Janssen, 2019).

Прорыв в создании технологии блокчейн был заложен изобретателем биткоина Сатоши Накамото. В 2008 г.[5] он опубликовал работу о биткоине под названием «Bitcoin: A Peer-to-peer Electronic Cash System», где, среди прочего, описывалась электронная система платежей, основанная на криптографии[6]. Этому предшествовали важные достижения таких ученых, как Стюарт Хабер (Stuart Haber), Скотт Сторнетта (Scott Stornetta), Дэвид Чаум (David Chaum) и Адам Бэк (Adam Back), которые публиковали работы, посвященные созданию цифровых валют, основанных на криптографии[7]. Таким образом, появление биткоина ознаменовало собой совершившуюся революцию в сфере цифровых валют, которая назревала в пространстве цифровых технологий на протяжении нескольких десятилетий.

В самом общем виде, блокчейн – это распределенная система записи проведенных транзакций, которая ведется отдельными узлами (Papadouli & Papakonstantinou, 2023). Поскольку эти записи нельзя изменить, информация о каждой транзакции, доступная на всех узлах системы, создает эффект целостности данных[8]. При этом все узлы анонимны, а их идентификаторы – нет. Это делает процесс прозрачным и более безопасным для других узлов в плане выполнения и подтверждения транзакций. Еще одно преимущество этой технологии – высокая устойчивость к любым модификациям и изменениям. Поскольку блокчейн представляет собой базу данных записей, которые не могут быть изменены или удалены в любой момент времени, он очень удобен в тех областях, где требуется безопасность данных и масштабируемость. Технология блокчейн сегодня используется не только в транзакциях, связанных с цифровой торговлей товарами или услугами посредством криптовалют, но и находит все большее применение в различных областях управления, финансов, здравоохранения, коммунальных услуг и смарт-контрактов. Она может быть реализована в различных вариантах в зависимости от функций и целей.

---

5 Sarmah, Sh. S. (2018). Understanding Blockchain Technology. Computer Science and Engineering, 8(2), 23–24.

6 Id. at 23.

7 Id. at 23.

8 Id. at 23.

Следует отметить, что, несмотря на уникальность данной технологии в целом, блокчейны различаются между собой. Выделяют четыре их категории, а именно публичный, частный, гибридный и консорциумный блокчейны. Из них публичный блокчейн является наиболее децентрализованной формой технологии, поскольку он не связан какими-либо ограничениями и использовать его может любой человек, имеющий доступ к Интернету[9]. Примерами публичного блокчейна являются Bitcoin и Ethereum. Частные блокчейны работают аналогично публичным, однако они оперируют своего рода централизованной базой данных, которая ограничивает доступ к ним только для пользователей, входящих в сеть (Vijai et al., 2019). Примеры такого блокчейна – Hyperledger и Corda. Гибридный блокчейн, как следует из названия, сочетает в себе черты как публичного, так и частного блокчейна; он частично находится под контролем организации, но проектируется как публичный блокчейн[10]. Известные примеры гибридного блокчейна включают сеть Ripple и токен XRP. Структура блокчейна-консорциума строится вокруг нескольких организаций, и процесс его работы определяют авторизованные пользователи (Vijai et al., 2019). Среди примеров консорциумных блокчейнов – Multichain и Tendermint. Несмотря на различия этих категорий блокчейна по некоторым признакам, все они работают на основе децентрализованной системы программного обеспечения, которая обрабатывает транзакции на множестве компьютеров, поэтому никакие изменения, взломы или мошенничество в этой системе невозможны.

1.3. Смарт-контракт

Термин «смарт-контракт» используется для описания компьютерных кодов, которые автоматически выполняют все или часть соглашения, хранящегося на платформе блокчейн[11]. Эта беспрецедентная форма контракта отличается от всех других тем, что условия смарт-контракта выполняются автоматически (Huang et al., 2024). Это происходит благодаря тому, что они привязаны к блокчейну, который автоматически передает денежные средства при выполнении сторонами заранее определенных условий. Благодаря эффективному исполнению условий в смарт-контракте, он снижает транзакционные и юридические издержки, риски и другие проявления неэффективности, обычно связанные с традиционными формами контрактов (Zibin Zheng et al., 2020). Смарт-контракты работают за счет хранения, копирования и обновления транзакций в рамках соглашения, записанного в блокчейне (Dixit et al., 2022; Detwal et al., 2023). Код, описывающий содержание смарт-контракта, децентрализован в сети блокчейн, что защищает транзакции, осуществляемые с его помощью, от несанкционированного доступа.

---

9 GEEKSFORGEEKS. https://clck.ru/3Beg9Y

10 Там же.

11 Levi, S., & Lipton, A. (2018, May 26). An Introduction to Smart Contracts and their Potential and Inherent Limitations, Harvard Law School Forum on Corporate Governance. https://clck.ru/3BegAy

Смарт-контракты появились в 1994 г. благодаря Нику Сабо , который придумал идею цифрового пространства, где можно торговать синтетическими активами с помощью цифровых контрактов, встроенных в распределенные реестры[12]. С этого времени информация о революционных функциональных возможностях смарт-контрактов стала широко известна. В последние годы эта идея все больше проникает в мир бизнеса (Ante, 2021; Chu et al., 2023). Описывая беспрецедентную форму контракта, Ник Сабо определил смарт-контракты как «компьютеризированные протоколы транзакций, которые выполняют условия контракта» (Szabo, 1996). Это краткое описание четко отличает смарт-контракты от обычных контрактов на основе их уникальных функциональных возможностей и особенностей. Идея состоит в том, чтобы перевести условия договора, например, о поручительстве, праве удержания имущества должника или залоге в компьютерный код, встроенный в аппаратное или программное обеспечение, способное самостоятельно обеспечивать их выполнение (Eenmaa & Schmidt-Kessen, 2019; Ferro et al., 2023). Таким образом, отпадает необходимость в доверенном посреднике в виде сторонней организации. Указанный код может быть традиционным полностью составленным договором или просто давать ссылку на него. Код работает с помощью криптографически подписанных транзакций в сети блокчейн. Коды реплицируются через множество узлов, зарегистрированных в блокчейне, и таким образом защищены от любых модификаций или уничтожения. Пользователи блокчейна, на котором зарегистрирован код, могут осуществлять транзакции, а сам он сохраняет данные в базе и передает их для исполнения публичных функций, предлагаемых смарт-контрактом[13].

В строго юридическом смысле смарт-контракты не являются ни традиционными, ни «умными» договорами, поэтому данный термин ошибочен. Ведутся споры о том, могут ли смарт-контракты иметь такую же юридическую силу, как и обычные контракты. Утверждается, что смарт-контракты способны улучшить реализацию условий договоров и, следовательно, устранить необходимость в третьей стороне, то есть суде; это должно произойти за счет цифровизации процесса принудительного исполнения: стороны автоматически принуждаются к исполнению условий контракта путем реагирования на выполнение обязательств, встроенных в блокчейн (Raskin, 2017). С другой стороны, утверждается, что смарт-контракты не отвечают всем универсальным условиям, определяющим существование договора, поэтому в случае возникновения определенных ситуаций суть заключения таких контрактов будет сведена на нет особенностями технологии блокчейн[14]. Какой бы точки зрения мы не придерживались, несомненным остается тот факт, что смарт-контракты – это форма контакта, которая рано или поздно будет применяться во всем мире, объединив право и технологии.

12 Frankein, J. (2022, August 30). Smart Contracts. Investopedia. https://clck.ru/3BegCJ

13 Mell, P. M., Kelsey, J. M., & Shook, J. (2022, August 30). Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness. NIST. https://clck.ru/3BegDG

14 O'Connell, J. (2019, December 19). The Trouble With Smart Contracts. Mayo Wyne Baxter Solicitors. https://clck.ru/3BegGR

Поскольку смарт-контракты и технология блокчейн все еще находятся в стадии зарождения, мы сможем наблюдать реакцию на их развитие со стороны различных правовых систем по всему миру с точки зрения налогообложения и других аспектов законодательства.

2. Смарт-контракты и децентрализованные финансы: инструменты для торговли синтетическими активами

Одно из самых известных преимуществ технологии блокчейн – это возможность создания децентрализованных платформ, на которых предоставляются финансовые услуги, как в банке или любом другом финансовом учреждении. В этих сетях ведется торговля синтетическими активами, которые являются токенизированными производными от базового актива. Синтетические активы на основе криптовалюты – это активы, которые обладают ценностью производного актива без необходимости владения базовым активом. Они дают пользователям все преимущества децентрализованных инвестиций, так как открыты и доступны пользователям по всему миру с помощью смарт-контракта. Децентрализованная платформа, на которой осуществляется торговля этими синтетическими активами, носит название Decentralized Finance (DeFi). Это финансовая инфраструктура на основе блокчейна, которая использует открытый, безразрешительный и высокофункциональный протокол, построенный на публичных платформах смарт-контрактов. По имеющимся данным, по состоянию на сентябрь 2021 г. стоимость активов на протоколах DeFi составляла 92 млрд долл. США[15].

DeFi работает по принципу многослойной системы. Каждый слой в архитектуре выполняет отдельную функцию, поддерживая функционирование друг друга и образуя открытую, легко компонуемую инфраструктуру, которая позволяет любому человеку создавать, модифицировать или использовать другие части стека протоколов. Первый слой предназначен для урегулирования. Он состоит из блокчейна и активов встроенного протокола. Для безопасного хранения информации об объектах собственности она хранится в данном слое, а любые изменения состояния должны происходить в соответствии с его правилами. Этот слой служит для урегулирования и разрешения споров, что делает блокчейн основой для бездоверительного исполнения. Второй слой – это слой активов, включающий все активы, выпущенные на первом слое. Для создания базовых активов во втором слое в качестве основной финансовой операции используются стандартизированные смарт-контракты. Здесь находятся все активы встроенного протокола, а также те активы, которые являются дополнительными и выпускаются на блокчейне. Третий слой называется слоем протоколов, где представлены стандарты для определенных сценариев использования, таких как децентрализованные биржи, долговые рынки, деривативы и управление активами на блокчейне. Любой пользователь может получить доступ к этим стандартам, и они часто реализуются как набор смарт-контрактов (или приложение DeFi). Поэтому эти протоколы легко взаимодействуют друг с другом. Четвертый слой – это слой приложений. На нем активы служат основой для все более сложных финансовых продуктов. Здесь приложения DeFi реализованы

[15] McDonald, E. (2021, November 5). Smart Contracts. Columbia Business Law Review. https://clck.ru/3BegHv

в виде сложных смарт-контрактов, которые обеспечивают надежное выполнение заданных бизнес-процессов.

Взаимодействие осуществляется с помощью внешнего интерфейса на основе веб-браузера, что упрощает использование протоколов. Реализованные приложения ориентированы на пользователя, что упрощает подключение к отдельным протоколам. Пятый слой – это слой агрегации. Приложения DeFi предоставляют различные финансовые услуги, удобство и прозрачность которых делает их привлекательными для пользователя. С помощью DeFi упрощаются все виды деятельности, такие как торговля, кредитование, страхование и управление активами. На слое агрегации легко управлять тарифами и сравнивать услуги для этих видов деятельности в рамках экосистемы. Агрегаторы предоставляют пользовательские платформы для подключения к нескольким приложениям и протоколам. Они также предоставляют инструменты, которые помогают сравнивать услуги и определять тарифы, а также выполнять сложные задачи, подключаясь к нескольким протоколам одновременно. Наконец, эти удобные приложения объединяют и обобщают данные, создавая сервис, аналогичный банковским приложениям.

3. Переосмысление международных торговых контрактов: синхронизация права с технологией блокчейн

На протяжении долгого времени ход экспортно-импортной торговли определялся различными версиями международных коммерческих условий Инкотермс, сформулированных МТП. Этот документ способствует заключению сделок между сторонами, определяя их роли, обязанности, ответственность и передачу рисков в ходе сделок. Нет сомнений, что Инкотермс сыграли важную роль в облегчении процесса осуществления международных торговых сделок с участием продавцов и покупателей. С другой стороны, верно и то, что функциональные возможности Инкотермс не раз оказывались недостаточными для того, чтобы предусмотреть скрытые обстоятельства, способные нарушить ход таких международных торговых операций (Petrová et al., 2021). Эти недостатки сами по себе являются неотъемлемой частью сложной природы экспортно-импортных торговых операций, которые всегда чреваты спорами. Значительная часть этих факторов обусловлена независящими от сторон неблагоприятными обстоятельствами, тогда как другие являются проявлением недостатков в процессе исполнения контракта. Несмотря на регулярный пересмотр Инкотермс в соответствии с современным глобальным деловым климатом, совсем устранить эти недостатки не удается. Сделать это призваны смарт-контракты на основе технологии блокчейн.

В целом, внедрение смарт-контрактов в международную торговлю позволит исключить вмешательство посредников, сократить расходы, повысить безопасность сделок и прозрачность процесса (Belú, 2019). Автоматизированный процесс исполнения смарт-контрактов способен устранить все проблемы, которые могут возникнуть при использовании Инкотермс в настоящее время. В ответ на такие вызовы, как интермодальные сложности, развитие электронной коммерции и появление новых услуг в международной торговле, в последнюю действующую версию Инкотермс-2020 были внесены значительные улучшения; однако трудности, сопутствующие внедрению этих поправок, все еще не преодолены. Весь спектр проблем, связанных с применением Инкотермс, можно полностью решить с помощью

смарт-контрактов. Смарт-контракты, созданные на основе технологии блокчейн, могут быть использованы в сфере международной торговли для повышения эффективности и уменьшения проблем в таких областях, как идентификация личности, подтверждение права собственности, снижение затрат и другие вопросы логистики.

Преобразование условий Инкотермс в смарт-контракт облегчит выполнение экспортно-импортной сделки для обеих участвующих сторон. Преимущества такой синхронизации не только повлияют на процесс исполнения контракта, но и гарантируют надежность механизма транзакций.

Одно из фундаментальных изменений, которое смарт-контракты внесут в экспортно-импортные торговые операции, заключается в сокращении количества ошибок и неправильного толкования правил Инкотермс. Это объясняется сложной природой экспортно-импортных контрактов, которые обычно изобилуют множество условий, весьма сложных для понимания. Внедрение смарт-контрактов не только упростит механизм заключения сделок (Belú, 2019), но и облегчит логистику. В экспортно-импортных операциях задействовано множество людей, протоколов и элементов логистики. В результате длительности процедур и участия множества посредников, компании и отдельные лица, задействованные в них, могут испытывать фрустрацию и не достичь своих целей, особенно при работе с чувствительными к срокам продуктами[16].

Проблема логистики и затянутых протоколов оказывает более серьезное влияние на торговлю в развивающихся странах. Приведем пример международного контракта купли-продажи, который повлек за собой множество юридических споров в результате сложной логистики экспортно-импортной торговли. Акционерная компания Pharmaplast (Александрия, Египет), производящая медицинские продукты, и корпорация из Калифорнии Urica, которая импортирует и распространяет средства по уходу за ранами, 10 февраля 2004 г. заключили эксклюзивный договор при посредничестве компании с ограниченной ответственностью URI как третьей стороны, осуществляющей процесс исполнения договора. По условиям контракта компания Pharmaplast обязалась в течение десяти лет поставлять компании Urica средства по уходу за ранами для распространения в Соединенных Штатах при посредничестве URI. В ходе выполнения договора возник ряд проблем, связанных с неправильным толкованием некоторых условий, что привело к судебному разбирательству[17], которое затянулось на долгие годы и привлекло в качестве сторон множество лиц. Подобные споры часто возникают в отношении международных договоров купли-продажи товаров. Однако внедрение смарт-контрактов позволит устранить подобные трудности и снизить вероятность того, что международные сделки купли-продажи закончатся спорами. Смарт-контракты работают на основе протокола «если..., то» (Lasmoles & Diallo, 2022). Следовательно, если условия

16 Nordas, H. K., Pinali, E., & Grosso, M. G. (2006). Logistics and Time as a Trade Barrier. OECD Yrade Policy Working Papers, 35, 1, 4.

17 Urica, Inc. v. Pharmaplast SAE, CV 11-02476 MM (RZx).

международных торговых контрактов (особенно экспортно-импортных) определяются протоколом «условие» и «исполнение» в блокчейне, который предусматривает его автоматическое исполнение, то вероятность неправильного толкования уменьшается.

Кроме того, смарт-контракты способны облегчить документирование экспортно-импортных контрактов. Известно, как непросто оформлять документацию и вести переписку между сторонами, контрагентами и посредниками. «В международной торговле количество необходимых документов и их характер сильно варьируются в зависимости от основного контракта (например, договора купли-продажи), характера товара, стоимости перевозки, сложности экспортной сделки, требований транспортировки, а также правил, ограничений и торговых соглашений соответствующих стран» (Sang Man Kim, 2021). Однако неизменным фактором остается то, что эти документы обычно громоздки, а иногда и слишком сложны, тогда как работать над ними приходится в течение короткого периода времени.

Масштабность контрактов сама по себе затрудняет для некоторых сторон полное понимание их условий, не говоря уже о процессе их исполнения. В экспортно-импортной сделке сложная документация, включающая несколько Инкотермс для контроля процесса исполнения контракта, относится к нескольким посредникам, каждый из которых играет свою особую роль. Это документы импортера и экспортера, документы, выданные властями и перевозчиком, банковские документы (Belú, 2019). Все они играют важную роль в оформлении и осуществлении типичной импортно-экспортной сделки. В процессе изучения этой длинной цепочки документов может оказаться, что некоторые условия контракта невыполнимы. Поэтому смарт-контракты являются лучшим способом сократить длительную переписку между сторонами и посредниками. Смарт-контракты работают автоматически, выполняя включенные в них действия при достижении определенных условий, поэтому, если включить в блокчейн все условия Инкотермс, применимые в международных договорах купли-продажи, то можно устранить задержки и проблемы, возникающие при обычном ручном документировании.

Еще один аспект, в котором синхронизация Инкотермс со смарт-контрактами окажется эффективной, – это процесс осуществления платежей в ходе международной торговли. Традиционно процесс оплаты в международных торговых сделках сопряжен с большим количеством рисков, поэтому стороны очень скрупулезно и осторожно подходят к способам оплаты. Как правило, импортеры осуществляют платежи после получения товара [18]. Самый надежный способ оплаты для импортера, скорее всего, окажется наименее надежным для экспортера, и наоборот. Известными методами оплаты в международных торговых контрактах являются: аванс наличными, аккредитив, документарное инкассо, условия открытого счета, консигнация и торговое финансирование (Sang Man Kim, 2021).

[18] Djon Ly, 5 Common Payment Methods and Terms for International Trade. Statrys, (September 11, 2022, 1: 15 PM WAT). https://clck.ru/3BegmU

Нередко на этом этапе сделки возникают споры. В качестве примера можно привести дело Comptoird'Achar v. Luis de Ridder[19], в котором рожь, проданная аргентинским продавцом на условиях Инкотермс «стоимость, страхование и фрахт» (CIF), не была доставлена покупателю в Бельгии, несмотря на полную оплату всех сборов. Покупатель потребовал возврата денег, что привело к большому количеству судебных разбирательств. Подобных инцидентов можно было бы избежать, если бы условия соглашения были прописаны в смарт-контракте на основе блокчейн, который автоматически выплачивает средства, когда все условия выполнены. Смарт-контракты регулируют платежи по сделкам с помощью одного из трех типов привязки – условно-эффективного, совместного контракта и связи контрактов[20]. Для международных торговых сделок наиболее подходящим является условно-эффективный тип, когда деньги могут быть переведены только при выполнении заранее определенных условий[21]. Такой безопасный метод оплаты избавляет все стороны сделки от рисков; это также сводит на нет дополнительные расходы, возникающие в процессе осуществления платежей традиционными методами, что, в свою очередь, способствует беспрепятственному осуществлению сделок.

4. Трансформация международной торговли: к вопросу об обновленной технологичной конфигурации Инкотермс

Сегодня смарт-контракты являются прототипом закона Амары – концепции, сформулированной компьютерным специалистом Роем Амарой из Стэндфордского университета, которая гласит, что мы склонны переоценивать новые технологии в краткосрочной перспективе и недооценивать их в долгосрочной[22]. Хотя смарт-контракты еще только зарождаются, в будущем они могут произвести революцию в структуре вознаграждения и системе стимулов, которые будут определять положение договаривающихся сторон. Несмотря на то, что для осуществления сложных коммерческих сделок смарт-контрактам еще только предстоит полностью эволюционировать, эксперты с оптимизмом смотрят на их потенциал, способный полностью изменить характер деловых операций[23].

В международных торговых сделках смарт-контракты могут не только минимизировать уровень рисков, но и создать платформу, позволяющую людям с разных континентов участвовать в торговле без длительных переписок, которые возникают перед началом выполнения условий контракта. Что касается управления рисками,

---

19 Comptoird'Achar v. Luis de Ridder, (1949) 1 ALL E.R. 26.

20 Xinyuan Ge. (2021). Smart Payment Contract Mechanism Based on Blockchain Smart Contract Mechanism. Scientific Programming, 2021. https://doi.org/10.1155/2021/3988070

21 Weber, I., & Staples, M. (2021). Programmable Money: Next-Generation Conditional Payments Using Blockchain. Proceedings of the 11th International Conference on Cloud Computing and Services Science (Vol. 1, pp. 7–14). https://doi.org/10.5220/0010535800070014

22 Levi, S., & Lipton, A. (2018, May 26). An Introduction to Smart Contracts and their Potential and Inherent Limitations, Harvard Law School Forum on Corporate Governance. https://clck.ru/3Begbw

23 McDonald, E. (2021, November 5). Smart Contracts. Columbia Business Law Review. https://clck.ru/3BegTr

то страховая индустрия также может использовать смарт-контракты для создания премиальных пакетов, которые выплачиваются в случае неблагоприятных обстоятельств, без необходимости проходить длительный и дорогостоящий процесс подтверждения претензий[24].

С помощью смарт-контрактов могут управляться даже цепочки поставок. Смарт-контракты избавляют от факторов, которые обычно снижают эффективность цепочек поставок в международной торговле, а именно, вопросов доверия и координации[25]. Для их решения смарт-контракты предлагают систему контроля, которая, при доступной стоимости, может управлять цепочками поставок для достижения общего блага в среднесрочной перспективе, тогда как в текущей ситуации каждый отдельный участник стремится к более низкой, но немедленной прибыли. Выступая в качестве стимулирующей технологии, смарт-контракты изменят управление цепочками поставок в международной торговле, обеспечив более тесное сотрудничество между их участниками, что, в свою очередь, повысит экономическую эффективность.

Как бы ни были замечательны перспективы, которые открывают смарт-контракты, их реализация не может происходить в вакууме. Для того чтобы огромные преимущества смарт-контрактов стали реальностью, необходимо создать определенные рамки и правила. С учетом этого факта были выработаны следующие рекомендации, способствующие созданию глобальной экономической среды, в которой смарт-контракты смогут дать наибольшие преимущества.

1. Внесение поправок в Инкотермс. Смарт-контракты в сфере международной торговли получат большее признание, если Международная торговая палата внесет поправки в Инкотермс и даст возможность смарт-контрактам выступать в качестве средства оформления экспортно-импортных контрактов. Создание соответствующей международной правовой базы позволит утвердить смарт-контракты как более безопасный метод оформления торговых контрактов, при котором стороны имеют больше контроля над ходом сделки. Такое официальное признание смарт-контрактов создаст благоприятный бизнес-климат для их развития в международном торговом пространстве.

2. Внедрение глобального принципа экспортно-импортной торговли: «Умные контракты не могут напрямую получать входные данные из (sic) реального мира, они должны получать эти данные из источников, уже находящихся в блокчейне»[26]. Смысл этого принципа – соединить информацию, находящуюся вне и внутри блокчейна[27] через интерфейс прикладного программирования (API), к которому стороны смарт-контракта могут обращаться за определенной информацией. Роль этого принципа в смарт-контрактах – помогать в выполнении сложных действий, таких как поиск различных данных в Интернете – котировки акций, данные о температуре, страхование, отчеты о ценах и т. д.

---

24 Там же.

25 Bottoni, P., Gessa, N., Massa, G., Pareschi, P., Hesham, S., & Archuri, E. (2020, November 26). Intelligent Smart Contracts for Innovative Supply Chain Management. Frontiers in Blockchain. https://doi.org/10.3389/fbloc.2020.535787

26 McDonald, E. (2021, November 5). Smart Contracts. Columbia Business Law Review. https://clck.ru/3BegTr

27 Mojtahedi Arshia. A Guide to Oracles: What Are They, Types and Use Cases, AI Multiple, (12 September 2022, 2: 12 PM).

Учитывая важную роль основополагающих принципов как катализатора смарт-контрактов, создание специальной системы принципов, предназначенной исключительно для развития экспортно-импортных торговых контрактов, заложит прочный фундамент для развития смарт-контрактов в сфере международной торговли. Создание такой системы позволит договаривающимся сторонам использовать Инкотермс по своему выбору в своих контрактах на основе блокчейна и одновременно выполнять другие функции, распределенные между посредниками.

Заключение

Смарт-контракт – это революционная концепция, которая изменит ландшафт корпоративной сферы. Его особенности позволяют устранить недостатки и недочеты традиционных контрактов. Кроме того, смарт-контракты снимают системные трудности, связанные с зависимостью от третьих лиц в процессе исполнения контрактов. В сфере международной торговли распространение смарт-контрактов не просто облегчит ход сделок, но и перевернет представление о международных торговых операциях, предоставив договаривающимся сторонам больше контроля над предметом контракта. В отличие от традиционных международных торговых контрактов, которые чреваты далеко идущими последствиями от вмешательства третьих лиц, выступающих в различных качествах, смарт-контракты берут на себя функции третьих лиц; это происходит посредством блокчейна, который работает на основе согласованных сторонами и закодированных в нем условий.

Использование смарт-контрактов устраняет недостатки, характерные для традиционных контрактов. Это не только ускорит процесс исполнения международных торговых контрактов, но и снимет риск мошенничества в ходе сделки. Известно, что международные торговые контракты имеют множество уязвимостей, тогда как смарт-контракты способны обеспечить уверенность в процессе исполнения, а значит, облегчить ведение бизнеса в общемировом масштабе. Таким образом, для повышения эффективности в сфере торговли и бизнеса можно использовать обновленную технологичную конфигурацию Инкотермс, что приведет нас к новым высотам развития.

Список литературы

Agaoglu, C. (2020). Incoterms. *Public and Private International Law Bulletin*, *40*(2), 1113–1149. https://doi.org/10.26650/ppil.2020.40.2.0008

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Belú, M. G. (2019). Application of Blockchain in International Trade: An Overview. *The Romanian Economic Journal*, *22*(71), 2–15.

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*, 107221. https://doi.org/10.1016/j.infsof.2023.107221

Coetzee, J. (2002). Incoterms: Development and Legal Nature – A Brief Overview. *Stellenbosch Law Review*, *13*, 115.

Davis, J., & Vogt, J. (2022). Incoterms® 2020 and Missed Opportunities for the Next Version. *International Journal of Logistics Research and Applications*, *25*(9), 1263–1286. https://doi.org/10.1080/13675567.2021.1897974

Detwal, P. K., Soni, G., Jakhar, S. K., Srivastava, D., Madaan, J., & Kayıkçı, Y. (2023). Machine learning-based technique for predicting vendor incoterm (contract) in global omnichannel pharmaceutical supply chain. *Journal of Business Research*, *158*, 113688. https://doi.org/10.1016/j.jbusres.2023.113688

Dixit, A., Deval, V., Dwivedi, V., Norta, A., & Draheim, D. (2022). Towards user-centered and legally relevant smart-contract development: A systematic literature review. *Journal of Industrial Information Integration*, *26*, 100314. https://doi.org/10.1016/j.jii.2021.100314

Durovic, M., & Janssen, A. (2019). The Formation of Blockchain-based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, *6*, 753–772. https://doi.org/10.54648/erpl2018053

Eenmaa, H., & Schmidt-Kessen, M. J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Giacomo Corrias, Moncada, R., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Huang, H., Guo, L., Zhao, L., Wang, H., Xu, C., & Jiang, S. (2024). Effective combining source code and opcode for accurate vulnerability detection of smart contracts in edge AI systems. *Applied Soft Computing*, *158*, 111556. https://doi.org/10.1016/j.asoc.2024.111556

Lasmoles, O., & Diallo, M. (2022). Impacts of Blockchains on International Maritime Trade. J*ournal of Innovation Economics & Management*, *1*(37), 91–116. https://doi.org/10.3917/jie.pr1.0114

Lim, A. G., & En-Rong, P. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Petrová, M., Krügerová, M., & Koziel, M. (2021). Incoterms – History and Future Development. *Proceedings of the 15th International conference liberec economic forum* (pp. 589–590).

Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(2), 306–315.

Sang Man Kim. (2021). *Payment methods and finance for international trade*. Springer.

Souei, W. B. S., Hog, C. E., Djemaa, R. B., Sliman, L., & Amous, I. (2023). Towards smart contract distributed directory based on the uniform description language. *Journal of Computer Languages*, *77*, 101225. https://doi.org/10.1016/j.cola.2023.101225

Stojanović, Đ., & Ivetić, J. (2020). Possibilities of using Incoterms clauses in a country logistics performance assessment and benchmarking. *Transport Policy*, *98*, 217–228. https://doi.org/10.1016/j.tranpol.2020.03.012

Szabo, N. (1996). Smart contracts: building blocks for digital markets. E*XTROPY: The Journal of Transhumanist Thought*, *16*, 18–20.

Vatiero, M. (2022). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Vijai, C., Elayaraja, M., Suriyalakshmi, S. M., & Joyce, D. (2019). The Blockchain Technology and Modern Ledgers Through Blockchain Accounting. *Adalya Journal*, *8*(12), 545–557.

Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, & Muhammad Imran (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Сведения об авторах

Ауду Принс Фатер – бакалавр права, юридический факультет, Университет Ахмаду Белло
Адрес: Нигерия, Зария 810107, кампус Конго
E-mail: pfateraudu@gmail.com
ORCID ID: https://orcid.org/0009-0000-8289-3081

Шабих Фатима – бакалавр права и гуманитарных наук, юридический факультет, Университет Джамия-Миллия-Исламия
Адрес: Индия, Нью-Дели 110025, Джамия Нагар
E-mail: Shabihfatima010@gmail.com
ORCID ID: https://orcid.org/0000-0003-1661-232X

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: 10.89.27 / Обязательственное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 18 ноября 2023 г.
Дата одобрения после рецензирования – 14 декабря 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:347.45/.47:339
EDN: https://elibrary.ru/zkuagz
DOI: https://doi.org/10.21202/jdtl.2024.16

Configuration of Incoterms into Smart Contracts: a View of International Sales Contracts through a Futuristic Periscope

Prince Fater Audu ✉
Ahmadu Bello University, Zaria, Nigeria

Fatima Shabih
Jamia Millia Islamia University, New Delhi, India

Keywords

blockchain technology,
contract,
decentralized finance (DeFi),
digital technologies,
digitalization,
Incoterms,
international law,
international trade,
law,
smart contract

Abstract

Objective: to identify the prospects of international trade in the light of synchronizing Incoterms with smart contracts.

Methods: the study is based on the general scientific methods of analysis, synthesis, comparison, and formal-legal method necessary to analyze the provisions of Incoterms.

Results: the authors analyzed the provisions of Incoterms and technological innovations in commercial law; showed the connection between the practice of commercial law and technological development due to the inclusion of contractual terms in blockchain. It is noted that the integration of blockchain technology with smart contracts has led to a variety of automated business transactions and the creation of a platform for synthetic assets trading. The authors describe the possibilities of secure and easy transactions in international trade using blockchain. Despite the uniqueness of this technology, its different types are distinguished, namely: public, private, hybrid, and consortium blockchain. It is substantiated that the synchronization of Incoterms with smart contracts can improve the prospects of international trade (especially export-import contracts). It is emphasized that smart contracts based on blockchain can revolutionize the application of Incoterms, consequently increasing the efficiency of transactions between parties to export-import relationships. One of the fundamental changes that smart contracts will bring to these trade transactions is the reduction of errors and misinterpretations of Incoterms. The authors use specific cases

✉ Corresponding author

to demonstrate disputes arising at the stages of transaction conclusion and execution, which could have been avoided using modern technologies.

Scientific novelty: The paper shows the phenomenon of synchronizing Incoterms with blockchain and how it can affect the form of contracts and facilitate their smooth execution. The proposed approach to analyzing the phenomenon takes into account the revolutionary innovations in cross-border trade, which are compared with the usual ways of applying Incoterms in traditional international trade contracts.

Practical significance: the research provides suggestions and recommendations for further development of innovations in the field of smart contracts, especially export-import trade contracts on a global scale.

For citation

Audu, P. F., & Shabin, F. (2024). Configuration of Incoterms into Smart Contracts: a View of International Sales Contracts through a Futuristic Periscope. *Journal of Digital Technologies and Law, 2*(2), 308–327. https://doi.org/10.21202/jdtl.2024.16

References

Agaoglu, C. (2020). Incoterms. *Public and Private International Law Bulletin*, *40*(2), 1113–1149. https://doi.org/10.26650/ppil.2020.40.2.0008

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Belú, M. G. (2019). Application of Blockchain in International Trade: An Overview. *The Romanian Economic Journal*, *22*(71), 2–15.

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*, 107221. https://doi.org/10.1016/j.infsof.2023.107221

Coetzee, J. (2002). Incoterms: Development and Legal Nature – A Brief Overview. *Stellenbosch Law Review*, *13*, 115.

Davis, J., & Vogt, J. (2022). Incoterms® 2020 and Missed Opportunities for the Next Version. *International Journal of Logistics Research and Applications*, *25*(9), 1263–1286. https://doi.org/10.1080/13675567.2021.1897974

Detwal, P. K., Soni, G., Jakhar, S. K., Srivastava, D., Madaan, J., & Kayıkçı, Y. (2023). Machine learning-based technique for predicting vendor incoterm (contract) in global omnichannel pharmaceutical supply chain. *Journal of Business Research*, *158*, 113688. https://doi.org/10.1016/j.jbusres.2023.113688

Dixit, A., Deval, V., Dwivedi, V., Norta, A., & Draheim, D. (2022). Towards user-centered and legally relevant smart-contract development: A systematic literature review. *Journal of Industrial Information Integration*, *26*, 100314. https://doi.org/10.1016/j.jii.2021.100314

Durovic, M., & Janssen, A. (2019). The Formation of Blockchain-based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, *6*, 753–772. https://doi.org/10.54648/erpl2018053

Eenmaa, H., & Schmidt-Kessen, M. J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Giacomo Corrias, Moncada, R., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Huang, H., Guo, L., Zhao, L., Wang, H., Xu, C., & Jiang, S. (2024). Effective combining source code and opcode for accurate vulnerability detection of smart contracts in edge AI systems. *Applied Soft Computing*, *158*, 111556. https://doi.org/10.1016/j.asoc.2024.111556

Lasmoles, O., & Diallo, M. (2022). Impacts of Blockchains on International Maritime Trade. *Journal of Innovation Economics & Management*, *1*(37), 91–116. https://doi.org/10.3917/jie.pr1.0114

Lim, A. G., & En-Rong, P. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Petrová, M., Krügerová, M., & Koziel, M. (2021). Incoterms – History and Future Development. *Proceedings of the 15th International conference liberec economic forum* (pp. 589–590).

Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(2), 306–315.

Sang Man Kim. (2021). *Payment methods and finance for international trade*. Springer.

Souei, W. B. S., Hog, C. E., Djemaa, R. B., Sliman, L., & Amous, I. (2023). Towards smart contract distributed directory based on the uniform description language. *Journal of Computer Languages*, *77*, 101225. https://doi.org/10.1016/j.cola.2023.101225

Stojanović, Đ., & Ivetić, J. (2020). Possibilities of using Incoterms clauses in a country logistics performance assessment and benchmarking. *Transport Policy*, *98*, 217–228. https://doi.org/10.1016/j.tranpol.2020.03.012

Szabo, N. (1996). Smart contracts: building blocks for digital markets. E*XTROPY: The Journal of Transhumanist Thought*, *16*, 18–20.

Vatiero, M. (2022). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Vijai, C., Elayaraja, M., Suriyalakshmi, S. M., & Joyce, D. (2019). The Blockchain Technology and Modern Ledgers Through Blockchain Accounting. *Adalya Journal*, *8*(12), 545–557.

Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, & Muhammad Imran (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Authors information

Prince Fater Audu – Bachelor of Law, Faculty of Law, Ahmadu Bello University
Address: 810107, Kongo Campus, Zaria, Nigeria
E-mail: pfateraudu@gmail.com
ORCID ID: https://orcid.org/0009-0000-8289-3081

Fatima Shabih – Bachelor in Arts and Law, Faculty of Law, Jamia Millia Islamia University
Address: 110025, Jamia Nagar, New Delhi, India
E-mail: Shabihfatima010@gmail.com
ORCID ID: https://orcid.org/0000-0003-1661-232X

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 18, 2023
Date of approval – December 14, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004: 341.1/8:003.26
EDN: https://elibrary.ru/zhayee
DOI: https://doi.org/10.21202/jdtl.2024.17

Правовое регулирование международной торговли криптографическими продуктами и технологиями: инструменты ВТО и региональные соглашения

Сайед Кудрат Хашими ✉
Майсурский университет, Майсур, Индия

Джексон Симанго Магоге
Университет Иринга, Иринга, Танзания

Ключевые слова

Всемирная торговая организация,
защита интеллектуальной собственности,
кибербезопасность,
криптография,
международная торговля,
международные соглашения,
недискриминационный режим,
право,
региональные торговые соглашения,
цифровые технологии

Аннотация

Цель: показать сложный правовой ландшафт, меняющийся под воздействием современного цифрового ландшафта, развивающегося в условиях интеграции криптографических технологий в международную торговлю и особенно в сферу продуктов информационно-коммуникационных технологий.

Методы: исследование документов построено прежде всего на совокупности способов толкования актов, позволяющих проанализировать содержание первичных источников права, а именно положений, регулирующих оборот криптографических продуктов, и предложить решения, восполняющие существующие пробелы в этой области. Также для формирования представления о предмете исследования были собраны и обобщены вторичные источники по исследуемой проблематике.

Результаты: выявлены области неопределенности в защите цифровых криптографических продуктов в рамках соглашений ВТО, что ставит под сомнение адекватность существующих мер защиты. Отмечается, что в ряде стран такая ситуация приводит к ограничениям или к полному запрету на импорт и экспорт криптографических технологий и зашифрованных данных по соображениям безопасности. Уделено внимание рассмотрению концепции недискриминационного отношения к криптографическим продуктам, разрабатываемой в первую очередь в рамках региональных торговых соглашений, чтобы устранить недостатки соглашений ВТО. Подчеркивается, что региональные торговые соглашения, несмотря на стимулирования

✉ Контактное лицо

роста сотрудничества и конкуренции в международной торговле, демонстрируют различные подходы к регулированию криптографических продуктов. Отмечается, что это создает проблемы для бизнеса, который должен быть готов к учету особенностей региональных соглашений, местного законодательства и меняющихся правовых требований. Делается вывод о важности баланса между защитой инноваций и содействием доверию и сотрудничеству, развитием криптографических технологий и вопросами безопасности и защиты прав интеллектуальной собственности.

Научная новизна: представлено видение сложного правового ландшафта, окружающего криптографические продукты, показаны различия в подходах к регулированию отношений, связанных с цифровыми и нецифровыми продуктами в рамках соглашений ВТО, и подходы к регулированию криптографических продуктов, применяемые в региональных торговых соглашениях.

Практическая значимость: результаты исследования представляют интерес для государственных органов, политических деятелей, коммерческих структур и частных лиц, участвующих в международной торговле с использованием криптографических технологий, поскольку могут помочь всем заинтересованным сторонам принимать обоснованные решения, ориентироваться в сложностях регулирования указанных отношений и отстаивать справедливое отношение в развивающейся среде цифровой торговли.

Для цитирования

Хашими, С. К., Магоге, Дж. С. (2024). Правовое регулирование международной торговли криптографическими продуктами и технологиями: инструменты ВТО и региональные соглашения. *Journal of Digital Technologies and Law*, *2*(2), 328–344. https://doi.org/10.21202/jdtl.2024.17

Содержание

Введение

Глобальный ландшафт криптографических продуктов, охватывающих технологии шифрования, аппаратное и программное обеспечение, претерпевает значительные изменения. Это вызывает озабоченность регуляторов в сфере международной торговли (Kumar et al., 2020; Primo Braga, 2005; Kennedy, 2000). В представленном исследовании рассматривается нормативная база в рамках Всемирной торговой организации (далее – ВТО) и региональных торговых соглашений (далее – РТС), затрагиваются вопросы доверия в деловой сфере, прав интеллектуальной собственности и глобальной торговли. В документах ВТО отсутствуют конкретные положения о криптографических продуктах. В Соглашении по торговым аспектам прав интеллектуальной собственности (Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS Agreement, Соглашение ТРИПС) подчеркивается необходимость защиты прав интеллектуальной собственности производителей, но не прописаны исчерпывающие правовые основы такой защиты (Huang & Li, 2024). Соглашение по техническим барьерам в торговле (далее – ТВТ) предусматривает использование технических спецификаций, но они не должны чрезмерно ограничивать торговлю. Такие РТС, как USMCA и Japan – UK EPA, накладывают ограничения на производителей криптографических продуктов, стремясь сбалансировать требования защиты интеллектуальной собственности (далее – ИС) и принципов доверия. Однако эти РТС могут различаться по своим подходам, что создает проблемы для бизнеса. В целом нормативно-правовая база стремится к балансу между защитой ИС и доверием, при этом страны – члены ВТО тщательно следят за тем, чтобы избежать злоупотреблений и адаптироваться к динамичному криптографическому рынку. До наступления «информационной эры» криптография и технологии защиты информации использовались в основном в военных и разведывательных целях (Rogers, 2021). В прошлом эти технологии рассматривались как инструменты ведения войны. Однако за последние тридцать лет криптография приобрела большое значение в обеспечении индивидуальной конфиденциальности в повседневной розничной торговле и потребительских технологиях. В условиях, когда растет обеспокоенность по поводу цензуры и законов о конфиденциальности, безопасность потребителей постоянно находится под угрозой. Они сталкиваются с необходимостью активно защищать свои данные. Кроме того, технологии значительно упростили процесс получения доступа к личной информации, поэтому необходимо понимать, как создать и поддерживать в актуальном состоянии меры по защите данных, соответствующие новейшим достижениям в области технологий защиты информации. Сбалансировать эти тенденции стало возможно благодаря интеграции технологии криптографии в современный цифровой мир (Saper, 2013). Криптография имеет огромное значение, поскольку она служит жизненно важным компонентом в обеспечении безопасности электронной коммерции и электронных коммуникационных систем (Thabit et al., 2023). Она играет ключевую роль в защите конфиденциальных данных как при их хранении, так и при передаче. Значение информационной безопасности постоянно растет по мере того, как продукты и услуги в области информационных технологий занимают все более заметное место на мировом рынке. Кроме того, компании, осуществляющие прямые иностранные инвестиции, делают акцент на высокотехнологичных секторах, которые несут в себе риски для интеллектуальной собственности, что еще больше подчеркивает важность информационной безопасности[1].

[1] Protecting privacy in practice – The current use, development and limits of Privacy Enhancing. (2019, March 20). Policy Commons. https://clck.ru/3BCb9M

Таким образом, в контексте международной торговли становится очевидной зависимость от криптографических технологий, поскольку они обеспечивают безопасность многочисленных онлайн-транзакций и способствуют быстрому осуществлению платежей по всему миру. Кроме того, развитие криптографических технологий оказывает значительное влияние на современную деловую практику, поскольку они играют решающую роль в защите корпоративных секретов и конфиденциальной информации от таких угроз, как кража персональных данных. В связи с этим наблюдается рост производства криптографических продуктов, обусловленный рыночным спросом. В настоящее время некоторые страны вводят ограничения на импорт и экспорт криптографических технологий.

Некоторые из них, например Китай, Россия и Израиль, ограничивают импорт зашифрованных данных, а другие, например Северная Корея, ограничивают или полностью запрещают использование шифрования в пределах своих границ[2]. В некоторых странах для отправки шифровальных продуктов за границу требуется официальное разрешение, независимо от того, производятся ли эти продукты внутри страны или нет. Это требование распространяется как на первоначально экспортируемые изделия, так и на те, которые реэкспортируются из страны. Основная цель такого требования – поддержание национальной безопасности и противодействие терроризму.

1. Криптография и ее технологические продукты

Криптография, древнее искусство кодирования и декодирования, стала краеугольным камнем цифровой эпохи, обеспечивая безопасную связь и защиту данных. С помощью математических методов можно сделать данные недоступными для неавторизованных лиц. Целями этого процесса является обеспечение конфиденциальности, целостности и подлинности информации. Эта технология лежит в основе таких продуктов, как приложения для безопасного обмена сообщениями, VPN, аппаратные модули безопасности (HSM), программное обеспечение для шифрования данных и защиты блокчейна. Криптографические инструменты, такие как цифровые подписи, двухфакторная аутентификация (2FA) и PKI, повышают уровень безопасности[3]. Криптография играет важную роль в защите данных, обеспечении подлинности цифровых документов и укреплении сетевой безопасности с помощью таких протоколов, как SSL и TLS. В условиях взаимосвязанного мира она является неотъемлемым элементом безопасности и конфиденциальности данных.

Криптография – это технология для обеспечения безопасной связи даже в присутствии вредоносных третьих сторон с помощью шифрования и дешифрования. Обычно она предполагает использование вычислительного алгоритма, например SHA256, как в биткоине, открытого ключа и закрытого ключа, который служит цифровой подписью для пользователя. При шифровании сообщения или документа только предполагаемые получатели могут узнать его содержание (Kimani et al., 2020; Zharova & Lloyed, 2018; Torrubia et al., 2001).

---

2 Human Rights Watch: Rape common in North Korea. (2018) https://clck.ru/3BCbAM

3 Understanding Digital Signatures. (2021, February 1). CISA. https://clck.ru/3BCbB6

В рамках международной торговли криптографические технологии могут быть интегрированы как в экспортируемые, так и в импортируемые продукты информационно-коммуникационных технологий (далее – ИКТ). Криптографический продукт включает в себя криптографический модуль; под эту категорию подпадает также защищенное программное обеспечение, способное создавать или воссоздавать ключи или сертификаты (Riebe et al., 2022). Примерами таких продуктов являются зашифрованные смартфоны и ноутбуки, защищенные факс-аппараты, VPN-устройства с возможностью шифрования, устройства для проведения финансовых операций в точках продаж, системы управления складским хозяйством с функцией шифрования; устройства ввода, оснащенные функцией шифрования; стандартные компьютеры, на которые предварительно установлено программное обеспечение для шифрования; медицинские устройства; промышленные и производственные системы, такие как робототехника и тяжелое оборудование; системы для охраны объектов, такие как пожарная сигнализация; а также специализированные компоненты шифрования, например, чипы, маршрутизаторы, шлюзы и брандмауэры.

1.1. Криптографическая продукция и политика в отношении нее ВТО и ОЭСР

В цифровую эпоху, когда конфиденциальность данных и безопасная связь имеют первостепенное значение, криптография играет важную роль в международной торговле. Хотя в соглашениях Всемирной торговой организации криптография прямо не рассматривается, эти документы косвенно влияют на продукты информационно-коммуникационных технологий, использующие криптографические методы (Sholihah & Afriansyah, 2020). Так, Соглашение о технических барьерах в торговле (Agreement on Technical Barriers to Trade, TBT) направлено на предотвращение препятствования международной торговле со стороны технических регламентов. Не упоминая криптографию напрямую, оно постулирует прозрачные и необходимые правила для достижения законных целей, таких как безопасность. Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS) косвенно затрагивает криптографические продукты, защищая права интеллектуальной собственности, в том числе патенты, авторские права и коммерческие тайны, связанные с криптографическими технологиями. Это стимулирует инновации и торговлю продуктами ИКТ, основанными на криптографии.

Организация экономического сотрудничества и развития (далее – ОЭСР) играет важную роль в формировании политики в отношении криптографических продуктов. Эта организация дает рекомендации по безопасности и конфиденциальности данных, что влияет на внедрение криптографических решений. Она подчеркивает важность кибербезопасности, жизненно важным инструментом которой является криптография, и способствует разработке криптографических продуктов. Работа ОЭСР также затрагивает трансграничные потоки данных и косвенно влияет на отрасль через экономическую политику. По сути, влияние ОЭСР на разработку и использование криптографических продуктов имеет глобальное значение для бизнеса и потребителей в цифровую эпоху[4]. В рамках ОЭСР были разработаны правила,

[4] OECD Guidelines for Cryptography Policy – OECD. (n.d.). Retrieved October 16, 2023. https://clck.ru/3BCf5o

касающиеся криптографии. Криптография играет важную роль в повышении безопасности информационно-коммуникационных сетей и систем, однако ее неправильное использование может пагубно сказаться на функциональности электронной коммерции и защите частной жизни. В 1997 г. ОЭСР представила Руководство по политике в области криптографии. В нем изложены принципы политики в области криптографии, одним из которых является законный доступ. В документе отмечено, что национальные нормы в области криптографии могут предоставлять законный доступ к незашифрованным данным или криптографическим ключам при условии, что эти нормы соответствуют принципам, изложенным в других руководствах.

2. Соглашения ВТО, касающиеся криптографических продуктов

2.1. Соглашение о технических барьерах в торговле (ТВТ)

Основная цель Соглашения по техническим барьерам в торговле (TBT Agreement) Всемирной торговой организации заключается в том, чтобы технические регламенты, стандарты и процедуры оценки соответствия не создавали ненужных препятствий для международной торговли. Хотя указанное Соглашение не содержит конкретных положений, регулирующих технические барьеры, связанные с криптографическими продуктами, оно позволяет странам – членам ВТО, согласно ст. 2.2, устанавливать технические спецификации для продуктов, включающих криптографические технологии, при условии, что эти спецификации не являются «более ограничивающими торговлю, чем это необходимо для достижения законной цели» (Lin et al., 2021). Кроме того, ст. 5 предоставляет странам – членам ВТО право обеспечивать соответствие импортируемых продуктов с криптографической технологией этим техническим спецификациям в соответствии с правилами, изложенными в Соглашении. Что касается устранения определенных барьеров, связанных с криптографическими продуктами в Китае, в частности, в контексте пересмотренного законопроекта КНР о шифровании, изданного государственным Управлением по вопросам коммерческой криптографии (OSCCA), Канада выразила свою обеспокоенность (Kang, 1998), запросив у Китая гарантии того, что практические нормы предусматривают:

1) определение сферы применения таким образом, чтобы обеспечить достижение законных целей в отношении криптографических товаров;

2) четкое указание на то, что стандарты будут установлены в соответствии с принципом прозрачности;

3) четкое указание важности использования международных стандартов, когда это возможно.

2.2. Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS)

Соглашение TRIPS не содержит четких положений, касающихся криптографических продуктов. Тем не менее ст. 10(1) Соглашения предписывает защищать исходный код, если он подпадает под защиту патента, авторского права или коммерческой тайны. Кроме того, Соглашение TRIPS предусматривает, что компьютерные программы, независимо от того, представлены ли они в исходном или объектном коде, должны рассматриваться как литературные произведения, охраняемые в соответствии с Бернской конвенцией 1971 г.

2.3. Соглашение GATT и недискриминационный режим в отношении криптографических продуктов

Концепция «недискриминационного отношения к криптографическим продуктам» подчеркивает беспристрастное регулирование со стороны правительств и регулирующих органов. Она направлена на обеспечение справедливых стандартов для всех криптографических продуктов, как отечественных, так и международных, признавая их роль в обеспечении безопасности данных. Ключевые принципы включают равный доступ на рынок, защиту конфиденциальности и международное сотрудничество. Эта концепция ставит во главу угла справедливость, прозрачность и оценку продукта на основе технических достоинств, а не происхождения, тем самым поддерживая развитие криптографии для обеспечения безопасности цифровых коммуникаций и защиты данных в нашем взаимосвязанном мире. Статья I Генерального соглашения по тарифам и торговле (General Agreement on Tariffs and Trade, GATT) предписывает, что государства – члены Соглашения не должны проявлять фаворитизма по отношению к своим торговым партнерам и создавать для них режим наибольшего благоприятствования, а также должны избегать дискриминации между своими и иностранными товарами, как это сформулировано в ст. III (Baldwin et al., 2000).

Аналогичным образом, Генеральное соглашение по торговле услугами (General Agreement on Trade in Services, GATS) требует, чтобы иностранным услугам предоставлялся режим наибольшего благоприятствования в соответствии со ст. II. Однако национальный режим, подробно описанный в ст. XVII, не является обязательным, если только государство-член не взяло на себя особые обязательства по его предоставлению (Muller, 2017). Несмотря на то, что GATT и GATS запрещают дискриминационный режим в отношении товаров и услуг, остается неясным, получают ли «цифровые продукты, включая криптографические», такую же защиту, как и нецифровые продукты в рамках соглашений ВТО. Кроме того, Орган по разрешению споров (Dispute Settlement Body, DSB) не дал никаких разъяснений относительно регулирования и защиты криптографических продуктов в соответствии с соглашениями ВТО. С ростом поставок продукции в цифровых форматах все большее значение приобретают вопросы справедливого отношения к «криптографическим продуктам».

В связи с этим концепция недискриминации разрабатывается в первую очередь в рамках региональных торговых соглашений, чтобы устранить недостатки соглашений ВТО. Однако важно отметить, что РТС обычно ссылаются на принципы, установленные в рамках соглашений ВТО.

3. Региональные соглашения, касающиеся криптографических продуктов

Региональные торговые соглашения оказывают значительное влияние на торговлю и регулирование криптографических продуктов в отдельных регионах. Они способствуют экономической интеграции и снижению торговых барьеров между странами-участницами, поощряя стандартизацию технических протоколов, снижение тарифов и расширение доступности рынков (Rahman & Rahman, 2022). РТС также оказывают влияние на права интеллектуальной собственности и правила защиты данных для технологий шифрования. Они способствуют росту сотрудничества и конкуренции в сфере безопасности, стимулируя инновации в криптографических

продуктах. Однако их конкретное воздействие зависит от условий соглашения, отраслевого и местного законодательства, что требует от предприятий бдительного контроля для адаптации к меняющимся правовым требованиям.

Речь идет о двусторонних или многосторонних торговых соглашениях, основанных на взаимных предпочтениях и санкционированных ВТО. В ст. XXIV:5 GATT предусмотрено создание таможенных союзов, зон свободной торговли или соглашений между регионами участвующих сторон (Dam, 1963) Аналогичным образом, согласно ст. V:1 GATS, страны-члены могут заключать соглашения, способствующие либерализации торговли. Ниже рассмотрим региональные торговые соглашения, содержащие особые положения в отношении продуктов ИКТ с использованием технологий шифрования.

3.1. Соглашение между США, Мексикой и Канадой (USMCA)

Соглашение между США, Мексикой и Канадой (USMCA) существенно влияет на рынок криптографических продуктов в Северной Америке. Оно затрагивает вопросы интеллектуальной собственности, локализации данных и цифровой торговли, влияя на развитие и регулирование криптографических технологий. Соглашение способствует сотрудничеству в области регулирования и доступности рынков, что благоприятно сказывается на предприятиях и потребителях в этой сфере[5]. Кроме того, в нем сделан акцент на сотрудничестве в области кибербезопасности, что подчеркивает важность криптографических продуктов для обеспечения безопасности и конфиденциальности данных. Компаниям данного сектора предлагается отслеживать, как положения Соглашения повлияют на их деятельность и соблюдение требований законодательства в регионе.

Указанное Соглашение выступило заменой Североамериканскому соглашению о свободной торговле (The North American Free Trade Agreement, NAFTA), действовавшему с января 1994 г. Оно было одобрено тремя странами 30 ноября 2018 г. и вступило в силу 1 июля 2020 г. Это соглашение рассматривается как взаимовыгодное для сотрудников и владельцев промышленных и сельскохозяйственных предприятий стран Северной Америки (van der Linden & Shirazi, 2023).

3.2. Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (Japan – UK EPA)

Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (The Japan – UK Comprehensive Economic Partnership Agreement, Japan – UK EPA) в первую очередь направлено на сферы торговли и экономики, но имеет последствия для криптографических продуктов. Оно упрощает доступ к рынкам за счет снижения торговых барьеров решает вопросы интеллектуальной собственности, поощряет сотрудничество в сфере регулирования, а также затрагивает вопросы конфиденциальности данных и сотрудничества в области кибербезопасности (Riebe et al., 2022). Электронная коммерция и цифровая торговля также влияют на цифровой рынок криптографических продуктов. Предприятия этого сектора

[5] United States – Mexico – Canada Agreement. United States Trade Representative. (n. d.). https://clck.ru/3BCbhB

должны знать положения данного Соглашения, чтобы соответствовать требованиям и полноценно использовать рыночные возможности.

Указанное соглашение о свободной торговле было подписано в Токио в октябре 2020 г. Оно направлено на содействие либерализации торговли и инвестиций, укреплению экономических отношений между сторонами-участницами и включает элементы соглашений ВТО. Примечательно, что ст. 1.9 Соглашения запрещает любые действия сторон, противоречащие их обязательствам по соглашениям ВТО. Документ также содержит положения, касающиеся коммерческих продуктов ИКТ, использующих криптографию.

Национальный режим в таких торговых соглашениях, как Japan – UK EPA и USMCA, имеет решающее значение для криптографических продуктов. Он обеспечивает равный режим для отечественных и иностранных криптографических товаров, способствуя честной конкуренции и доступу на рынок. Оба указанных соглашения поддерживают этот принцип, устраняя дискриминацию по признаку происхождения продукции (Burri, 2021). Это крайне важно в связи с чувствительным характером криптографических технологий, а также с необходимостью содействовать инновациям и кибербезопасности. Предприятия этой отрасли должны строго соблюдать нормы соглашений для обеспечения соответствия требованиям законодательства и равного доступа на рынки.

Документы не содержит четкого описания национального режима криптографических продуктов. Однако, согласно ст. 2.7 Japan – UK EPA и 2.3 USMCA, каждая сторона обязана предоставлять национальный режим товарам другой стороны, как указано в ст. III GATT (Burri, 2023). Кроме того, частью соглашений являются ст. III и XX GATT. Таким образом, защита криптографических продуктов обеспечивается положениями этих конкретных статей.

4. Проблема доступа к криптографическим продуктам

Для обеспечения безопасности и конфиденциальности данных жизненно важен доступ к криптографическим продуктам. Эти продукты используют сложные алгоритмы для защиты информации от киберугроз и обеспечения целостности данных. Они необходимы для защиты персональных данных, национальной безопасности и безопасных онлайн-транзакций[6]. Однако глобальное регулирование повлияет на режим такого доступа, и может быть крайне сложно достичь баланса между требованиями безопасности и доступности. Ключевым фактором для трансграничной защиты данных является международное сотрудничество. Поскольку криптографические продукты выпускаются в различных формах, важнейшее значение имеет повышение осведомленности и их правильное использование. Таким образом, доступ к криптографическим продуктам необходим для защиты данных, обеспечения конфиденциальности и безопасности в условиях развивающейся нормативной базы.

Доступ к криптографическим продуктам подразумевает передачу или получение доступа к закрытому ключу или другим конфиденциальным параметрам, особенностям алгоритма или деталям конструкции стороной или лицом, находящимся

6 OECD Guidelines for Cryptography Policy – OECD. (n.d.). https://clck.ru/3BCf5o

под юрисдикцией этой стороны (например, производителями или поставщиками)[7]. Соглашения Всемирной торговой организации прямо не затрагивают вопрос доступа к криптографическим продуктам. Однако Соглашение между США, Мексикой и Канадой (USMCA) и Соглашение об экономическом партнерстве между Японией и Великобританией (EPA) накладывают ограничения на своих участников, заставляя производителей и поставщиков криптографических продуктов передавать или предоставлять доступ к патентованной информации, связанной с криптографией. USMCA накладывает строгие ограничения на все криптографические товары, тогда как EPA ограничивает доступ к коммерческой информации и продуктам информационно-коммуникационных технологий, использующим криптографию, включая программное обеспечение. Обоснованием введения этих ограничений на доступ к криптографическим продуктам является установление доверительных деловых отношений между участниками соглашения и соблюдение положений статьи 10(1) Соглашения по торговым аспектам прав интеллектуальной собственности (TRIPS), которая обеспечивает защиту прав интеллектуальной собственности для производителей[8]. Напротив, Руководство по политике в области криптографии ОЭСР предлагает альтернативный подход к доступу к криптографическим продуктам. Национальное законодательство в области криптографии может разрешать законный доступ к открытому тексту или криптографическим ключам для зашифрованных данных, но при этом должны соблюдаться и другие принципы, изложенные в Руководстве. Страны-участницы могут по своему усмотрению принимать законы, касающиеся доступа к криптографическим продуктам, однако существует опасность злоупотреблений в этой сфере.

Важно отметить, что в соответствии со ст. 2.2 Соглашения о технических барьерах в торговле членам ВТО разрешается устанавливать технические спецификации для продуктов, использующих технологию криптографии, при условии, что эти спецификации не создают торговых барьеров, которые являются более ограничительными, чем это необходимо для достижения законной цели. Возникает вопрос, может ли разрешение законного доступа к криптографическим продуктам представлять собой злоупотребление в области делового доверия и прав интеллектуальной собственности.

Заключение

В заключение следует отметить, что криптография – играет важную роль в обеспечении безопасности связи, защиты данных, конфиденциальности, целостности и подлинности информации. От безопасных приложений для обмена сообщениями до защиты блокчейна – применение криптографических технологий разнообразно и широко распространено, они лежат в основе современного цифрового ландшафта. Интеграция криптографических технологий в международную торговлю, особенно в сферу продуктов информационно-коммуникационных технологий, порождает сложные проблемы регулирования. Хотя соглашения Всемирной торговой организации прямо не касаются криптографии, они косвенно влияют на криптографические продукты, способствуя прозрачному регулированию в целях безопасности и защиты

7 Encryption in the Microsoft Cloud. Microsoft. https://clck.ru/3BCboE

8 WTO. Overview: the TRIPS Agreement. (n. d.).https://clck.ru/3BCbpN

прав интеллектуальной собственности. Соглашение по техническим барьерам в торговле призвано предотвратить препятствование международной торговле со стороны технических норм, а Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS) косвенно защищает права интеллектуальной собственности, связанные с криптографическими технологиями, тем самым способствуя инновациям и торговле продуктами ИКТ, использующими криптографию.

Проблема недискриминационного отношения к криптографическим продуктам по-прежнему вызывает серьезную озабоченность. Решить эту проблему, предлагая рамки для обращения с криптографическими продуктами, призваны региональные торговые соглашения, такие как Соглашение между США, Мексикой и Канадой (USMCA) и Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (Japan – UK EPA). Сложная и непрерывно развивающаяся нормативная база для криптографических продуктов подчеркивает необходимость международных соглашений для адаптации к меняющемуся ландшафту глобального криптографического рынка. Для формирования будущего международной торговли криптографическими продуктами очень важен баланс между защитой инноваций и содействием доверию и сотрудничеству. Кроме того, продолжающиеся дебаты вокруг использования экспортных и импортных ограничений, препятствующих развитию криптовалютных технологий, подчеркивают важность этого вопроса в глобальном масштабе.

Таким образом, по мере того как мир становится все более взаимосвязанным и зависимым от криптографических технологий, международные соглашения, национальные нормы и региональные торговые соглашения будут продолжать играть ключевую роль в формировании политики в отношении криптографических продуктов, обеспечивая инновации и безопасность в цифровую эпоху.

Список литературы

Baldwin, R. E., McLaren, J., & Panagariya, A. (2000). Regulatory Protectionism, Developing Nations, and a Two-Tier World Trade System. *Brookings Trade Forum*, *3*(2674), 237–293. https://doi.org/10.1353/btf.2000.0001

Burri, M. (2021). Data Flows and Global Trade Law. In *M. Burri (Ed.), Big Data and Global Trade Law* (pp. 11–41). Cambridge University Press. https://doi.org/10.1017/9781108919234.003

Burri, M. (2023). A WTO agreement on electronic commerce: an inquiry into its legal substance and viability. *Georgetown Journal of International Affairs*, *53*(4), 565–625.

Dam, K. W. (1963). Regional Economic Arrangements and the GATT: The Legacy of a Misconception. *The University of Chicago Law Review*, *30*(4), 615–665. https://doi.org/10.2307/1598756

Huang, Q., & Li, Z. (2024). *Trade and peace: The WTO case*. China Economic Review, 83, 102072. https://doi.org/10.1016/j.chieco.2023.102072

Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, *50*(4), 1193–1294. https://doi.org/10.2307/1229286

Kennedy, G. (2000). Encryption Policies: codemakers, codebreakers and rulemakers. *Computer Law & Security Review*, *16*(4), 240–247. https://doi.org/10.1016/s0267-3649(00)89131-1

Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J., & Kim, J. (2020). Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how? *Technological Forecasting and Social Change*, *161*(161), 120254. https://doi.org/10.1016/j.techfore.2020.120254

Kumar, G., Saha, R., Buchanan, W. J., Geetha, G., Thomas, R., Rai, M. K., Kim, T.-H., & Alazab, M. (2020). Decentralized accessibility of e-commerce products through blockchain technology. *Sustainable Cities and Society*, *62*, 102361. https://doi.org/10.1016/j.scs.2020.102361

Lin, C.-F., Peng, S., & Streinz, T. (Eds.). (2021). Reconceptualizing World Trade Organization Law for the Artificial Intelligence Economy. In *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Part II, pp. 95–172). Cambridge University Press.

Muller, G. (2017). Troubled Relationships under the GATS: Tensions between Market Access (Article XVI), National Treatment (Article XVII), and Domestic Regulation (Article VI). *World Trade Review*, *16*(3), 449–474. https://doi.org/10.1017/S1474745616000471

Primo Braga, C. A. (2005). E-commerce regulation: New game, new rules? *The Quarterly Review of Economics and Finance*, *45*(2–3), 541–558. https://doi.org/10.1016/j.qref.2004.12.019

Rahman, M. N., & Rahman, N. (2022). Exploring digital trade provisions in Regional Trade Agreements (RTAs) in times of crisis: India and Asia-Pacific countries. *Asia and the Global Economy*, *2*(2), 100036. https://doi.org/10.1016/j.aglobe.2022.100036

Riebe, T., Kühn, P., Imperatori, P., & Reuter, C. (2022). U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance. *European Journal for Security Research*, *7*(1), 39–65. https://doi.org/10.1007/s41125-022-00080-0

Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age: What Happened? *The Cyber Defense Review*, *6*(1), 81–106.

Saper, N. (2013). International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property*, *11*(7), 673.

Sholihah, R., & Afriansyah, A. (2020). Regulation of Crypto Currency in World Trade Organization. In *Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*. https://doi.org/10.2991/aebmr.k.200321.006

Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography Algorithms for Enhancing IoT Security. *Internet of Things*, *22*, 100759. https://doi.org/10.1016/j.iot.2023.100759

Torrubia, A., Mora, F. J., & Marti, L. (2001). Cryptography Regulations for E-commerce and Digital Rights Management. *Computers & Security*, *20*(8), 724–738. https://doi.org/10.1016/s0167-4048(01)00814-8

van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, *9*(1), 22. https://doi.org/10.1186/s40854-022-00432-8

Zharova, A., & Lloyd, I. (2018). An examination of the experience of cryptocurrency use in Russia. In search of better practice. *Computer Law & Security Review*, *34*(6), 1300–1313. https://doi.org/10.1016/j.clsr.2018.09.004

Сведения об авторах

Хашими Сайед Кудрат – PhD в области права, кафедра правоведения, Майсурский университет
Адрес: Индия, г. Майсур, 570005, Вишвавидьянилайа Карья Судха, Крофорд Холл
E-mail: sayedqudrathashimy@law.uni-mysore.ac.in
ORCID ID: https://orcid.org/0000-0001-9835-0575
Google Scholar ID: https://scholar.google.com/citations?user=_XhWcpEAAAAJ

Магоге Джексон Симанго – ассистент преподавателя, Университет Иринга
Адрес: Танзания, г. Иринга, а/я 200
E-mail: simangojackson@gmail.com
ORCID ID: https://orcid.org/0000-0001-8096-6929
Google Scholar ID: https://scholar.google.com/citations?user=8FERpVoAAAAJ

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: 10.89.27 / Обязательственное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 16 октября 2023 г.
Дата одобрения после рецензирования – 10 ноября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004: 341.1/8:003.26
EDN: https://elibrary.ru/zhayee
DOI: https://doi.org/10.21202/jdtl.2024.17

Legal Regulation of International Trade in Cryptographic Products and Technologies: WTO Tools and Regional Agreements

Sayed Qudrat Hashimy ✉
University of Mysore, Mysore, India

Jackson Simango Magoge
University of Iringa, Iringa, Tanzania

Keywords

cryptography,
cybersecurity,
digital technologies,
intellectual property rights protection,
international agreements,
international trade,
law,
non-discriminatory regime,
regional trade agreements,
World Trade Organization

Abstract

Objective: to demonstrate the complex legal landscape which is being changed under the influence of the modern digital landscape developing with the integration of cryptographic technologies into international trade and especially into the field of information and communication technology products.

Methods: the study of the documents is built primarily on a set of ways of interpreting legal acts, which allows analyzing the content of primary legal sources, namely the provisions for cryptographic products circulation, and proposing solutions to fill the gaps in this area. Also, secondary sources were collected and summarized to form an idea of the study subject.

Results: areas of uncertainty in the protection of digital cryptographic products under the WTO agreements have been identified, raising questions about the adequacy of existing protection measures. It is noted that in some countries this situation has led to restrictions or bans on the import and export of cryptographic technologies and encrypted data on security grounds. The authors pay attention to the concept of non-discriminatory treatment of cryptographic products, which is being developed primarily within the framework of regional trade agreements to address the shortcomings of WTO agreements. It is emphasized that regional trade agreements,

✉ Corresponding author

although stimulating cooperation and competition in international trade, demonstrate various approaches to the regulation of cryptographic products. The authors note that this creates challenges for business and it must be prepared to take into account the specificities of regional agreements, local legislation and evolving legal requirements. A conclusion is made that it is important to balance the innovation protection with the promotion of trust and cooperation, between the cryptographic technologies development and the issues of security and intellectual property rights protection.

Scientific novelty: a vision of the complex legal landscape surrounding cryptographic products is presented, showing the differences in approaches to regulating relations around digital and non-digital products under WTO agreements and approaches to regulating cryptographic products applied in regional trade agreements.

Practical significance: the study results are of interest to government agencies, policy makers, commercial entities and individuals involved in international trade in cryptographic technologies, as they can help all stakeholders to make informed decisions, navigate the complexities of regulating these relationships and advocate for fair treatment in the evolving digital trade environment.

For citation

Hashimy, S. Q., & Magoge, J. S. (2024). Legal Regulation of International Trade in Cryptographic Products and Technologies: WTO Tools and Regional Agreements. *Journal of Digital Technologies and Law, 2*(2), 328–344. https://doi.org/10.21202/jdtl.2024.17

References

Baldwin, R. E., McLaren, J., & Panagariya, A. (2000). Regulatory Protectionism, Developing Nations, and a Two-Tier World Trade System. *Brookings Trade Forum*, *3*(2674), 237–293. https://doi.org/10.1353/btf.2000.0001

Burri, M. (2021). Data Flows and Global Trade Law. In *M. Burri (Ed.), Big Data and Global Trade Law* (pp. 11–41). Cambridge University Press. https://doi.org/10.1017/9781108919234.003

Burri, M. (2023). A WTO agreement on electronic commerce: an inquiry into its legal substance and viability. *Georgetown Journal of International Affairs*, *53*(4), 565–625.

Dam, K. W. (1963). Regional Economic Arrangements and the GATT: The Legacy of a Misconception. *The University of Chicago Law Review*, *30*(4), 615–665. https://doi.org/10.2307/1598756

Huang, Q., & Li, Z. (2024). *Trade and peace: The WTO case*. China Economic Review, 83, 102072. https://doi.org/10.1016/j.chieco.2023.102072

Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, *50*(4), 1193–1294. https://doi.org/10.2307/1229286

Kennedy, G. (2000). Encryption Policies: codemakers, codebreakers and rulemakers. *Computer Law & Security Review*, *16*(4), 240–247. https://doi.org/10.1016/s0267-3649(00)89131-1

Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J., & Kim, J. (2020). Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how? *Technological Forecasting and Social Change*, *161*(161), 120254. https://doi.org/10.1016/j.techfore.2020.120254

Kumar, G., Saha, R., Buchanan, W. J., Geetha, G., Thomas, R., Rai, M. K., Kim, T.-H., & Alazab, M. (2020). Decentralized accessibility of e-commerce products through blockchain technology. *Sustainable Cities and Society*, *62*, 102361. https://doi.org/10.1016/j.scs.2020.102361

Lin, C.-F., Peng, S., & Streinz, T. (Eds.). (2021). Reconceptualizing World Trade Organization Law for the Artificial Intelligence Economy. In *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Part II, pp. 95–172). Cambridge University Press.

Muller, G. (2017). Troubled Relationships under the GATS: Tensions between Market Access (Article XVI), National Treatment (Article XVII), and Domestic Regulation (Article VI). *World Trade Review*, *16*(3), 449–474. https://doi.org/10.1017/S1474745616000471

Primo Braga, C. A. (2005). E-commerce regulation: New game, new rules? *The Quarterly Review of Economics and Finance*, *45*(2–3), 541–558. https://doi.org/10.1016/j.qref.2004.12.019

Rahman, M. N., & Rahman, N. (2022). Exploring digital trade provisions in Regional Trade Agreements (RTAs) in times of crisis: India and Asia-Pacific countries. *Asia and the Global Economy*, *2*(2), 100036. https://doi.org/10.1016/j.aglobe.2022.100036

Riebe, T., Kühn, P., Imperatori, P., & Reuter, C. (2022). U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance. *European Journal for Security Research*, *7*(1), 39–65. https://doi.org/10.1007/s41125-022-00080-0

Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age: What Happened? *The Cyber Defense Review*, *6*(1), 81–106.

Saper, N. (2013). International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property*, *11*(7), 673.

Sholihah, R., & Afriansyah, A. (2020). Regulation of Crypto Currency in World Trade Organization. In *Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*. https://doi.org/10.2991/aebmr.k.200321.006

Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography Algorithms for Enhancing IoT Security. *Internet of Things*, *22*, 100759. https://doi.org/10.1016/j.iot.2023.100759

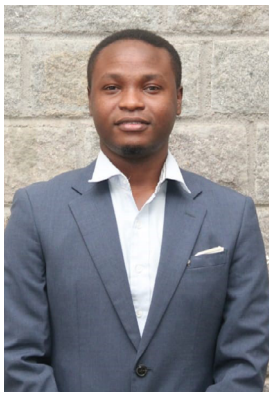
Torrubia, A., Mora, F. J., & Marti, L. (2001). Cryptography Regulations for E-commerce and Digital Rights Management. *Computers & Security*, *20*(8), 724–738. https://doi.org/10.1016/s0167-4048(01)00814-8

van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, *9*(1), 22. https://doi.org/10.1186/s40854-022-00432-8

Zharova, A., & Lloyd, I. (2018). An examination of the experience of cryptocurrency use in Russia. In search of better practice. *Computer Law & Security Review*, *34*(6), 1300–1313. https://doi.org/10.1016/j.clsr.2018.09.004

Authors information

Sayed Qudrat Hashimy – PhD Scholar (Law), Department of Studies in Law, University of Mysore
Address: Vishwavidyanilaya Karya Soudha, Crawford Hall, Mysuru-570005, India
E-mail: sayedqudrathashimy@law.uni-mysore.ac.in
ORCID ID: https://orcid.org/0000-0001-9835-0575
Google Scholar ID: https://scholar.google.com/citations?user=_XhWcpEAAAAJ



Jackson Simango Magoge – Assistant Lecturer, University of Iringa
Address: P.O Box 200, Iringa, Tanzania
E-mail: simangojackson@gmail.com
ORCID ID: https://orcid.org/0000-0001-8096-6929
Google Scholar ID: https://scholar.google.com/citations?user=8FERpVoAAAAJ

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 – October 16, 2023
Date of approval – November 10, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:347.21:004.4
EDN: https://elibrary.ru/uxqado
DOI: https://doi.org/10.21202/jdtl.2024.18

Опыт правового регулирования лутбоксов в различных странах: сравнительный анализ

Сэппи Пор

Группа компаний «Кун Консалтинг», Сидней, Австралия

Ключевые слова

азартные игры,
видеоигры,
виртуальный товар,
защита прав потребителей,
игровая индустрия,
лицензирование,
лутбокс,
право,
сравнительное правоведение,
цифровые технологии

Аннотация

Цель: показать как использование новой бизнес-модели, получившей название лутбоксов и лежащей в основе современных видеоигр, стало правовой проблемой для юрисдикций разных стран.

Методы: опираясь на существующую литературу и современные источники, в статье раскрываются потенциальные негативные последствия использования лутбоксов, проводится комплексный анализ действующего или предлагаемого регулирования, а также сравнение подходов, применяемых в различных национальных юрисдикциях.

Результаты: в данной статье рассматривается растущая обеспокоенность вокруг широкого распространения особой формы внутриигровых покупок называемой лутбоксами. Она подвергается резкой критике на том основании, что лутбоксы предположительно являются своего рода азартной игрой в составе видеоигры. Исходя из этого, в данной статье приводятся аргументы в пользу их законодательного регулирования. Изучив нормативно-правовую базу в странах, которые уже приняли меры против использования лутбоксов, таких как Бельгия, Нидерланды, Китай, Япония и Республика Корея, а также в странах, где в настоящее время обсуждается вопрос их регулирования, подчеркивается необходимость принятия мер по защите потребителей в игровой индустрии. Особенно это относится к уязвимым слоям населения, подверженных вредным последствиям, связанным с азартными играми. Кроме того, отмечается необходимость обеспечения этичного и ответственного использования лутбоксов, а также снижения рисков для здоровья и финансовых рисков, связанных с использованием данной бизнес-модели.

Научная новизна: в работе представлено сравнительное исследование проблем действующего или проектируемого социального регулирования лутбоксов в видеоиграх, решение которых предлагается искать на основе баланса между инновациями в игровой индустрии, защитой потребителей и благополучием пользователей, что в конечном итоге будет способствовать созданию более здоровой среды для геймеров.

Практическая значимость: представленное исследование подчеркивает международный масштаб рассматриваемой проблемы, различие принятых в странах регулятивных мер юридического и этического характера, направленных на решение психологических, социальных и финансовых последствий, связанных с распространением лутбоксов в видеоиграх, оценку которым еще предстоит дать в дальнейшем с учетом полученных данных в отрасли игровой индустрии.

Для цитирования

Пор, С. (2024). Опыт правового регулирования лутбоксов в различных странах: сравнительный анализ. *Journal of Digital Technologies and Law*, *2*(2), 345–371. https://doi.org/10.21202/jdtl.2024.18

Содержание

Введение

Во всем мире более 3 млрд человек играют в видеоигры[1]. Ожидается, что к 2025 г. это число достигнет 3,6 млрд человек, а рыночная стоимость индустрии видеоигр возрастет до 211,2 млрд долларов[2]. Часть этой стоимости определяется «микротранзакциями». Это бизнес-модель, которая позволяет игрокам приобретать виртуальные товары или другие внутриигровые преимущества за реальные деньги. Один из таких виртуальных товаров, которые можно приобрести с помощью микротранзакций, – это лутбоксы.

Лутбоксы (трофеи, добыча, гача) – это любой внутриигровой механизм, в котором из виртуальной коробки можно получить случайный игровой предмет (Drummond & Sauer, 2018). Лутбоксы обычно покупаются за реальные деньги или открываются помощью «ключей», которые необходимо приобрести за реальные деньги. Заранее неизвестно, какой предмет будет в коробке; вместо этого предлагаются ряд предметов, различающихся по редкости, силе, ценности и вероятности получения, причем вероятность появления более важных или ценных предметов будет ниже (Gong & Rodda, 2022). Из-за сходства с традиционными формами азартных игр, такими как игровые автоматы или лотерейные билеты, использование лутбоксов в современных видеоиграх вызвало бурные споры о его этических и юридических аспектах.

Игроки, особенно несовершеннолетние, зачастую тратят чрезмерные суммы на лутбоксы[3]; не редкость и поведение, которое традиционно описывается как азартная игра[4]. Исследования показывают корреляцию между использованием лутбоксов и степенью вовлеченности в азартные игры, что позволяет предположить, что некоторые люди могут быть особенно подвержены зависимости в этой сфере (Zendle & Cairns, 2019). Поэтому крайне важно обратить внимание на эти проблемы и принять меры регулирования для защиты потребителей, особенно тех, кто подвержен вредным последствиям, связанным с азартными играми.

В данной статье рассматриваются различные аргументы в пользу регулирования лутбоксов. Во-первых, мы изучим определение лутбоксов и их распространенность в современных видеоиграх. Во-вторых, будут рассмотрены возможные психологические и финансовые последствия этой бизнес-модели. Затем мы проанализируем существующие политические подходы и нормативные рамки в различных юрисдикциях и обсудим их обоснования и историю возникновения. Наконец, мы коснемся проблем, связанных с внедрением регулирования лутбоксов. Авторы стремились осветить различные аспекты регулирования лутбоксов и внести свой вклад в текущую научную и отраслевую дискуссию, касающуюся их механики. Мы выступаем за принятие мер по защите потребителей в игровой индустрии, а также по снижению рисков для здоровья и финансовых рисков, связанных с лутбоксами.

---

1 Wijman, T. (2023). Free Global Games Market Report. Newzoo. https://clck.ru/3A9d8c

2 Там же.

3 Gach, E. (2017, November 30). Meet The 19-Year-Old Who Spent Over $17,000 On Microtransactions. Kotaku. https://goo.su/cQpxD6g

4 Там же.

1. Лутбоксы: возникновение и определение

1.1. Возникновение микротранзакций

Использование реальных денег для покупки внутриигровых предметов не является чем-то новым; оно восходит к аркадной игре 1990 г. “Double Dragon 3: Rosetta Stone”, которая приобрела печальную известность введением микротранзакций[5]. Это классический однопользовательский сайд-скроллер и файтинг . В начале каждого из первых трех уровней игроки могут зайти в магазин и приобрести оружие, специальные атаки («трикс») и дополнительных персонажей.

Как и любая аркадная игра, Rosetta Stone побуждала игроков тратить деньги[6]. Без покупок во внутриигровом магазине персонажи имели всего одну жизнь, меньше здоровья, чем в предыдущих играх Double Dragon, и не имели доступа к оружию (из-за чего игрок также не мог использовать некоторые атаки и видеть анимации боя с оружием)[7]. После перевода игры для японской аудитории микротранзакции были полностью удалены, вероятно, из-за конфликтов, которые они вызвали в Северной Америке[8]. Одновременно с этим в игре «поменяли баланс»: теперь всех персонажей нужно было выбирать с самого начала, им усилили здоровье, дали доступ ко всем «трикс» и возможность добывать оружие на протяжении всей игры.

1.2. Лутбоксы в мейнстриме

В 2000-х гг. микротранзакции начали становиться нормой. В это время большую популярность приобрел игровой формат, известный как массовые многопользовательские онлайн-игры (multiplayer online game, MMO), в которые могли играть десятки миллионов людей[9]. В них использовались различные бизнес-модели[10].

Одна из них – это модель подписки, или «платы за игру», которая обычно составляла около 15 долларов в месяц. Например, столько стоила самая популярная MMO всех времен, World of Warcraft[11]. Другие популярные игры, такие как Guild Wars или Elder Scrolls Online, использовали модель «покупка игры», когда игрок должен купить полную версию игры, но затем может играть бесконечно без каких-либо дополнительных затрат. Существует также модель «бесплатная игра»: обычно разработчики стремятся максимально увеличить количество игроков, а затем вводят требование подписки или просто продают игру другому разработчику.

---

5 Derboo, S. (2016, November 4). Double Dragon 3 (Arcade). Hardcore Gaming 101. https://clck.ru/3A9dYA

6 (2022, June 9). Double Dragon 3: The Rosetta Stone (Arcade). The Cutting Room Floor. https://clck.ru/3A9dZS

7 Derboo, S. (2016, November 4). Double Dragon 3 (Arcade). Hardcore Gaming 101. https://clck.ru/3A9dbT

8 (2022, June 9). Double Dragon 3: The Rosetta Stone (Arcade). The Cutting Room Floor. https://clck.ru/3A9dc6

9 Top MMOs. MMO Populations. https://clck.ru/3A9ddP

10 Olivetti, J. (2016, 30 April). Massively OP’s guide to MMO business models. Massively Overpowered. https://clck.ru/3A9de5

11 Предполагается, что игрок оплачивает игру ежемесячно, а при оплате 6 или 12 месяцев авансом можно получить скидку.

На практике в MMO часто использовались гибридные бизнес-модели. Например, игра RIFT рекламируется как бесплатная, но позволяет игрокам приобрести «вип-пропуск», дающий «доступ к преимуществам подписки на определенный период времени»[12]. В игре также есть внутриигровой магазин предметов, где игроки могут тратить «кредиты» – внутриигровую валюту, которую можно купить за реальные деньги. Гибридный подход означает, что микротранзакции могли вводить в игру независимо от типа бизнес-модели. Это привело к появлению новой модели получения дохода, а именно основанной на продаже предметов (So & Westland, 2012).

Точно неизвестно, как возникли лутбоксы. So & Westland считают, что это произошло в китайском игровом сообществе, где игроки, как правило, не имели ни домашних компьютеров, ни игровых консолей, так как последние были запрещены по всей стране в 2000 г. (Liao, 2016). Таким образом, геймеры в основном играли в интернет-кафе, поэтому не покупали игры целиком; это заставило разработчиков искать альтернативные формы дохода. Тогда в 2007 г. компания Zhengtu Network выпустила игру Zhengtu Online. Это бесплатная MMO, позволяющая покупать «виртуальные коробки с сокровищами, которые могут содержать внутриигровые предметы, стоящие больше, чем стоимость самой коробки» (So & Westland, 2012). В том же году игра побила рекорды как в финансовом плане, так и по количеству игроков (So & Westland, 2012). В погоне за прибылью другие разработчики также стали обращать внимание на возможности лутбоксов в достижении крупного коммерческого успеха.

1.3. Определение и распространенность

Юридические определения азартных игр обычно включают три элемента: (а) привлекательность, (б) элемент удачи и (в) получение вознаграждения (Devereux, 1979). Такое толкование исключает игры, в которых требуется мастерство (Brenner & Brenner, 1990). Этому определению, безусловно, удовлетворяет часть, если не большинство существующих систем лутбоксов. В некоторых юрисдикциях это определение трактуют узко, объявляя лутбоксы легальными в рамках своей нормативной базы, поскольку игроки не получают вознаграждение в виде реальных денег (или в форме, которую можно напрямую обменять на реальные деньги, как, например, фишки казино)[13].

Другие специалисты отмечают хищнический и заманивающий характер лутбоксов, что оправдывает их отнесение к категории азартных игр (King & Delfabbro, 2018). Эти авторы полагают, что лутбоксы и другие хищнические схемы в видеоиграх «все больше сближают игровой процесс с азартными играми», поскольку «маскируют или придерживают долгосрочные затраты до тех пор, пока у игроков не разовьется финансовая и психологическая вовлеченность». Griffiths также утверждал, что непредсказуемость содержания лутбоксов по своей сути представляет азартную игру, поскольку стоимость вознаграждения зачастую меньше уплаченной цены (1995).

---

12 Game Guide | FAQ. Rift. https://clck.ru/3A9dgs

13 Nettleton, J., & Chong, K. (2013, October 16). Online social games – the Australian position. Mondaq. https://clck.ru/3A9dhY

После Zhengtu лутбоксы стали появляться во многих играх. Такие известные игры, как Call of Duty, Counter-Strike, FIFA, Destiny, Valorant и Overwatch, в настоящее время предлагают несколько различных форм лутбоксов. Например, в Counter-Strike из «контейнеров» можно получить «скины», что позволяет игрокам изменять внешний вид своего игрового оружия без каких-либо изменений в его функции (т. е. эффект чисто косметический)[14]. В игре FIFA игроки открывают «пакеты», чтобы получить лучших персонажей в свою команду и повысить ее шансы на победу[15].

В отчете за 2021 г., подготовленном компанией Juniper Research, было показано, что в 2020 г. доход от лутбоксов составил 15 млрд долларов, а к 2025 г. без вмешательства регулирующих органов этот показатель, по прогнозам, превысит 20 млрд долларов[16]. Лутбоксы получили широкое распространение в видеоиграх, особенно на мобильных платформах (Zendle et al., 2020a). Согласно анализу, проведенному Zendle et al., 58 % из 100 самых кассовых мобильных игр в магазине Google Play и 59 % в магазине приложений Apple содержат лутбоксы. Для сравнения, анализ 463 самых популярных игр на платформе Steam (цифровой сервис по продаже видеоигр) показал, что 71 % из них содержат лутбоксы (Zendle et al., 2020b). Таким образом, использование лутбоксов в компьютерных играх в период 2010–2019 гг. выросло на 67 %, причем самый быстрый рост наблюдался в 2012–2014 гг. Хотя бы один лутбокс приобрели 78 % взрослых геймеров (Zendle et al., 2020a).

2. Аргументы в пользу правового регулирования

2.1. Обеспечение этического поведения

2.1.1. Психологическое манипулирование

Притягательность элемента удачи при получении вознаграждения и использование методов убеждения могут оказывать значительное психологическое воздействие, потенциально приводя к зависимому поведению или к укреплению склонности к азартным играм. Как и в случае традиционных азартных игр, здесь используются такие психологические техники, как оперантное обучение (Staddon & Cerutti, 2003) и режим подкрепления с изменяющейся пропорцией (Zuriff, 1970). Они повышают вовлеченность и удовлетворенность игроков.

Мотивация повышается от предвкушения и волнения от неопределенности того, что они могут получить. Это создает ощущение награды и эйфории при получении редких или ценных предметов. Как отмечается в литературе по поведенческой психологии, эти явления основаны на представлении о том, что непредсказуемые вознаграждения сильнее мотивируют и вызывают привыкание, чем предсказуемые или ожидаемые (Deans et al., 2017). Переменный характер вознаграждений в лутбоксах, иногда приводящий к сценарию «еще чуть-чуть», может подпитывать цикл предвкушения и постоянного вовлечения, поскольку игроки стремятся получить все новые и более ценные предметы.

---

14 Container. Counter Strike Wiki. https://clck.ru/3A9dji

15 Your Guide to: FIFA Ultimate Team Packs. FIFA. https://clck.ru/3A9dk3

16 Moar, J., & Hunt, N. (2021, March 9). ‘Video Game Loot Boxes to Generate Over $20 Billion in Revenue by 2025. Juniper Research. https://clck.ru/3A8Xn6

Неопределенность и элемент случайности могут вызвать дополнительные когнитивные искажения, такие как «иллюзия контроля» и «ошибка игрока», заставляя игроков верить, что они сильнее контролируют результат, чем есть на самом деле. Это может привести к зависимому поведению и чрезмерным тратам, когда игроки гонятся за желанными предметами или не могут смириться с потерей.

2.1.2. Финансовая эксплуатация

Специалисты утверждают, что среди молодых людей использование лутбоксов может закрепить поведение, схожее с поведением азартного игрока, что может привести к проблемам на более поздних этапах жизни. Недавний анализ, проведенный Primi et al., показал, что использование лутбоксов оказывает значительное влияние на частоту обращений к видеоиграм, проблем в ходе видеоигры и обращений к азартным играм (2022). Повторяющийся характер открытия лутбоксов, вызванный желанием получить редкие или ценные предметы, может создать психологический механизм под названием «петля поиска вознаграждения». Этот механизм усиливает импульсивное поведение и подрывает представление о получении вознаграждения через достижения или развитие навыков.

Кроме того, лутбоксы используют различные подсознательные приемы, чтобы побудить игроков совершить покупку. К ним относятся привлекательные и эстетичные визуальные и звуковые эффекты (яркая анимация, музыка), повышающие воспринимаемую ценность открытия лутбокса независимо от его объективной стоимости. Кроме того, игроков побуждают тратить больше денег, стимулируя чувство срочности через предложения с ограниченным сроком действия, эксклюзивные предметы и внутриигровые события, что вызывает «страх пропустить важное» (fear of missing out, FOMO).

В целом механика лутбоксов сочетает в себе элементы удачи, предвкушения и переменного вознаграждения, что создает психологическое воздействие, которое может быть как привлекательным, так и потенциально вредным для игроков. Это требует тщательного рассмотрения и регулирования в целях защиты потребителей. Понимание механики и психологических последствий использования лутбоксов необходимо для решения соответствующих проблем и разработки адекватных мер регулирования.

2.2. Минимизация вреда

2.2.1. Уязвимые группы населения

Психологическое воздействие лутбоксов особенно сильно сказывается на уязвимых группах населения, более склонных к действиям, связанным с азартными играми. У лиц с предрасположенностью к азартным играм сходство между лутбоксами и традиционными формами азартных игр может вызвать привыкание или привести к проблемному поведению. В крупномасштабном исследовании (Zendle & Cairns, 2019) была выявлена связь между суммой, которую геймеры тратили на лутбоксы, и тяжестью их проблемного поведения. Оказалось, что эта зависимость сильнее, чем связь между проблемными азартными играми и покупкой за реальные деньги предметов, не относящихся к лутбоксам. Это позволяет предположить, что именно сходство лутбоксов с азартными играми обусловливает наблюдаемую связь между тратами на лутбоксы и проблемным поведением азартных игроков.

В исследовании (Drummond et al., 2022) было обнаружено, что у покупателей лутбоксов риск возникновения тяжелых психологических расстройств по результатам стандартного клинического скрининга был примерно в 1,87 раза выше, чем у тех, кто не покупал лутбоксы. Этот эффект наблюдался даже у лиц, не проявлявших симптомов проблемного пристрастия к азартным играм.

2.2.2. Дети и подростки

Механика лутбоксов также в значительной степени ориентирована на несовершеннолетних, которые могут хуже понимать понять последствия трат реальных денег или негативные последствия азартных игр. Анализ, проведенный Zendle et al. (2020b), показывает, что из 50 самых популярных игр на платформе Steam, содержащих лутбоксы, 43 % классифицируются как подходящие для детей в возрасте от 12 лет. Что касается мобильных платформ, то 93 и 94 % из 100 самых кассовых игр, содержащих лутбоксы, в магазинах Google Play и Apple App соответственно, считаются подходящими для детей в возрасте от 12 лет.

Согласно недавнему австралийскому исследованию, до 40 % подростков играли в цифровые игры в течение последних 12 месяцев, в том числе 36,5 % участников приобретали коробки с лутбоксами[17]. Покупка лутбоксов подростками была связана с большей частотой азартных игр и проблем с азартными играми (Rockloff et al., 2021), а также с большим риском развития игровых расстройств (Hing et al., 2023a). В частности, девочки-подростки, которые чаще покупали лутбоксы, выражали более положительное отношение к азартным играм по сравнению с теми, кто их не покупал. Это говорит о том, что интерес к азартным играм у девочек может развиваться одновременно с интересом к лутбоксам.

В исследовании Hing et al. (2023b) было показано, что подростки, использующие симуляторы азартных игр в видеоиграх, впоследствии в жизни используют симуляторы азартных игр чаще и в более разнообразных ситуациях и что они чаще обращаются к деятельности, напоминающей азартные игры на деньги. Как показало исследование, молодые люди, к сожалению, часто не понимают, что симуляции в видеоиграх немногим отличаются от настоящих азартных игр и могут нанести вред, связанный как с игровой, так и с иными видами зависимостей (Hing et al., 2023b).

3. Сравнительный анализ национальных подходов к регулированию

3.1. Бельгия

17 ноября 2017 г. компания Electronic Arts Inc. (EA) выпустила игру Star Wars Battlefront II для Windows, Playstation 4 и Xbox One[18]. Игру много критиковали за то, что в ней использовалась сложная система продвижения, которую можно было обойти, совершая микротранзакции, включая покупку лутбоксов[19]. Вскоре после выхода

[17] Hing, N., Rockloff, M., & Browne, M. Submission to the Inquiry into online gambling and its impacts on those experiencing gambling harm. No 24. Parliament of Australia Standing Committee on Social Policy and Legal Affairs, Inquiry into online gambling and its impacts on those experiencing gambling harm. https://goo.su/lkp6

[18] (2023, 17 July). Star Wars Battlefront II (2017 Video Game). Wikipedia. https://clck.ru/3A9due

[19] Там же.

игры пользователь Reddit MBMMaverick запустил на форуме StarWarsBattlefront тему под названием «Серьезно? Я заплатил 80 долларов [sic] за то, чтобы Вейдера заблокировали?»[20]. Тема набрала более 228 тысяч положительных голосов и около 3 тысяч комментариев, почти все из которых осуждали дизайн игры, якобы заставляющий игроков тратить деньги на продвижение. На это сообщение пришел ответ из отдела EA по работе с сообществом, в котором утверждалось, что трудоемкая система продвижения призвана дать игрокам «чувство гордости и достижения»[21]. Комментарий, разумеется, вызвал волну негативных откликов, быстро став рекордсменом Reddit по этому критерию[22]. Вскоре после этого компания обновила игру, убрав все микротранзакции[23]. Считается, что Battlefront II стала одной из тех игр, которые привлекли широкое внимание к проблеме микротранзакций и лутбоксов[24].

В результате медийной активности вокруг Battlefront II министр юстиции Бельгии Коэн Гинс инициировал расследование законности лутбоксов в соответствии с законодательством страны об азартных играх[25]. Специальная комиссия по азартным играм сочла, что механика лутбоксов не соответствует определению азартных игр по бельгийскому законодательству. Для этого должны быть соблюдены три условия: «элемент удачи; ставка может привести к прибыли или убытку; элемент случайности»[26]. Проанализировав четыре самые известные онлайн-игры 2017–2018 гг. (Overwatch, FIFA, Star Wars Battlefront II и Counter-Strike: Global Offensive), комиссия определила их соответствие бельгийскому законодательству об азартных играх, и поэтому лутбоксы должны регулироваться как азартные игры[27].

Излагая свои выводы, Комиссия сформулировала режим соблюдения следующим образом:

«Система лутбоксов в… видеоиграх может рассматриваться как азартная игра, однако игроки всегда остаются незащищенными. Вызывает беспокойство тот факт, что в играх часто участвуют несовершеннолетние. Скрытый характер азартных игр особенно опасен в случае участия детей. Если не принять надлежащих мер, азартные видеоигры нанесут огромный ущерб гражданам, семьям и обществу в целом…»[28]

«Рассмотренные игры с платными лутбоксами в том виде, в котором они предлагаются в нашей стране в настоящее время, нарушают законодательство об азартных

---

20 MBMMaverick, (2017). Seriously? I paid 80$ [sic] to have Vader locked? Reddit. https://goo.su/zw33

21 Там же.

22 Baculi, S. (2019, September 11). EA's Response to Star Wars Battlefront II Microtransaction Complaint Recognized by Guinness World Records as "Most-Downvoted Comment on Reddit". Bounding into Comics. https://clck.ru/3A9dzX

23 Corden, J. I (2018, November 21). Confirmed: EA has removed all microtransactions from Star Wars Battlefront II (update). Windows Centra. https://clck.ru/3A9e25

24 Kim, M. (2019, August 27). Star Wars Battlefront 2 Loot Box Controversy: 'We Hit Rock Bottom,' EA DICE Says. IGN. https://clck.ru/3C4D37

25 (25 April 2018). Loot boxen in drie videogames in strijd met kansspelwetgeving. Koen Geens. https://clck.ru/3A9e2Z

26 Там же.

27 Там же.

28 Там же.

играх и могут быть предметом рассмотрения в рамках уголовного права. Поэтому лутбоксы должны быть удалены. В противном случае операторам грозят тюремное заключение сроком до пяти лет и штраф в размере до 800 тысяч евро. Если в игре участвуют несовершеннолетние, срок наказания может быть удвоен»[29].

На момент публикации Бельгия является единственной юрисдикцией в Европе, которая однозначно запретила использование лутбоксов.

3.2. Нидерланды

В Нидерландах дебаты о лутбоксах ведутся с 2019 г., когда Управление по азартным играм наложило гражданский штраф в размере 5 млн евро на компанию EA, разработчика серии игр FIFA, за нарушение Закона Нидерландов об азартных играх[30]. В соответствующем пресс-релизе Управление так описало систему лутбоксов в игре FIFA: «…[содержимое лутбокса] определяется случайностью, на которую невозможно повлиять. Тот факт, что [содержимое] иногда имеет высокую стоимость и что его иногда можно продать, нарушает Закон об азартных играх. Согласно голландскому законодательству, азартная игра, позволяющая выиграть приз или вознаграждение, может проводиться только при наличии соответствующей лицензии»[31].

Принятые Управлением меры основывались на проведенном им в 2018 г. исследовании, которое выявило взаимосвязь между играми, содержащими лутбоксы, и игровой зависимостью[32]. В результате была введена политика «строгого разделения между играми и азартными играми».

Компания EA незамедлительно оспорила эти меры в окружном суде Гааги, который 15 октября 2020 г. вынес решение в пользу Управления[33]. По утверждению компании, хотя открытие «пакетов» было случайным, оно является частью более широкой игры на умения, в которой и состоит суть игры FIFA в целом. Кроме того, по словам компании, персонажей нельзя напрямую конвертировать в деньги, как указано в голландском законодательстве об азартных играх. Суд решительно отверг эти аргументы, постановив, что режим, использующий механику лутбокса, можно рассматривать как самостоятельную игру, отличную от остальной части FIFA.

После апелляции Государственный совет Нидерландов отменил решение окружного суда, постановив, что игровой режим, включающий открытие пакетов, не является отдельной игрой[34]. Совет не поддержал мнение суда, поскольку получение персонажей через открытие пакетов было необходимым действием по созданию команды для участия в соревнованиях и, следовательно, являлось неотъемлемой частью игры в целом, а последняя не является азартной игрой в соответствии с голландским законодательством. В своем решении, которое может послужить ориенти-

---

29 Там же.

30 Wet op de kansspelen, Artikel 33f(1).

31 (2020, October 29). Imposition of an order subject to a penalty on Electronic Arts for FIFA video game. Kansspelautoriteit. https://clck.ru/3A9e5i

32 Там же.

33 Electronic Arts Swiss Société à responsabilité limitée en de raad van bestuur van de Kansspelautoriteit (2020) AWB-20_3038.

34 Raad van State, Uitspraak 202005769/1/A3, ECLI:NL:RVS:2022:690.

ром для будущего регулирования лутбоксов по всему миру, Государственный совет Нидерландов определил критерии, соблюдение которых означает, что данная видеоигра не подпадает под действие голландского Закона об азартных играх: а) механизм лутбоксов является одной из частей игры; б) игра основана на умениях; в) игрок получает и открывает лутбоксы внутри игры, а не на отдельной платформе; г) лутбоксы в игре в основном получаются путем самой игры (без необходимости использования реальных денег).

На момент публикации правительство Нидерландов заявило о готовности добиваться запрета лутбоксов в соответствии с законодательством Европейского союза[35].

3.3. Испания

1 июля 2022 г. Министерство по проблемам потребителей Испании объявило, что заинтересовано в регулировании лутбоксов, опубликовав законопроект, предусматривающий строгие меры защиты потребителей в отношении игр, содержащих механизмы получения вознаграждения на основе случайности[36]. В законопроекте предлагается приравнять видеоигры с лутбоксами к азартным играм и ввести такие меры, как проверка личности пользователя на достижение совершеннолетия[37], запрет на рекламу между пятью часами утра и часом ночи[38], публикация коэффициентов вероятности получения каждой потенциальной награды (т. е. показателей отсева)[39], обязательное внедрение системы самоисключения[40], заранее установленные лимиты расходов[41]. За нарушение этих мер предусмотрены штрафы в размере от 200 тысяч до 5 млн евро и возможное закрытие доступа к лутбоксам[42].

Примечательно, что законопроект прямо запрещает лицензированным операторам азартных игр использовать механику лутбоксов при предложении любых услуг или продуктов[43]. Этот запрет распространяется на компании, которые продают традиционные азартные игры в качестве третьих лиц, и не позволяет им делать это в отношении продуктов, связанных с лутбоксами[44]. Если этот законопроект будет принят, то в сочетании с вышеупомянутыми мерами по минимизации вреда от азартных игр он сделает Испанию самой жесткой страной в отношении регулирования продуктов с лутбоксами.

---

35 (2023, June 29). Consumentenagenda minister Adriaansens: aanpak deurverkoop, eenvoudig online opzeggen. Rijksoverheid. https://clck.ru/3A9e8L

36 Ministerio de Consumo. Anteproyecto de Ley por el que se regulan los mecanismos aleatorios de recompensa asociados a productos de software interactivo de ocio. https://clck.ru/3A9e8q

37 Там же. С. 9.

38 Там же. С. 10.

39 Там же. С. 11.

40 Там же. С. 12.

41 Там же.

42 Там же. С. 15.

43 Там же. С. 16.

44 Там же.

3.4. Великобритания

Еще в 2016 г. Комиссия по азартным играм Великобритании выразила свою обеспокоенность потенциальным риском лутбоксов для детей и молодежи, в результате чего был опубликован документ с изложением позиции по виртуальным валютам, киберспорту и игре в казино[45]. Ранее уже принимались меры в отношении сторонних сайтов, принимающих ставки на скины[46]. Однако в этом случае Комиссии пришлось признать свое бессилие, так как предметы в лутбоксах нельзя было обменять непосредственно на реальные деньги[47].

Не желая мириться с этой ситуацией, комитет Палаты общин по цифровым технологиям, культуре, СМИ и спорту[48] и специальный комитет Палаты лордов по социальным и экономическим последствиям игорного бизнеса[49] совместно предложили внести поправки в Закон об азартных играх 2005 г. и включить лутбоксы в сферу регулирования азартных игр[50]. В ответ на этот призыв правительство Великобритании пересмотрело Закон об азартных играх и признало потенциальный вред лутбоксов в видеоиграх, но отказалось включать их в Закон об азартных играх в отсутствие четких научных данных, устанавливающих причинно-следственную связь между тратами на лутбоксы и проблемами, связанными с азартными играми[51]. Было заявлено, что позиция правительства не изменится, пока не будут проведены дополнительные исследования о вреде лутбоксов[52].

Несмотря на отсутствие законодательных действий, правительство Великобритании дало две рекомендации по обращению с лутбоксами: 1) дети и молодежь не должны иметь возможности приобретать лутбоксы без согласия родителей или опекунов, 2) все игроки должны иметь как возможность контролировать свои расходы, так и доступ к прозрачной информации для безопасности игрового процесса[53]. Эти рекомендации в конечном итоге привели к тому, что в июле 2023 г. индустрия перешла к саморегулированию, опубликовав «Отраслевые принципы», призванные усилить защиту игроков[54]. Эти меры включают в себя раскрытие информации о ценах, борьбу с несанкционированными сторонними веб-сайтами, занимающимися продажами, обязательство проводить «благоприятную» политику возврата денег, а также

---

45 Gambling Commission. (2017, March). Virtual currencies, eSports and social casino gaming – position paper. https://clck.ru/3A9eBu

46 Gambling Commission. (2017, February 6). Two men convicted after offering illegal gambling parasitic upon popular FIFA computer game. https://clck.ru/3A9eCc

47 Gambling Commission. (2017, November 24). Loot boxes within video games. https://clck.ru/3A9eDE

48 (2019, 12 September). House of Commons Digital, Culture, Media and Sport Committee. Immersive and addictive technologies. https://clck.ru/3A9eDr

49 House of Lords. Select Committee on the Social and Economic Impact of the Gambling Industry. (2020, July 2). Gambling Harm – Time for Action. https://clck.ru/3A9eEs

50 Gambling Act 2005 (UK).

51 (2022, July 18). Department for Digital, Culture, Media & Sport, Government response to the call for evidence on loot boxes in video games. https://clck.ru/3A9eG4

52 Там же.

53 Там же.

54 UKIE, New Principles and Guidance on Paid Loot Boxes. https://goo.su/me0Y3

обязательство раз в год оценивать эффективность указанных принципов в сотрудничестве с правительством[55].

Поскольку на момент публикации «Принципы» действуют всего несколько недель, еще предстоит выяснить, является ли модель саморегулирования эффективной мерой по снижению вреда от механики лутбоксов.

3.5. Финляндия

Подобный интерес к регулированию возник и в Финляндии. В сентябре 2022 г. член финского парламента Sebastian Tynkkynen представил законопроект о регулировании лутбоксов как разновидности азартных игр[56]. Законопроект предусматривает внесение изменений в определение «лотереи» в соответствии с Законом о лотереях 2001 г., включив в него «виртуально используемые доходы», т. е. предметы, имеющие лишь виртуальную ценность[57]. Согласно этим изменениям, лутбоксы должны считаться разновидностью азартных игр в соответствии с существующими законами об азартных играх, даже в тех случаях, когда полученные внутриигровые предметы нельзя продать вне игры или обменять на реальные деньги. Это отличает Финляндию от других стран ЕС, так как в остальных юрисдикциях разработчики имеют возможность реализовать обмен лутбоксов на реальные деньги. Кроме того, благодаря широте применения финских норм в этой сфере их будет сложнее обойти.

3.6. Китай

Сфера регулирования видеоигр в Китае отличается сложностью. Опасения, связанные с зависимостью, привели к запрету консолей в Китае в 2000-х гг. и вылились в ряд дополнительных нормативных требований. В частности, в играх нельзя изображать непристойности, обнаженное тело, «пугающие» сцены или образы, прославлять войну и преступность, очернять культурные традиции, пропагандировать употребление наркотиков и их незаконный оборот[58]. За соблюдением этих требований следит Государственное управление по делам изданий, прессы, радио, кино и телевидения Китая (China's State Administration of Publication, Press, Radio, Film and Television, SAPPRFT).

Вскоре после отмены запрета на использование видеоигровых консолей Китай начал регулировать использование лутбоксов, ссылаясь на те же опасения по поводу Star Wars Battlefront II , что и бельгийское правительство. 1 мая 2017 г. Министерство культуры Китая ввело жесткие ограничения на использование лутбоксов, запретив покупать их за реальные деньги (а также за виртуальные деньги, купленные за реальные деньги), а также обязав разработчиков раскрывать информацию о показателях отсева и о расходах игроков за последние 90 дней[59].

---

55 Там же.

56 LA 42 /2022 vp, Bill to amend Section 2 of the Lotteries Act 2001.

57 Heilbuth, H. (2022, December 15). Exploring Finland's proposed loot box regulation. GamesIndustry.Biz. https://clck.ru/3A9eQv

58 Kuhns, T. (2016, May 24). Mobile Game Content Standard (2016 Edition). AppInChina. https://clck.ru/3A9eRa

59 Tang, T. (2018, May 16). A Middle-Ground Approach: How China Regulates Loot Boxes And Gambling Features In Online Games. Mondaq. https://clck.ru/3A9eYS

Поскольку традиционные азартные игры в Китае запрещены законом, на механизмы лутбоксов накладываются дополнительные ограничения, призванные не допустить, чтобы использование лутбоксов стало азартной игрой. Управление SAPPRFT как орган, отвечающий за содержание и утверждение игр, запрещает выпуск игр, содержащих «петлю принуждения» (механизм, подталкивающий игрока к использованию лутбоксов) и других систем, сближающих их с азартными играми[60]. К примеру, если определенный предмет можно получить только путем открытия лутбоксов, SAPPRFT, скорее всего, не разрешит выпустить игру. Таким образом, некоторые элементы игры, связанные с лутбоксами, могут препятствовать ее выпуску в Китае.

3.7. Япония

Япония стала первой страной, где регулируется механика лутбоксов. Здесь уже давно существуют игры модели «гача» – это бесплатные игры, обычно на базе мобильного телефона, которые побуждают игроков тратить деньги (как внутриигровые, так и реальные) на приобретение определенных предметов или персонажей для развития сюжетной линии[61]. 18 мая 2012 г. Министерство по делам потребителей Японии объявило незаконными игры модели «полная гача» – это разновидность модели «гача», в которой для продвижения необходимо собрать полный набор предметов[62]. Министерство объясняет это решение «чрезвычайно высокими суммами, собираемыми с игроков», и жалобами, получаемыми в связи с этим[63].

Примечательно, что на момент публикации данного запрета несколько крупнейших разработчиков таких игр уже прекратили использовать эту механику[64]. Разработчики называют разные причины такого решения, в том числе низкие показатели продаж[65], стремление к саморегулированию отрасли[66], а также желание минимизировать убытки от этого запрета[67].

3.8. Республика Корея

Как и Китай, Южная Корея имеет богатую историю регулирования видеоигр. В 2011 г. на весь мир прогремел Закон о защите молодежи, прозванный Законом об отключении, по которому детям до шестнадцати лет было запрещено играть в онлайн-видеоигры с полуночи до шести утра (Sang et al., 2017). Этот комендантский час был

60 Там же.

61 (2023, August 20). Gacha. Wiktionary. https://clck.ru/3A9ixg

62 Gantayat, A. (2012, May 18). Complete Gacha Officially Deemed Illegal. Andriasang. https://clck.ru/3A9eZZ

63 (2012, May 6). 'Kompu gacha' online games may be illegal. The Yomiuri Shinbun. https://goo.su/Z2k9Q

64 Gantayat, A. (2012, May 18). Complete Gacha Officially Deemed Illegal. Andriasang. https://clck.ru/3A9ebn

65 Gantayat, A. (2012, May 10). DeNA and GREE Stock Values Plummet Following Reports of Government Regulation. Andriasang. https://clck.ru/3A9edQ

66 Gantayat, A. (2012, May 9). Social Game Maker KLab Puts Halt to Complete Gacha Sales. Andriasang. https://clck.ru/3A9eeT

67 Gantayat, A. (2012, May 8). Analysts Expect Major Social Game Losses if Sales Tactics is Banned. Andriasang. https://clck.ru/3A9efC

ужесточен в 2012 г. с введением дополнительного законодательства, обязавшего крупных производителей внедрить систему выбора периода доступности игр – фактически это техническая возможность родителям установить комендантский час[68]. На сегодняшний день только Китай и Вьетнам имеют подобные ограничения[69].

К началу 2021 г. Закон об отключении был пересмотрен в связи с серьезными логистическими проблемами, связанными с обеспечением его соблюдения[70]. В то же время в стране все чаще звучат призывы регулировать онлайн-игры в отношении мошенничества с использованием лутбоксов[71]. Толчком послужили споры вокруг использования лутбоксов в популярной корейской MMORPG-игре MapleStory[72]. Обычно в лутбоксе находится случайный внутриигровой предмет, но в MapleStory игроки могли получить три случайно выбранные «способности». Разработчик игры, компания Nexon, призналась, что при этом невозможно «сорвать джекпот» (т. е. получить три очень мощные способности); механика была разработана так, чтобы предотвратить одновременное появление самых мощных способностей[73]. После расследования, проведенного Комиссией по справедливой торговле Кореи, компания Nexon вернула деньги от покупок лутбоксов за предыдущие два года – период, в течение которого эти покупки регистрировались[74].

На следующий день после того, как Nexon согласилась вернуть средства, Корейская ассоциация игровой индустрии объявила о введении нового свода правил; в них содержалось требование раскрывать информацию о случайных событиях, приводящих к улучшению способностей персонажа, его навыков или модернизации оборудования, а не только о приобретении предметов[75]. Не удовлетворившись такими мерами саморегулирования в отрасли, Национальное собрание Южной Кореи 27 февраля 2023 г. почти единогласно приняло поправку к Закону о развитии игровой индустрии, обязывающую раскрывать информацию о вероятности появления лутбоксов в самой игре, на официальном сайте игры и в рекламных объявлениях[76]. Непредоставление такой информации или предоставление ложных сведений теперь наказывается штрафом в размере до 20 млн вон (15 000 долларов США) или тюремным заключением на срок до двух лет[77].

---

68 Tassi, P. (2012, July 2). New Korean Law Lets Parents Decide When Their Kids Can Play Games. Forbes. https://clck.ru/3A9ejW

69 (2023, August 9). Shutdown Law. Wikipedia. https://clck.ru/3A9ek3

70 (2021, November 16). Shutdown law shuttered. Korea Herald. https://clck.ru/3A9eke

71 K. Byung-wook. (2021, March 9). Game firms under increasing scrutiny over loot box odds. Korea Herald. https://clck.ru/3A9s2F

72 Там же.

73 Там же.

74 Maple Story. (2021, May 28). (Compensation payment completed) We apologize for not meeting the customer's expectations in the process of disclosing the cube probability. https://clck.ru/3A9emF

75 Min-Je, P. (2021, May 29). Game association introduces own loot box disclosure rules. Korea JoongAng Daily. https://clck.ru/3A9emd

76 Mi-hee, K. (2023, February 27). Stochastic Item Information Disclosure Act, passed the plenary session of the National Assembly. GameMeca. https://clck.ru/3A9eqz

77 Obedkov, E. South Korea passes new amendment on loot box probability disclosure. Game World Observer. https://clck.ru/3A9eru

3.9. Германия

В марте 2021 г. парламент Германии принял поправки к Закону о защите молодежи, направленные на усиление защиты детей и молодежи в отношении медиаконтента[78]. В частности, были обновлены национальные стандарты классификации видеоигр; теперь они позволяют учитывать «риски взаимодействия», включая, в частности, наличие лутбоксов и других внутриигровых покупок[79].

Совет по саморегулированию развлекательного программного обеспечения (Unterhaltungssoftware Selbstkontrolle, USK), отвечающий за возрастную классификацию, ратифицировал закон и ввел соответствующие правила с 1 января 2023 г.[80] При этом Совет обратил внимание на то, что в классификацию новых цифровых игр могут быть включены «потенциальные онлайн-риски, например, в ходе покупки или общения»[81]. Согласно новым правилам, игре будет присваиваться более высокий возрастной рейтинг, если она может «повредить развитию детей и подростков или их воспитанию как самостоятельных и социально компетентных личностей»[82]. Далее Совет указал: «Участие несовершеннолетних в азартных играх строго запрещено, поскольку является частью признанной медициной клинической картины игровой зависимости с серьезными психосоциальными последствиями и значительными финансовыми рисками для пострадавших… Если на цифровые игры не распространяется законодательный запрет на азартные игры, то возрастная классификация цифровых игр должна учитывать… что [они] могут нарушить или поставить под угрозу развитие личности детей и подростков в аспекте их отношения к азартным играм. В частности, речь идет об игровом контенте, который может привести к привыканию или злоупотреблению азартными играми путем поощрения позитивного отношения к ним, способствуя десенсибилизации к проигрышам или вызывая нереалистичные ожидания прибыли»[83].

3.10. Канада

В сентябре 2020 г. двое мужчин подали коллективный иск в Верховный суд Британской Колумбии против компании EA[84]. В иске утверждается, что использование компанией лутбоксов в играх нарушает законы Британской Колумбии о защите прав потребителей[85], как и положения против азартных игр федерального Уголов-

---

78 Puppe, M. (2021, March 10). German Bundestag passes new Youth Protection Act. The German Games Industry Association. https://clck.ru/3A9iuW

79 Там же.

80 (2022, December 14). In-game purchases, chats and loot boxes: USK expands test criteria. Unterhaltungssoftware Selbstkontrolle. https://clck.ru/3A9is6

81 Там же.

82 (2022, December). Unterhaltungssoftware Selbstkontrolle, Guiding criteria of the USK for the evaluation of youth protection law digital games, 8 (translated from German to English). https://clck.ru/3A9isY

83 Там же. С. 23.

84 Sutherland v Electronic Arts Inc. (2020, September 30). Vancouver S-209803 (BCSC) (Plaintiff's Notice of Civil Claim). https://clck.ru/3A9evu

85 Business Practices and Consumer Protection Act [SBC 2004].

ного кодекса[86]. В марте 2023 г. судья Флеминг вынес решение о возможности рассмотрения иска о защите прав потребителей, но не иска о нарушении Уголовного кодекса. Судья отметил, что награды в виде лутбоксов в играх компании EA можно обменять только на внутриигровом рынке и что в отсутствие «возможности получить или потерять что-либо, имеющее реальную ценность», иск не имеет шансов на успех[87]. В деле Sutherland были поданы коллективные иски против десятков компаний, производящих видеоигры в Британской Колумбии и Квебеке[88]. Соответственно, судебные, нормативные и социальные последствия этих действий еще предстоит выяснить.

3.11. Австралия

28 ноября 2022 г. член австралийского парламента Andrew Wilkie представил частный законопроект о внесении изменений в Закон о классификации публикаций, фильмов и компьютерных игр 1995 г.[89] Законопроект обязывает Австралийский совет по классификации маркировать компьютерные игры, содержащие лутбоксы, как R18+ или RC (последнее запрещает продажу, аренду, рекламу или ввоз продукта в Австралию), а также помещать предупреждение о том, что игры содержат лутбоксы или подобные режимы, аналогично новым стандартам классификации в Германии[90]. По состоянию на 1 августа 2023 г. законопроект исключен из парламентской повестки, так как не был рассмотрен в течение времени, предусмотренного правилами[91].

4. Проблемы внедрения регулирования

4.1. Оспаривание статус-кво

Лутбоксы в их нынешнем виде часто рассматривают как разновидность традиционных азартных игр[92]. Однако в большинстве юрисдикций такой подход все еще встречает противодействие. Для этого приводят различные обоснования, общим для которых является нежелание считать что-либо азартной игрой только потому, что на первый взгляд оно не похоже на традиционную азартную игру, несмотря на то, что общепринятое определение азартной игры соблюдается.

---

86 Criminal Code, RSC 1985, c C-46, Part VII.

87 Dring, Ch. (2023, March 21). Canada Judge rejects unlawful gambling accusation in EA loot box lawsuit. GamesIndustry.Biz. https://clck.ru/3A9exW

88 Loot Boxes Class Action Lawsuits – Canada. Slater Vecchio LLP. https://clck.ru/3A9eyM

89 Classification (Publications, Films and Computer Games) Act 1995 (Cth).

90 Classification (Publications, Films and Computer Games) Amendment (Loot Boxes) Bill 2022. Parliament of Australia. https://goo.su/NkJWUmp

91 Там же.

92 Moar, J., & Hunt, N. (2021, March 9). 'Video Game Loot Boxes to Generate Over $20 Billion in Revenue by 2025. Juniper Research. https://clck.ru/3A8Xn6

Например, регулирующие органы Австралии отказались регулировать лутбоксы в соответствии с существующими законами об азартных играх на том основании, что получаемые награды не состоят из реальных денег и не существует средств или методов, позволяющих напрямую конвертировать полученные награды в реальные деньги[93]. На заре появления лутбоксов такая трактовка могла быть верной, но она не учитывает стоимость продажи внутриигровых предметов в игровой экосистеме, а также растущую распространенность сайтов для покупки/обмена/продажи и ставок с использованием лутбоксов, т. е. игры на «скины» (Greer et al., 2023). Большинство из этих сторонних сайтов открыто рекламируют себя как «азартные игры» или «слоты», предлагая стимулы, практически идентичные тем, что используются традиционными сайтами для онлайн-ставок (Deans et al., 2017)

По оценкам компании Eilers & Krejcik, в 2015 г. около 3 млн человек поставили на исход киберспортивных игр скины на сумму 2,3 млрд долларов[94], а в 2016 г. было разыграно скинов на сумму 5 млрд долларов, причем около 60 % этой суммы – на «игровых сайтах типа казино»[95]. Эти сайты, как правило, ориентированы на несовершеннолетних и часто сотрудничают с известными производителями видеоигр и медийными персонажами для продвижения среди своей аудитории[96]. Сайты, занимающиеся игрой на скины, также спонсируют или контролируют собственные киберспортивные команды, что вызывает опасения относительно рекламы для зрителей-подростков и вероятности договорных матчей[97].

Более того, как утверждают Hing et al., требование регуляторов о «реальных деньгах» не соответствует цели, поскольку причиняемый вред может возникнуть независимо от того, можно ли обменять вознаграждение на реальные деньги или нет (Hing et al., 2023a). Психологическая привлекательность механики лутбоксов не требует, чтобы вознаграждение было финансовым; оно может просто представлять собой что-то, имеющее воспринимаемую ценность, например, внутриигровое оружие высокой прочности, предмет для украшения (например, скин) или любой другой социально одобряемый показатель успеха. Этот аргумент подтверждается результатами исследования 2023 г., в котором подростки, игравшие в симуляторы азартных игр, высоко оценивали не только виртуальные призы, но и социальные преимущества, возможность узнать новые азартные игры, посоревноваться с другими игроками и продемонстрировать мастерство (Hing et al., 2023b).

---

93 Nettleton, J. & Chong, K. (2013, October 16). Online social games – the Australian position. https://goo.su/tuWnN

94 Brustein, J. & Novy-Williams, E. (2016, April 20). Virtual Weapons are Turning Teen Gamers into Serious Gamblers. Bloomberg. https://goo.su/lnjzto

95 Assael, Sh. (2017, January 20). Skin in the Game. ESPN. https://goo.su/dMvYMsR

96 Sacco, D. (2016, July 4). Syndicate apologises after failing to disclose ownership of CSGO Lotto gambling site. Esports News UK. https://goo.su/fGi5t

97 Wynne, J. (2015, September 15). Popular betting website to sponsor pro Counter-Strike team. Dot eSports. https://clck.ru/3A9fJp

4.2. Прозрачность отрасли и понимание ее особенностей

Аналитики James Moar и Nick Hunt в своем отчете Juniper Research за 2021 г. заявили: «Мы ожидаем, что в будущем производители игр отреагируют [на усиление мер регулирования против лутбоксов] изменением форматов лутбоксов, чтобы они оставались привлекательными, но не попадали в правовую сферу азартных игр»[98]. В какой-то степени эти ожидания оправдались. Например, в Китае компания Blizzard, один из крупнейших разработчиков видеоигр в мире, обошла национальный запрет на продажу лутбоксов; в их игре внутриигровая валюта продается за реальные деньги, а игроки одновременно получают «бесплатные» лутбоксы[99]. На момент публикации статьи никаких мер в связи с этим явным обходом закона принято не было.

Отсутствие прозрачности усугубляется нежеланием разработчиков предоставлять для изучения данные, связанные с лутбоксами. В работе Etchells et al. (2022) отмечается необходимость дальнейших исследований взаимосвязи между расходами на лутбоксы и благосостоянием игроков, но при этом подчеркивается, что для этого исследователи должны получить доступ к соответствующим данным. Заявления ученых о превращении видеоигр в азартные служат основанием для того, чтобы отрасль продемонстрировала добрую волю, сотрудничая с исследователями, медицинскими работниками, общественными деятелями и другими заинтересованными сторонами для исправления ситуации в этой сфере (Greer et al., 2023). И наоборот, участники отрасли не хотят участвовать в консультациях, так как это может привести к усилению регулирования, а значит, к снижению прибыли. Однако в этой сфере наблюдаются и положительные сдвиги: недавно компания Valve, одна из крупнейших в мире, ввела запрет на участие пользователей в конкурсах, азартных играх и продаже предметов[100].

4.3. Возможность принудительного исполнения

В связи с тем, что деятельность по регулированию лутбоксов в разных странах мира ведется не так давно, оценить ее эффективность довольно сложно. Что касается Бельгии, которая одной из первых ввела ограничения на лутбоксы, то обнаруживается, что запрет на лутбоксы соблюдается слабо. В работе Xiao показано, что 82 % из 100 самых кассовых игр для iPhone в бельгийском App Store продолжают использовать тот или иной метод рандомизированной монетизации, в том числе 80,2 % игр для возраста от 12 лет (Xiao, 2023). И это несмотря на то, что некоторые известные разработчики полностью убрали механику случайности из игр, продаваемых в Бельгии[101], а Комиссия по азартным играм Бельгии угрожает привлечь к уголовной

[98] Moar, J., & Hunt, N. (2021, March 9). 'Video Game Loot Boxes to Generate Over $20 Billion in Revenue by 2025. Juniper Research. https://clck.ru/3A8Xn6

[99] Handrahan, M. (2017, June 6). Blizzard avoids China's loot laws by selling Overwatch in-game currency. GamesIndustry.biz. https://clck.ru/3A9fPN

[100] Biazzi, L. (2023, May 11). Valve launches offensive against gamblers on Steam, possibly affecting CS:GO's skin market. Dot Esports. https://clck.ru/3A9fPz

[101] Statement Belgium. 2k Games. https://clck.ru/3A9fQn

ответственности компании, занимающиеся видеоиграми и использующие лутбоксы без соответствующей лицензии[102].

В той же работе Xiao показывает, что использование виртуальных частных сетей (VPN) позволяет игрокам получить доступ к лутбоксам, которые были удалены из бельгийской версии мобильной игры. В ходе исследования эффективности запрета на доступ несовершеннолетних к порнографии в Великобритании Thurman и Obster обнаружили, что 46 % подростков 16 и 17 лет использовали VPN или частный браузер для доступа к порнографическим сайтам, которые в противном случае потребовали бы проверки на соответствие возрасту (Thurman & Obster, 2021)[103]. В исследовании, проведенном VPN-провайдером ExpressVPN, 24 % респондентов признались, что лгали о своем возрасте, чтобы пользоваться социальными сетями (в которых минимальный возраст, как правило, составляет 13 лет)[104], а 16 % также заявили, что солгали о своем адресе или местонахождении[105]. Таким образом, с точки зрения нормативно-правового регулирования для обеспечения соблюдения положений о лутбоксах необходимо сосредоточить внимание на действиях как разработчика, так и потребителя.

Заключение

В работе проведено комплексное исследование необходимости правового регулирования лутбоксов в видеоиграх. Анализ комментариев к мерам регулирования, принятым в различных юрисдикциях, позволил создать основу для понимания потенциального негативного воздействия лутбоксов на потребителей, особенно на детей и молодежь. Высказанные в данной работе опасения подтверждают тезис о необходимости ужесточить государственное регулирование в целях защиты потребителей, обеспечения прозрачности и подотчетности отрасли, а также этичного и ответственного использования механики лутбоксов. Применяя эффективные меры регулирования, можно найти баланс между инновациями в игровой индустрии, защитой потребителей и благополучием пользователей, что в конечном итоге будет способствовать созданию более здоровой среды для геймеров.

В статье анализируются различные подходы к действующему или предлагаемому регулированию механики лутбоксов в видеоиграх. Некоторые из них направлены на оценку того, подпадают ли лутбоксы под определение азартных игр в соответствии с действующим законодательством в соответствующей юрисдикции. В Бельгии и Нидерландах регулирующие органы дали положительный ответ на этот вопрос, хотя в случае Нидерландов суд опроверг это решение. Для сравнения, пример Австралии демонстрирует, что понимание предмета регулирования или

[102] Belgian Gaming Commission. (2018, April). Research report loot boxes., 18 (Translated from Dutch to English). https://goo.su/qsuW

[103] Thurman, N. & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. Policy Internet, 13(3), 415.

[104] (2023, January 19). Dangers of social media for kids and how to protect them. ExpressVPN. https://goo.su/Ks8N1JT

[105] Там же.

отсутствие такого понимания может оказать решающее влияние на политическую волю к регулированию.

Другие юрисдикции применяют просветительский подход к регулированию. Например, в Германии потребители (а в случае с несовершеннолетними – их опекуны) стали получать больше информации о наличии лутбоксов в продуктах. Наиболее детальным является подход Китая и Кореи, где игроку должны быть показаны коэффициенты вероятности всех лутбоксов, включая те, которые дают вознаграждение не в виде предметов. Если такой облегченный подход окажется эффективным способом снижения вреда, то его могут принять и другие юрисдикции, избежав необходимости введения ограничений или запрета на лутбоксы.

Следует еще раз подчеркнуть, что большинство регулятивных мер, проанализированных в данной статье, еще предстоит проверить на предмет их эффективности. Поэтому одним из направлений будущих исследований может стать оценка этих мер не только с точки зрения их влияния на использование лутбоксов, но и с точки зрения их воздействия на благополучие игроков, их психическое здоровье и финансовое благосостояние. Автор еще раз подчеркивает, что для проведения такой оценки необходимо, чтобы разработчики и другие заинтересованные стороны в отрасли предоставляли независимым исследователям данные о покупках и использовании лутбоксов.

Еще один аспект регулирования лутбоксов, который упоминался в данной работе, но не стал предметом основного исследования, – это правовой статус сайтов, предлагающих игру на скины. Анализ взаимосвязи между использованием лутбоксов и игрой на скины позволил бы установить роль критерия «возможность обмена на реальные деньги», который требуют некоторые юрисдикции для рассмотрения лутбоксов в соответствии с действующим законодательством об азартных играх. Кроме того, следует изучить совместное воздействие использования лутбоксов и игры на скины. Теоретически их совместное использование может оказывать более сильное психологическое или финансовое воздействие на потребителей.

Список литературы

Brenner, R., & Brenner, G. A. (1990). *Gambling and speculation: A theory, a history, and a future of some human decisions*. Cambridge University Press.

Deans, E. G., Thomas, S. L., Derevensky, J., & Daube, M. (2017). The influence of marketing on the sports betting attitudes and consumption behaviours of young men: implications for harm reduction and prevention strategies. *Harm Reduction Journal*, *14*, 1–12. https://doi.org/10.1186/s12954-017-0131-8

Devereux, E. (1979). Gambling. In *The International Encyclopedia of the Social Sciences* (vol. 17). New York: Macmillan.

Drummond, A., & Sauer, J. D. (2018). Video game loot boxes are psychologically akin to gambling. *Nature human behaviour*, *2*(8), 530–532. https://doi.org/10.1038/s41562-018-0360-1

Drummond, A., Hall, L. C., & Sauer, J. D. (2022). Surprisingly high prevalence rates of severe psychological distress among consumers who purchase loot boxes in video games. *Scientific Reports*, *12*(1), 16128. https://doi.org/10.1038/s41598-022-20549-1

Etchells, P. J., Morgan, A. L., & Quintana, D. S. (2022). Loot box spending is associated with problem gambling but not mental wellbeing. *Royal Society Open Science*, *9*(8), 220111. https://doi.org/10.1098/rsos.220111

Gong, L., & Rodda, S. N. (2022). An exploratory study of individual and parental techniques for limiting loot box consumption. *International Journal of Mental Health and Addiction*, *20*, 398–425. https://doi.org/10.1007/s11469-020-00370-5

Greer, N., Rockloff, M., Hing, N., Browne, M., & King, D. L. (2023). Skin gambling contributes to gambling problems and harm after controlling for other forms of traditional gambling. *Journal of Gambling Studies*, *39*, 225–247. https://doi.org/10.1007/s10899-022-10111-z

Griffiths, M. D. (1995). *Adolescent gambling*. London: Routledge.

Hing, N., Lole, L., Thorne, H., Sproston, K., Hodge, N., & Rockloff, M. (2023b). 'It Doesn't Give Off the Gambling Vibes… It Just Feels Like a Part of the Game': Adolescents' Experiences and Perceptions of Simulated Gambling While Growing Up. *International Journal of Mental Health and Addiction*. https://doi.org/10.1007/s11469-023-01119-6

Hing, N., Russell, A. M., King, D. L., Rockloff, M., Browne, M., Newall, P., & Greer, N. (2023a). Not all games are created equal: Adolescents who play and spend money on simulated gambling games show greater risk for gaming disorder. *Addictive Behaviors*, *137*, 107525. https://doi.org/10.1016/j.addbeh.2022.107525

King, D. L., & Delfabbro, P. H. (2018). Predatory monetization schemes in video games (eg 'loot boxes') and internet gaming disorder. *Addiction*, *113*(11), 1967–1969. https://doi.org/10.1111/add.14286

Liao, S. X. (2016). Japanese console games popularization in China: Governance, copycats, and gamers. *Games and Culture*, *11*(3), 275–297. https://doi.org/10.1177/1555412015583574

Primi, C., Sanson, F., Vecchiato, M., Serra, E., & Donati, M. A. (2022). Loot boxes use, video gaming, and gambling in adolescents: Results from a path analysis before and during COVID-19-pandemic-related lockdown in Italy. *Frontiers in psychology*, *13*, 1009129. https://doi.org/10.3389/fpsyg.2022.1009129

Rockloff, M., Russell, A. M., Greer, N., Lole, L., Hing, N., & Browne, M. (2021). Young people who purchase loot boxes are more likely to have gambling problems: An online survey of adolescents and young adults living in NSW Australia. *Journal of Behavioral Addictions*, *10*(1), 35–41. https://doi.org/10.1556/2006.2021.00007

Sang, Y., Park, S., & Seo, H. (2017). Mobile Game Regulation in South Korea: A Case Study of the Shutdown Law. In D. Jin (Eds.). Mobile Gaming in Asia. *Mobile Communication in Asia: Local Insights, Global Implications* (pp. 55–72). Springer, Dordrecht. https://doi.org/10.1007/978-94-024-0826-3_4

So, Sh., & Westland, J. Ch. (2012). Red Wired: China's Internet Revolution. Marshall Cavendish.

Staddon, J. E. R, & Cerutti, D. T. (2003). Operant conditioning. *Annual Review of Psychology*, *54*, 115–144. https://doi.org/10.1146/annurev.psych.54.101601.145124

Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, *13*(3), 415–432. https://doi.org/10.1002/poi3.250

Xiao, L. Y. (2023). Breaking Ban: Belgium's ineffective gambling law regulation of video game loot boxes. *Collabra: Psychology*, *9*(1), 57641. https://doi.org/10.1525/collabra.57641

Zendle, D., & Cairns, P. (2019). Video game loot boxes are again linked to problem gambling: Results of a large-scale survey. *PLoS ONE*, *14*(3), e0214167. https://doi.org/10.1371/journal.pone.0214167

Zendle, D., Meyer, R., & Ballou, N. (2020b). The changing face of desktop video game monetisation: An exploration of exposure to loot boxes, pay to win, and cosmetic microtransactions in the most-played Steam games of 2010–2019. *PloS ONE*, *15*(5), e0232780. https://doi.org/10.1371/journal.pone.0232780

Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020a). The prevalence of loot boxes in mobile and desktop games. *Addiction*, *115*(9), 1768–1772. https://doi.org/10.1111/add.14973

Zuriff, G. E. (1970). A comparison of variable-ratio and variable-interval schedules of reinforcement. *Journal of the Experimental Analysis of Behavior*, *13*(3), 369–374. https://doi.org/10.1901/jeab.1970.13-369

Сведения об авторе

Пор Сэппи – бакалавр права (по углубленной программе), бакалавр искусств, магистр права, главный консультант, группа компаний «Кун Консалтинг»
Адрес: Австралия NSW 2006, г. Сидней
E-mail: seppypour@gmail.com
ORCID ID: https://orcid.org/0000-0001-9032-062X

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 – 25 августа 2023 г.
Дата одобрения после рецензирования – 20 сентября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:347.21:004.4
EDN: https://elibrary.ru/uxqado
DOI: https://doi.org/10.21202/jdtl.2024.18

Experience of Legal Regulation of Lootboxes in Different Countries: a Comparative Analysis

Seppy Pour
Kun Consulting Group, Sydney, Australia

Keywords

comparative legal studies,
consumer protection,
digital technologies,
gambling,
gaming industry,
law,
licensing,
Loot box,
video games,
virtual goods

Abstract

Objective: to show how the use of a new business model called Loot boxes, on which modern video games are based, has become a legal problem for jurisdictions in different countries.

Methods: drawing on existing literature and contemporary sources, the article explores the potential negative consequences of Loot boxes, provides a comprehensive analysis of existing or proposed regulation, and compares the approaches taken in various national jurisdictions.

Results: the article examines the growing concern surrounding the widespread use of a particular form of in-game purchases called Loot boxes. It is strongly criticized on the grounds that Loot boxes are presumed to be a form of gambling within a video game. On this basis, this article argues in favor of their legislative regulation. Having examined the regulatory framework in countries that have already taken action against the use of Loot boxes, such as Belgium, the Netherlands, China, Japan and the Republic of Korea, as well as in countries currently debating their regulation, the author emphasizes the need to adopt consumer protection measures in the gaming industry. This is particularly relevant for vulnerable strata exposed to gambling-related harms. In addition, there is a need to ensure the ethical and responsible use of Loot boxes, as well as to reduce the health and financial risks associated with the use of this business model.

Scientific novelty: the paper presents a comparative study of the problems of current or projected social regulation of Loot boxes in video games. The author proposes to seek the solution in a balance between game industry innovations, consumer protection and user well-being, which will ultimately contribute to the creation of a healthier environment for gamers.

Practical significance: the study highlights the international scope of the problem the difference in legal and ethical regulatory measures taken in different countries to address the psychological, social and financial consequences associated with the proliferation of lootboxes in video games. These measures are yet to be assessed, taking into account the findings concerning the gaming industry.

For citation

Pour, S. (2024). Experience of Legal Regulation of Lootboxes in Different Countries: a Comparative Analysis. *Journal of Digital Technologies and Law*, *2*(2), 345–371. https://doi.org/10.21202/jdtl.2024.18

References

Brenner, R., & Brenner, G. A. (1990). *Gambling and speculation: A theory, a history, and a future of some human decisions*. Cambridge University Press.

Deans, E. G., Thomas, S. L., Derevensky, J., & Daube, M. (2017). The influence of marketing on the sports betting attitudes and consumption behaviours of young men: implications for harm reduction and prevention strategies. *Harm Reduction Journal*, *14*, 1–12. https://doi.org/10.1186/s12954-017-0131-8

Devereux, E. (1979). Gambling. In *The International Encyclopedia of the Social Sciences* (vol. 17). New York: Macmillan.

Drummond, A., & Sauer, J. D. (2018). Video game loot boxes are psychologically akin to gambling. *Nature human behaviour*, *2*(8), 530–532. https://doi.org/10.1038/s41562-018-0360-1

Drummond, A., Hall, L. C., & Sauer, J. D. (2022). Surprisingly high prevalence rates of severe psychological distress among consumers who purchase loot boxes in video games. *Scientific Reports*, *12*(1), 16128. https://doi.org/10.1038/s41598-022-20549-1

Etchells, P. J., Morgan, A. L., & Quintana, D. S. (2022). Loot box spending is associated with problem gambling but not mental wellbeing. *Royal Society Open Science*, *9*(8), 220111. https://doi.org/10.1098/rsos.220111

Gong, L., & Rodda, S. N. (2022). An exploratory study of individual and parental techniques for limiting loot box consumption. *International Journal of Mental Health and Addiction*, *20*, 398–425. https://doi.org/10.1007/s11469-020-00370-5

Greer, N., Rockloff, M., Hing, N., Browne, M., & King, D. L. (2023). Skin gambling contributes to gambling problems and harm after controlling for other forms of traditional gambling. *Journal of Gambling Studies*, *39*, 225–247. https://doi.org/10.1007/s10899-022-10111-z

Griffiths, M. D. (1995). *Adolescent gambling*. London: Routledge.

Hing, N., Lole, L., Thorne, H., Sproston, K., Hodge, N., & Rockloff, M. (2023b). 'It Doesn't Give Off the Gambling Vibes… It Just Feels Like a Part of the Game': Adolescents' Experiences and Perceptions of Simulated Gambling While Growing Up. *International Journal of Mental Health and Addiction*. https://doi.org/10.1007/s11469-023-01119-6

Hing, N., Russell, A. M., King, D. L., Rockloff, M., Browne, M., Newall, P., & Greer, N. (2023a). Not all games are created equal: Adolescents who play and spend money on simulated gambling games show greater risk for gaming disorder. *Addictive Behaviors*, *137*, 107525. https://doi.org/10.1016/j.addbeh.2022.107525

King, D. L., & Delfabbro, P. H. (2018). Predatory monetization schemes in video games (eg 'loot boxes') and internet gaming disorder. *Addiction*, *113*(11), 1967–1969. https://doi.org/10.1111/add.14286

Liao, S. X. (2016). Japanese console games popularization in China: Governance, copycats, and gamers. *Games and Culture*, *11*(3), 275–297. https://doi.org/10.1177/1555412015583574

Primi, C., Sanson, F., Vecchiato, M., Serra, E., & Donati, M. A. (2022). Loot boxes use, video gaming, and gambling in adolescents: Results from a path analysis before and during COVID-19-pandemic-related lockdown in Italy. *Frontiers in psychology*, *13*, 1009129. https://doi.org/10.3389/fpsyg.2022.1009129

Rockloff, M., Russell, A. M., Greer, N., Lole, L., Hing, N., & Browne, M. (2021). Young people who purchase loot boxes are more likely to have gambling problems: An online survey of adolescents and young adults living in NSW Australia. *Journal of Behavioral Addictions*, *10*(1), 35–41. https://doi.org/10.1556/2006.2021.00007

Sang, Y., Park, S., & Seo, H. (2017). Mobile Game Regulation in South Korea: A Case Study of the Shutdown Law. In D. Jin (Eds.). Mobile Gaming in Asia. *Mobile Communication in Asia: Local Insights, Global Implications* (pp. 55–72). Springer, Dordrecht. https://doi.org/10.1007/978-94-024-0826-3_4

So, Sh., & Westland, J. Ch. (2012). Red Wired: China's Internet Revolution. Marshall Cavendish.

Staddon, J. E. R, & Cerutti, D. T. (2003). Operant conditioning. *Annual Review of Psychology*, *54*, 115–144. https://doi.org/10.1146/annurev.psych.54.101601.145124

Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, *13*(3), 415–432. https://doi.org/10.1002/poi3.250

Xiao, L. Y. (2023). Breaking Ban: Belgium's ineffective gambling law regulation of video game loot boxes. *Collabra: Psychology*, *9*(1), 57641. https://doi.org/10.1525/collabra.57641

Zendle, D., & Cairns, P. (2019). Video game loot boxes are again linked to problem gambling: Results of a large-scale survey. *PLoS ONE*, *14*(3), e0214167. https://doi.org/10.1371/journal.pone.0214167

Zendle, D., Meyer, R., & Ballou, N. (2020b). The changing face of desktop video game monetisation: An exploration of exposure to loot boxes, pay to win, and cosmetic microtransactions in the most-played Steam games of 2010–2019. *PloS ONE*, *15*(5), e0232780. https://doi.org/10.1371/journal.pone.0232780

Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020a). The prevalence of loot boxes in mobile and desktop games. *Addiction*, *115*(9), 1768–1772. https://doi.org/10.1111/add.14973

Zuriff, G. E. (1970). A comparison of variable-ratio and variable-interval schedules of reinforcement. *Journal of the Experimental Analysis of Behavior*, *13*(3), 369–374. https://doi.org/10.1901/jeab.1970.13-369

Author information

Seppy Pour – LLB (Hons), BA, LLM, Principal Consultant, Kun Consulting Group
Address: NSW 2006, Sydney, Australia
E-mail: seppypour@gmail.com
ORCID ID: https://orcid.org/0000-0001-9032-062X

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – August 25, 2023
Date of approval – September 20, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:346.6:004.4
EDN: https://elibrary.ru/vdvuuk
DOI: https://doi.org/10.21202/jdtl.2024.19

Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии

Исмаила Озовехе Харуна ✉
Университет принца Абубакара Ауду, Аньигба, Нигерия

Пол Атагамен Айдоноджи
Кампальский международный университет, Кампала, Уганда

Онивеху Джулиус Бейда
Университет Бингема, Кару, Нигерия

Ключевые слова

аутентификация,
безопасность,
конфиденциальность,
Нигерия,
право,
цифровизация,
цифровые технологии,
электронная подпись,
электронная транзакция,
электронные платежи

Аннотация

Цель: выявить правовые проблемы, мешающие бесперебойной работе электронных платежных систем в Нигерии в условиях, когда официальными лицами и нигерийскими органами власти уже предприняты определенные шаги по регулированию системы электронных платежей в стране, но их недостаточно.

Методы: исследование строится на нескольких подходах к изучению вопросов, касающихся правового режима электронных платежей в Нигерии. Наряду с применением доктринального толкования нормативно-правовой базы, регулирующей отношения, связанные с использованием системы электронных платежей, задействован социологический познавательный инструментарий в виде анкетирования респондентов, проживающих в различных геополитических зонах Нигерии. Описание и анализ полученных данных показывает реальное отношение опрошенных лиц к происходящим процессам.

Результаты: рассмотрены международное регулирование и национальное законодательство в области электронных платежей, действующее в Нигерии. Исследование показало, что электронные платежи являются эффективным средством транзакций, однако существует ряд юридических проблем, которые могут мешать беспрепятственному использованию электронных платежей в Нигерии. Установлено, что хотя в стране принят ряд законов, касающихся регулирования банковской и других видов финансовой деятельности,

✉ Контактное лицо

их недостаточно для решения проблем, обусловленных применением современных технологий. В статье нашли отражение вопросы, связанные с применением электронной подписи, доверием к технологиям, конфиденциальностью данных, безопасностью электронных транзакций, мошенничеством, аутентификацией и авторизацией, определенностью прав и обязанностей, юрисдикцией и площадкой для разрешения интернет-споров, налогообложением электронных платежей и др. Отмечается, что задачу создания безопасной цифровой среды для бесперебойной работы электронной коммерции и электронных платежей в Нигерии нельзя возлагать исключительно на правительство.

Научная новизна: на примере одного из перспективных государств Африки раскрывается спектр проблематики, касающийся работы электронных платежных систем, подкрепленный опросом общественного мнения для выяснения отношения по целому ряду вопросов, с которыми чаще всего сталкиваются граждане при использовании системы электронных платежей, и возможных направлений изменений в этой области.

Практическая значимость: актуальные правовые вопросы, поднимаемые в проведенном исследовании, в значительной степени препятствуют нормальному использованию системы электронных платежей в Нигерии, в связи с чем возрастает значимость предлагаемых авторами возможных путей для ее совершенствования.

Для цитирования

Харуна, И. О., Айдоноджи, П. А., Бейда, О. Дж. (2024). Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии. *Journal of Digital Technologies and Law*, *2*(2), 372–393. https://doi.org/10.21202/jdtl.2024.19

Содержание

Введение

Появление Интернета принесло с собой улучшения в различных сферах жизни (Iriobe & Akinyede, 2017). Одним из них являются электронные платежные системы, которые представляют собой программное обеспечение, позволяющее переводить денежные средства с использованием цифровых технологий (Adkwodimmah & Ochei, 2019). Электронные платежные системы обладают множеством преимуществ, включая скорость, анонимность, открытость, совместимость, цифровизацию и применимость в глобальном масштабе. Это делает их предпочтительным средством оплаты в режиме реального времени для различных операций (Dupas et al., 2018).

Не вызывает сомнений, что в Нигерии развитие технологий достигло высокого уровня практически во всех секторах экономики, и особенно в банковском секторе (Sobehart, 2016). Это связано с тем, что большинство видов деятельности в банковском секторе были переведены в цифровой формат, благодаря чему значительно упростились транзакции между сторонами, участвующими в коммерческой деятельности (Aidonojie & Ong Argo, 2022). Одним из самых полезных усовершенствований стало использование систем электронных платежей (Sokolowska, 2015). Система электронных платежей позволяет человеку с легкостью оплачивать любые операции, не используя наличных денег и не вступая в непосредственный контакт с другими сторонами. Однако следует отметить, что эта технология не только улучшила деятельность человека, но и сопровождалась рядом угроз при проведении договорных и финансовых операций (Sokolowska, 2015). Это произошло в результате злоупотреблений со стороны недобросовестных субъектов, которые используют пробелы в законодательстве о системах электронных платежей в Нигерии. Ситуация усугубляется низким уровнем знаний в области информационных технологий у большинства граждан, которые часто вынуждены использовать каналы электронных платежей для транзакций.

Кроме того, существуют и другие серьезные проблемы, связанные с развитием электронных платежей. Это, в частности, такие области, которые связаны с электронной подписью, доверием и уверенностью, конфиденциальностью, безопасностью электронных транзакций, мошенничеством, аутентификацией и авторизацией, определенностью прав и обязанностей, юрисдикцией и площадкой для разрешения интернет-споров, налогообложением электронных платежей и др. Перечисленные проблемы в значительной степени препятствуют нормальному использованию электронных платежей в Нигерии (Laven & Bruggink, 2016). Хотя в стране принят ряд законов, касающихся регулирования банковской и других видов финансовой деятельности, их недостаточно для решения проблем, связанных с применением технологий (Gabor & Brooks, 2017). Например, Центральный банк Нигерии (Omoyajowo, 2021), который является надзорным органом и заинтересованным лицом нигерийской финансовой системы, предпринял некоторые шаги по регулированию систем электронных платежей в стране, однако ряд проблем, связанных с инфраструктурой, законодательством и информационными технологиями, по-прежнему мешают их бесперебойной работе. Существующие проблемы могут быть решены только путем расширения сферы применения действующего законодательства и внесения в него необходимых поправок (Aidonojie & Ong Argo, 2022).

Исходя из вышесказанного, данное исследование предполагает использование гибридного метода исследования при анализе законов, касающихся систем электронных платежей в Нигерии. В работе также приведен краткий обзор концептуального характера электронных платежей в Нигерии. Мы также описываем ряд правовых вопросов, препятствующих развитию системы электронных платежей в Нигерии, и предлагаем возможные пути для ее усовершенствования.

1. Правовая база в области электронных платежей в Нигерии

Концепция электронных платежей получила мировое признание, поэтому существуют международные законы, регулирующие электронные платежи. Рассмотрим международные и национальные законы в области электронных платежей, действующие в Нигерии.

Типовой закон об электронных подписях Комиссии ООН по законодательству о международной торговле (United Nations Commission for International Trade Law Model Law on Electronic Signatures, UNCITRAL) был принят в ответ на все более широкое использование электронных методов удостоверения подлинности в качестве замены рукописных подписей и других традиционных способов удостоверения подлинности сделок. При этом утверждалась необходимость создания специального правового режима для уменьшения неопределенности в отношении правовых последствий использования таких современных методов (т. е. электронных подписей). Ставилась задача обеспечить гармонизацию законодательства об электронных сделках и соответствующую техническую совместимость на международном уровне (Tasneem, 2014). Основные цели Типового закона заключаются в следующем:

1. Обеспечить возможность или способствовать использованию электронных подписей.

2. Обеспечить равные возможности для пользователей бумажной и компьютерной документации.

Эти цели имеют важное значение для повышения экономичности и эффективности международной торговли. Однако этот документ не имеет силы закона, учитывая тот факт, что, согласно разделу 12 Конституции Нигерии, все международные документы должны быть приняты и ратифицированы Национальной ассамблеей.

Кроме того, следует упомянуть Закон о доказательствах – национальный закон, который также имеет отношение к электронным платежам в Нигерии. Актуальность этого закона для нашего исследования заключается в том, что он санкционирует использование значительного числа компьютерных документов для доказательства. Самая большая проблема с допустимостью электронных доказательств в Нигерии связана с законодательным признанием электронных документов. Разделы 34 и 84 Закона о доказательствах 2011 г. (с поправками) предусматривают допустимость документов, хранящихся в электронной форме, в качестве доказательств. Эти положения отсутствовали в Законе о доказательствах 1945 г. Тем самым электронным доказательствам придается необходимый вес.

В связи с этим могут возникнуть следующие вопросы: допустимы ли компьютерные распечатки в качестве доказательств в гражданских или уголовных процессах? Если да, то будут ли они считаться первичными или вторичными доказательствами? Или же они должны быть отнесены к доказательствам в виде исключений, подобно слухам? Можно ли считать документы, созданные в электронном виде, документальными доказательствами? (Tasneem, 2014).

Верховный суд Нигерии постановил, что электронные доказательства являются допустимыми. Кроме того, в деле Kajala V. Noble (1982) 75 CR APP R.149 суд подтвердил допустимость в качестве доказательства видеозаписи новостей BBC, на которой запечатлено участие ответчика в массовых беспорядках. Суды Нигерии придерживаются либерального подхода к толкованию и применению Закона о доказательствах и существующих правовых норм и учитывают компьютерные распечатки и подобные документы в качестве доказательств.

Следует также отметить, что правительство Нигерии уделяет большое внимание укреплению кибербезопасности. С этой целью оно инициировало ряд мер и законов, включая регистрацию пользователей GSM в 2011 г. и введение Центральным банком Нигерии (CBN) централизованной системы биометрической идентификации для банковской отрасли (Bank Verification Number, BVN). Кроме того, в 2015 г. был принят первый закон, посвященный кибербезопасности. Законом о киберпреступности 2015 г. была введена в действие директива ЭКОВАС о борьбе с преступностью на местном и глобальном уровнях.

Согласно разделу 58 этого закона, финансовые учреждения признаются заинтересованными сторонами в системе кибербезопасности. Термин «финансовое учреждение» определяется как «любое лицо, орган, ассоциация или группа лиц, корпоративных или некорпоративных, которые занимаются бизнесом и другими видами деятельности, определяемыми Центральным банком или соответствующими органами. Основные обязанности, возлагаемые на финансовые учреждения, перечислены в части IV данного Закона» (Ezike, 2013). Однако Закон о киберпреступности не является основным законодательным актом, который регулирует электронные платежи, а, скорее, относится к сфере кибербезопасности в Нигерии.

Кроме того, с целью обеспечить технологическое развитие страны и полнее использовать преимущества глобализации, в Нигерии был предложен законопроект об электронных транзакциях (Abubakar & Adebayo, 2015). Он содержит важные положения, которые в случае принятия будут способствовать развитию системы электронных платежей. Так, часть III законопроекта устанавливает действительность электронных сделок и аспекты, регулирующие формирование электронных контрактов. Часть IV предусматривает ответственность онлайн-посредников и создателей онлайн-контента, а также защиту пользователей. Часть V регулирует различные аспекты электронной торговли, такие как защита прав потребителей и онлайн-реклама электронных торговых операций. Часть VI посвящена безопасности в цифровой экономике. В законопроекте также содержатся положения о целостности информации и признании иностранных электронных документов и подписей.

Хотя законопроект еще не одобрен правительством Нигерии, однако если он будет принят в качестве закона, это обеспечит уверенность деловых кругов в надежности и законности различных деловых операций в Интернете. Кроме того, он ускорит экономический рост за счет бесперебойности и точности договорных и финансовых операций, особенно в вопросах электронных платежей.

2. Правовые проблемы, связанные с электронными платежами в Нигерии

2.1. Конфиденциальность

Электронные транзакции предоставляют гражданам и правительству возможность собирать информацию о клиентах или субъектах данных, которая впоследствии может быть использована для маркетинга или в качестве ключевого фактора при принятии оперативных и политических решений (Tasneem, 2014). Электронные транзакции открывают перед гражданами широкие возможности, однако при этом угрожают неприкосновенности их частной жизни. Поэтому необходимо обеспечить строгие меры безопасности данных, чтобы защитить граждан от незаконных действий по сбору информации и ее использованию в целях, не связанных с причинами сбора таких данных.

Хотя Конституция Нигерии содержит специальное положение, касающееся права граждан на неприкосновенность частной жизни, все же существует необходимость в принятии специальных законов о конфиденциальности данных. Раздел 37 Конституции Нигерии гласит: «неприкосновенность частной жизни каждого гражданина Нигерии, тайна его телефонных разговоров, жилища, переписки и телеграфных сообщений гарантируются и защищаются»[1]. Однако этого может быть недостаточно для решения проблем, связанных с обработкой персональных данных. Хорошим примером является Закон о защите данных Соединенного Королевства, адаптированный в Нигерии, который содержит важные принципы, а именно:

«1. Обработка данных должна осуществляться с соблюдением справедливости и законности.

2. Сбор данных может осуществляться исключительно для одной или нескольких конкретных и законных целей.

3. Данные должны быть точными и актуальными.

4. Данные не должны храниться дольше, чем необходимо.

5. Обработка данных должна осуществляться с соблюдением прав субъекта данных.

6. Безопасность и сохранность данных должна обеспечиваться с помощью организационных и технических методов.

7. Данные не могут передаваться и перемещаться за пределы Европейской экономической зоны (ЕЭЗ), за исключением случаев, когда обеспечивается адекватный или достаточный уровень защиты данных»[2].

2.2. Определенность прав и обязанностей

Определяющим компонентом любой успешной рыночной экономики в цифровой среде является верховенство закона и обеспечение юридической силы письменных соглашений и сделок, которые следуют заранее установленным правилам относительно уведомления сторон, прав и обязательств по раскрытию информации (Zhaohui, 2012). Как и в традиционных платежных системах, вопросы определенности прав и обязанностей занимают важное место в сфере электронных платежей. В частности, это касается таких вопросов:

1. Когда электронный платеж можно считать завершенным?

2. Признаются ли электронные платежи средством оплаты в коммерческой сфере?

3. Доступны ли бенефициару средства, переведенные с помощью электронного платежа?

4. Существует ли возможность отмены договора электронного платежа?

Что касается вышесказанного, мы вынуждены констатировать отсутствие четкой правовой базы по данному вопросу, неопределенность и непредсказуемость в области прав сторон электронной транзакции. При этом баланс сил в основном складывается в пользу банков, которые являются поставщиками услуг, тогда как потребители зачастую вынуждены заключать односторонне выгодное соглашение. К сожалению, на сегодняшний день в Нигерии не существует законодательства, регулирующего вышеупомянутые вопросы.

---

1 Constitution of the Federal Republic of Nigeria 1999. https://clck.ru/3B7Cpa

2 Nigerian Data Protection Act. https://clck.ru/3B7DZp

2.3. Мошенничество

Хотя системы электронных платежей имеют большое значение для нигерийской экономики, однако в Нигерии существуют серьезные проблемы, связанные с киберпреступностью и мошенничеством, которые нигерийское правительство до сих пор не в состоянии решить (Aguda, 2021). Одним из способов мошенничества в сфере электронных платежей является «фишинг». При этом пользователю без запроса отправляют электронное письмо якобы от финансового или правительственного учреждения; отправитель требует сообщить ему некоторые ключевые элементы личной информации по каким-либо официальным или административным причинам (например, для внесения обновлений в систему). В письме может содержаться предупреждение о том, что отказ от сообщения этой информации приведет к приостановке или закрытию счета. Мошенник обманом получает у жертвы личные данные, например коды доступа и пароли, которые затем использует в своих преступных целях. Такая деятельность может включать незаконный доступ к банковским счетам жертвы с целью выкачивания из них средств.

Еще один способ мошенничества в сфере электронных платежей – «кража личности». В этом случае преступник получает доступ к вашей личной информации любым способом, включая фишинг. Затем он может использовать эту информацию для открытия банковских счетов для незаконных операций, например, для получения кредитов с использованием государственных документов, таких как паспорта и водительские права. В информационную эпоху появление систем электронных платежей открывает возможность совершения подобных преступлений. Во многих юрисдикциях специальные законы квалифицируют использование чужой личности в корыстных целях как преступление. В Нигерии на данный момент документом, который напрямую касается предотвращения или криминализации такого рода мошенничества, является Закон о киберпреступности от 2015 г.

2.4. Электронная аутентификация

Методы аутентификации личности снижают скорость и эффективность электронных транзакций (Aguda, 2021). Поэтому финансовые учреждения используют альтернативные методы аутентификации. К ним относятся:

1) персональные идентификационные номера и пароли;

2) цифровые сертификаты с использованием инфраструктуры открытых ключей;

3) устройства на основе микрочипов, включая смарт-карты или другие типы жетонов;

4) методы сравнения баз данных, например, в приложениях для проверки на мошенничество;

5) устройства биометрической идентификации.

Эти методы аутентификации обеспечивают различные уровни безопасности и надежности. Стоимость и сложность инфраструктуры, лежащей в их основе, также различны. Поэтому выбор метода (методов) аутентификации должен быть соразмерен рискам, связанным с продуктами и услугами, доступ к которым они контролируют.

3. Юрисдикция и площадка для разрешения споров в области электронных платежей

Ключевым компонентом деятельности, связанной с Интернетом, являются его универсальность и более широкая доступность по сравнению с взаимодействием традиционными средствами. Благодаря этому время, границы государств, расстояния и другие физические факторы не препятствуют быстрому и эффективному проведению сделок. Таким образом, коммерсанты могут получать прибыль от широкой аудитории и бесконечных возможностей. Поэтому возникают вопросы, связанные с определением интернет-юрисдикции, поскольку договоры, заключенные в Интернете, не привязаны к конкретной территории. В случае возникновения споров по договорам, заключенным через Интернет, если стороны онлайн-сделки проживают в разных юрисдикциях, какие факторы будут определять место разрешения такого спора? Вопросы могут также возникать в ситуации, когда веб-сайт размещен на личном сервере и доступен людям из разных точек мира; подпадает ли его владелец под действие всех юрисдикций мира? (Adkomolede, 2008).

Чтобы определить юрисдикцию, регулирующую конкретный спор в Интернете, необходимо ответить на ряд актуальных вопросов:

1. Где велись переговоры или выполнялись другие действия с использованием Интернета?

2. Как в юрисдикции данного государства расценивается деятельность или сделка, выполняемая с использованием Интернета?

Конкретные правила в отношении «типовых законов», касающихся интернет-юрисдикции, еще предстоит разработать. Так, в Нигерии еще не введены Типовой закон об электронной торговле Комиссии ООН по законодательству о международной торговле и Конвенция ООН об использовании электронных сообщений в международных договорах. В связи с этим, согласно разделу 12 Конституции Нигерии, международные законы, которые еще не введены во внутреннее право, не имеют юридической силы.

Однако общее правило для интернет-контрактов заключается в том, что юрисдикция определяется путем установления места или страны, где был исполнен конкретный интернет-контракт. В случаях, когда исполнение связанных с Интернетом действий или договоров происходило во многих местах одновременно, соответствующей юрисдикцией будет считаться государство, в котором возник спор. Кроме того, при определении юрисдикции может иметь значение место жительства сторон. Однако общее правило, применимое к потребительским товарам, гласит, что потребители могут подавать иски и привлекаться к суду в своих государствах.

4. Доверие к электронным платежам

Электронные платежи помогают преодолеть факторы расстояния и времени между потребителями и продавцами во время транзакций (Jessah, 2019). Это означает, что большая часть коммерческих и договорных действий, происходящих между потребителем и продавцом, должна осуществляться в виртуальном пространстве. Можно выделить три основные проблемные области, связанные с концепцией доверия:

1) экспертиза: доверяя какой-либо стороне сделки, мы верим в то, что она обладает необходимой квалификацией и техническими знаниями;

2) добросовестность: мы верим, что другая сторона настроена на добросовестное отношение к клиенту в процессе деловой активности и получения прибыли;

3) честность: мы верим, что доверенная сторона будет соблюдать общепринятые правила поведения и вести дела честным и надежным образом, выполняя свои обязательства.

Электронные сделки по своей природе более сложны, чем обычные сделки, совершаемые в традиционной среде. Поэтому доверие является важнейшим элементом, лежащим в основе их проведения. Установить доверие между клиентом и продавцом в ходе онлайн-сделки особенно сложно. Это связано с тем, что онлайновые сделки сопровождаются мерами по соблюдению анонимности между сторонами, осуществляющими сделку в виртуальной среде (Acha, 2008).

5. Налогообложение при электронных платежах

Экономическая свобода, появившаяся благодаря сделкам в Интернете, привела к увеличению трафика онлайн-операций, что оттеснило на задний план традиционные способы совершения сделок. Однако существующее налоговое законодательство не учитывает значительных изменений, вызванных появлением Интернета или «новой экономики» (Udobi-Owoloja et al., 2020). В связи с этим возникает вопрос: как облагать налогом товары, приобретенные в Интернете потребителями, которые не проживают в пределах страны, где находится компания или платформа продавца, и нужно ли вообще облагать налогом интернет-транзакции? Существующие законы государств и местные законы о налогообложении, несомненно, испытывают огромные трудности в связи с появлением электронных транзакций в небывалых ранее масштабах. В Нигерии вопросы налогообложения регулирует Закон об учреждении Федеральной службы внутренних доходов (Federal Inland Revenue Service, FIRS) 2007 г., который наделяет эту службу полномочиями по установлению и сбору налогов. Традиционная налоговая система основывается на определении места осуществления экономической деятельности, однако Интернет позволяет осуществлять деловые операции в разных странах. Эти проблемы усугубляются тем, что электронная торговля обладает огромным потенциалом в качестве источника государственных доходов в информационную эпоху. В Нигерии такая эпоха наступает с ростом автоматизации транзакций.

Среди других актуальных вопросов, связанных с налогообложением при электронных платежах, можно назвать следующие: Какие инфраструктурные объекты необходимы для создания эффективной и справедливой системы налогообложения в коммерческой сфере? Как государство может контролировать налоговые отчисления, не ставя препятствий развитию Интернета? Важной проблемой является также борьба с уклонением от уплаты налогов и мошенничеством. Таким образом, возникает необходимость разработки закона, который бы адекватно регулировал экономическую деятельность в Интернете, чтобы увеличить доходную базу государства и поддержать рост и развитие электронной коммерции в Нигерии.

6. Представление и анализ данных

Данные были получены с помощью метода онлайн-анкетирования. Анализ полученных данных представлен ниже.

6.1. Размер выборки и методы

За основу исследования взяты ответы 302 респондентов, проживающих в различных районах Федеративной Республики Нигерия.

Для отбора респондентов исследователи использовали метод простой случайной выборки. Этот метод считается наиболее подходящим и надежным для получения адекватного результата (Majekodunmi et al., 2022). Кроме того, в ряде исследований (Aidonojie & Ong Argo, 2022) отмечалось, что метод простой случайной выборки обладает следующими качествами:

1) хорошо подходит для выборки в условиях неоднородности населения;
2) достоверен и подходит для получения объективного результата;
3) прост в использовании;
4) соответствует гибридному подходу к правовым исследованиям.

6.2. Анализ данных

Анализ данных, собранных в данном исследовании с помощью анкетирования, показал следующее.

В табл. 1 показано, в каких регионах Федеративной Республики Нигерия проживают респонденты, принявшие участие в исследовании.

Таблица 1. Регионы проживания респондентов в Нигерии

№	Регион Нигерии	Количество	%
1	Северо-центральный	58	19,2
2	Северо-восточный	38	12,6
3	Северо-западный	44	14,6
4	Юго-восточный	57	18,8
5	Южный	65	21,5
6	Юго-западный	40	13,3
	Всего	302	100

В табл. 2 показаны ответы респондентов на вопрос, имеют ли электронные платежи перспективы в деловой сфере Нигерии.

Таблица 2. Распределение ответов респондентов о наличии перспективах развития электронных платежей в коммерческой деятельности

Ответ респондента	Количество	%
Да	248	82,1
Нет	54	17,9
Всего	302	100

В табл. 3 показаны различные перспективы системы электронных платежей в Нигерии, упомянутые респондентами.

Таблица 3. Распределение ответов респондентов о перспективах системы электронных платежей

Варианты ответов	Количество	%
Удобство перевода средств или платежа	222	88,8
Экономическая эффективность	202	80,8
Используется как средство мгновенного платежа в различных сделках	192	76,8
Применяется во всем мире	183	73,2
Анонимность, т. е. возможность сохранить конфиденциальность пользователя	166	66,4
Быстрота проведения транзакции	107	42,8

Таблица 4 демонстрирует, что большинство респондент осознают наличие проблем, связанных с функционированием системы электронных платежей в Нигерии.

Таблица 4. Распределение ответов респондентов о проблемах системы электронных платежей

Ответ респондента	Количество	%
Да	248	82,1
Нет	54	17,9
Всего	302	100

В табл. 5 показаны проблемы по значимости для респондентов, связанные с системой электронных платежей в Нигерии.

Таблица 5. Распределение ответов о проблемах в системах электронных платежей

Варианты ответов	Количество	%
Неэффективность и неадекватность правовой базы в сфере электронных платежей в Нигерии	236	94
Проблема защиты персональных данных пользователя системы электронных платежей	231	92
Низкое качество интернет-обслуживания	215	85,7
Высокая вероятность мошенничества	195	77,7
Проблемы налогообложения электронных сделок	188	74,9
Вопросы юрисдикции и площадки для разрешения споров в случае их возникновения	138	55
Определенность прав и обязанностей в случае сбоя в электронной транзакции	90	35,9
Сложность аутентификации пользователей системы электронных платежей	88	35,1

В табл. 6 приведены возможные пути решения проблем, связанных с системой электронных платежей в Нигерии, предложенные респондентами.

Таблица 6. Распределение ответов о совершенствовании системы электронных платежей

Варианты ответов	Количество	%
Обеспечить защиту персональных данных пользователя системы электронных платежей	223	89,2
Усовершенствовать правовую базу в сфере электронных платежей для адекватного регулирования сферы цифровых платежей	221	88,4
Снизить вероятность мошенничества в интернете правовыми и технологическими средствами	215	86
Провайдеры должны обеспечить эффективное интернет-обслуживание	212	84,8
Адаптировать международные договоры, направленные на решение вопросов юрисдикции и площадки для разрешения споров в сфере электронных платежей	131	52,4
Банки и иные стороны должны упростить процесс электронной аутентификации пользователей системы электронных платежей	65	26

6.3. Обсуждение результатов

Данные, полученные с помощью анкеты и проанализированные выше, показывают следующее. На вопросы анкеты ответили 302 респондента из различных геополитических зон Нигерии, что отражено в табл. 1. Респонденты обладают достаточными знаниями, чтобы дать обоснованный ответ по вопросам, касающимся системы электронных платежей в Нигерии. По данным табл. 2, 82,1 % респондентов отметили, что существуют различные перспективы, связанные с внедрением электронных платежей в Нигерии. Так, некоторые из перспектив электронных платежей были определены респондентами следующим образом (табл. 3):

1) 80,8 % респондентов заявили, что это экономически выгодно;

2) 88,8 % согласились с тем, что это удобный метод передачи средств или расчета по сделке;

3) 42,8 % отметили, что электронные платежи позволяют быстро осуществлять расчеты;

4) 66,4 % высказали мнение, что это позволяет обеспечить анонимность пользователей электронных платежей, если они того пожелают;

5) 73,2 % заявили, что система электронных платежей применима в глобальном масштабе;

6) 76,8 % респондентов согласились с тем, что электронные платежи стали предпочтительным средством оплаты в режиме реального времени для различных операций.

В связи с вышесказанным можно констатировать, что результаты, показанные в табл. 3, соответствуют выводам других исследований, согласно которым использование технологий значительно упрощает финансовые операции. Однако, согласно табл. 4, 82,1 % респондентов считают, что существуют проблемы, препятствующие нормальному использованию системы электронных платежей в Нигерии. В этой связи в табл. 5 перечислены некоторые из проблем в этой сфере, указанные респондентами, а именно;

1) 94 % респондентов отметили неэффективность и неадекватность нигерийской нормативно-правовой базы, касающейся электронных платежей;

2) 92 % респондентов согласились с тем, что существует проблема конфиденциальности данных пользователей электронных платежей;

3) 35,9 % респондентов отметили проблему, связанную с определенностью прав и обязанностей в случае сбоя электронной операции;

4) 77,7 и 35,1 % назвали проблемой случаи мошенничества и сложность электронной аутентификации пользователей электронных платежей соответственно;

5) 55,1 % респондентов называют одной из основных проблем системы электронных платежей в Нигерии вопросы юрисдикции и площадки для разрешения споров в данной сфере;

6) кроме того, 74,9 и 85,7 % респондентов считают частой проблемой налогообложение электронных платежей и низкое качество интернет-услуг соответственно.

Актуальность электронных платежей для финансовой системы Нигерии, несомненно, очень высока. Это связано с тем, что система электронных платежей значительно упрощает оплату транзакций, а также способствует реализации политики

безналичного оборота денежных средств, которую уже в течение некоторого времени продвигает правительство страны. Понимая значимость и положительное влияние электронных платежей на экономику Нигерии, респонденты определяли некоторые возможные пути решения проблем, связанных с системой электронных платежей в Нигерии (табл. 6):

1) 88,4 % респондентов заявили, что необходимо внести изменения в законодательную базу, обеспечивающую адекватное регулирование цифровых платежей;

2) 89,2 % респондентов согласились с тем, что правительство должно обеспечить защиту права пользователей электронных платежей на конфиденциальность их данных;

3) 26 % заявили, что банки и другие заинтересованные стороны должны упростить процесс электронной аутентификации для совершения электронных платежей;

4) 52,4 % ответивших назвали важным внедрение международных договоров для решения вопросов юрисдикции и площадок для разрешения споров по электронным платежам;

5) 86 % заявили, что пресечение случаев интернет-мошенничества с помощью правовых и технологических средств позволит усовершенствовать систему электронных платежей;

6) наконец, 84,8 % респондентов считают, что поставщики интернет-услуг должны повысить эффективность предоставления этих услуг.

Учитывая вышесказанное, можно сделать вывод, что если перечисленные средства будут реализованы различными заинтересованными сторонами нигерийской экономики, это поможет усовершенствовать систему электронных платежей в Нигерии.

Заключение

Современный мир стал более компактным и доступным по своей структуре. Прежние препятствия для взаимодействий людей в форме общения, бизнеса и управления уничтожены Интернетом – время, пространство и географические барьеры сжались до размеров компьютеров и других связанных с ними цифровых устройств. Все пространство человеческой жизни сегодня находится под влиянием технологических инноваций, масштабы и возможности которых продолжают бросать вызов существующим традиционным законам как внутри стран, так и на международном уровне. Компьютер и Интернет помогли человеку покорить ранее недоступные территории в плане развития и прогресса человечества.

Однако тщеславные побуждения и другие недостатки человеческой природы привели к тому, что это важнейшее достижение в истории человечества стало объектом манипулирования информацией, киберкраж, хакерства, отмывания денег, взломов систем, рассылки спама и ряда других неблаговидных действий в Интернете. В киберпространстве Нигерии присутствуют все эти угрозы, что, несомненно, требует усилий страны по обеспечению безопасности и защиты Интернета, включая электронные платежные средства. В данной работе исследованы формы систем безопасности, помогающие обеспечить целостность систем электронных

платежей в Нигерии, а также проведен анализ существующих законов в этой сфере с целью выявления их сильных и слабых сторон.

В работе отмечается, что законодательные органы Нигерии предприняли ряд адекватных мер, в результате которых были созданы некоторые ключевые законопроекты, связанные с электронными платежами. Однако необходимо незамедлительно утвердить эти законопроекты, чтобы они гарантированно привели к желаемому оздоровлению в сфере проведения электронных транзакций в Нигерии. При этом следует отметить, что задачу создания безопасной цифровой среды для бесперебойной работы электронной коммерции и электронных платежей в Нигерии нельзя возлагать исключительно на правительство. Для противодействия криминальным действиям владельцы интернет-компаний должны обеспечить полноценную интеграцию необходимых аналитических данных в бизнес-операции. Кибербезопасность также должна стать приоритетом в сфере электронной коммерции, поэтому следует разработать широкие программы обеспечения безопасности с учетом различных непредвиденных обстоятельств.

Список литературы

Abubakar, A. S., & Adebayo, F. O. (2014). Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects. *Mediterranean Journal of Social Sciences*, *5*(2), 215. https://doi.org/10.5901/mjss.2014.v5n2p215

Acha, I. A. (2008). Electronic Banking in Nigeria: Concept, Challenges and Prospects. *International Journal of Development and Management Review*, *3*(1), 23–45.

Adkomolede, T. (2008). Contemporary Legal Issues on Electronic Commerce in Nigeria. *Potchefstroom Electronic Law Journal*, *11*(3) 9–18. https://doi.org/10.4314/pelj.v11i3.42234

Adkwodimmah, C., & Ochei, A. I. (2019). Financial Technology and Liquidity in the Nigerian Banking Sector. *Journal of Association of Professional Bankers in Education*, *5*(1), 243–162.

Aguda, O. O. (2021). An Appraisal of the Legal Framework for Online Banking in Nigeria and South Africa. *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law*, *3*(1), 11–17.

Aidonojie, P. A., & Ong Argo, V. (2022). The Societal and Legal Missing Link in Protecting a Girl Child against abuse before and Amidst the Covid-19 Pandemic in Nigeria. *Jurnal Hukum UNISSULA*, *38*(1), 61–80. http://dx.doi.org/10.26532/jh.v38i1.18412

Dupas, P., Karlan, D., Robinson, J., & Ubfal, D. (2018). Banking the Unbanked? Evidence from Three Countries. *American Economic Journal: Applied Economics*, *10*(2), 257–297. https://doi.org/10.1257/app.20160597

Ezike, E. O. (2013). Online Contracts in Nigeria –An Overview. *The Nigerian Juridical Review*, *11*, 53–82.

Gabor, D., & Brooks, S. (2017). The Digital Revolution in Financial Inclusion: International Development in the Fintech Era. *New Political Economy*, *22*(4), 423–436. https://doi.org/10.1080/13563467.2017.1259298

Iriobe, G., & Akinyede, O. M. (2017). The Effect of Financial Technology Services on Banks Customers Satisfaction in Nigeria. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2984215

Jessah, J. E. (2019). E-Commerce in Nigeria: Liability for Loss or Damage to Goods Supplied by a Seller Pursuant to an Electronic Contract. *IJOCLLEP*, *1*(3), 105–114.

Laven, M., & Bruggink, G. (2016). How FinTech is transforming the way money moves around the world. *Journal of Payments Strategy & Systems*, *10*(1), 6–12.

Majekodunmi, T. A., Akintola, J. O., Aidonojie, P. A., Ikubbanni, O. O., & Oyebade, A. A. (2022). Legal Issues in Combating the Scourge of Terrorism; Its Impact on International Trade and Investment: Nigeria as a Case Study. *KIU Journal of Humanities*, *7*(3), 129–139.

Omoyajowo, K. (2021). Crowdfunding Regulatory Framework in Nigeria: An Appraisal of the Highlights of SEC Crowdfunding Regulation. *SSRN Electronic Journal*.

Sobehart, J. R. (2016). The FinTech revolution: Quantifying earnings uncertainty and credit risk in competitive business environments with disruptive technologies. *Journal of Risk Management in Financial Institutions*, *9*(2), 67–78.

Sokołowska, E. (2015). Innovations in the payment card market: The case of Poland. *Electronic Commerce Research and Applications*, *14*(5), 292–304. https://doi.org/10.1016/j.elerap.2015.07.005

Tasneem, F. (2014). Legal Effect of Electronic Contracts in Australia. *Global Research Journal of Engineering, Technology and Innovation*, *3*(1), 020–026.

Udobi-Owoloja, P. I., Ahigbe, B. E., Ubi, A. E., Gbajumo-Sheriff, M. A., & Umoru, B. (2020). Digital Banking and Bank Profitability in Nigeria. *Nigerian Journal of Management Studies*, *20*(2), 24–34.

Zhaohui, L. (2012). Motivation of Virtual Goods Transactions Based on the Theory of Gaming Motivations. *Journal of Theoretical and Applied Information Technology*, *43*(2), 254–260.

Сведения об авторах

Харуна Исмаила Озовехе – адвокат, бакалавр права, магистр права, аспирант в области педагогики, консультант отдела аспирантуры
Юридический факультет, Университет принца Абубакара Ауду
Адрес: Нигерия, штат Коги, г. Аньигба, P.M.B 1008
E-mail: Ozovehe.ih@ksu.edu.ng
ORCID ID: https://orcid.org/0009-0006-8773-768X
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=8xkClmoAAAAJ

Айдоноджи Пол Атагамен– PhD, заместитель декана по научной работе, Кампальский международный университет
Адрес: Уганда, г. Кампала, район Кансанга, Ггаба роуд, 20000
E-mail: paul.aidonojie@kiu.ac.ug
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Бейда Онивеху Джулиус – PhD, заведующий кафедрой публичного и частного права, юридический факультет, Университет Бингема
Адрес: Нигерия, штат Насарава, г. Кару, P.M.B 005, KM 26 Абуджа-Кеффи
E-mail: beida.onivehu@binghamuni.edu.ng
ORCID ID: https://orcid.org/0000-0002-6089-5059
Google Scholar ID: https://scholar.google.com/citations?user=fxTBqlMAAAAJ

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: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 22 сентября 2023 г.
Дата одобрения после рецензирования – 21 октября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:346.6:004.4
EDN: https://elibrary.ru/vdvuuk
DOI: https://doi.org/10.21202/jdtl.2024.19

Prospects and Issues Concerning the Regulatory Regime of E-Payment System in Nigeria

Ismaila Ozovehe Haruna ✉
Prince Abubakar Audu University, Anyigba, Nigeria

Paul Atagamen Aidonojie
Kampala International University, Kampala, Uganda

Onivehu Julius Beida
Bingham University, Karu, Nigeria

Keywords

authentication,
digital technologies,
digitalization,
electronic payments,
electronic signature,
electronic transaction,
law,
Nigeria,
privacy,
security

Abstract

Objective: to reveal the legal challenges impeding the smooth operation of electronic payment systems in Nigeria, given that Nigerian official bodies and individuals have already taken some steps to regulate the electronic payment system in the country, but the said step are insufficient.

Methods: the study is built on several approaches to the issues of the legal regime of electronic payments in Nigeria. Alongside with the doctrinal interpretation of the legal framework regulating the relations associated with the use of electronic payment system, the authors used sociological cognitive tools and conducted a survey of respondents residing in different geopolitical zones of Nigeria. The description and analysis of the data obtained shows the actual attitude of the respondents to the ongoing processes.

Results: international regulation and national legislation on electronic payments in force in Nigeria were examined. The study revealed that e-payments are an effective means of transactions but there are some legal challenges that may hinder the smooth use of e-payments in Nigeria. It was found that although the country has enacted a number of laws relating to the regulation of banking and other financial activities, they are not sufficient to address the challenges posed by modern technologies. The article reflects

✉ Corresponding author

the issues of electronic signature, trust in technology, data privacy, security of electronic transactions, fraud, authentication and authorization, certainty of rights and obligations, jurisdiction and platforms for resolving online disputes, taxation of electronic payments, and others. The authors note that the task of creating a secure digital environment for the smooth operation of e-commerce and e-payments in Nigeria should not be solely imposed on the government.

Scientific novelty: by the example of one of the most promising African states, the authors revealed a spectrum of issues related to the work of electronic payment systems, supporting it with a survey of public opinion. They managed to find out the citizens' attitude to a number of issues that are most often faced when using the system of electronic payments, and possible areas of change.

Practical significance: the current legal issues raised in the study largely hinder the smooth use of the electronic payment system in Nigeria. Hence, the possible ways to improve it suggested by the authors are increasingly significant.

For citation

Haruna, I. O., Aidonojie, P. A., & Beida, O. J. (2024). Prospects and Issues Concerning the Regulatory Regime of E-Payment System in Nigeria. *Journal of Digital Technologies and Law, 2*(2), 372–393. https://doi.org/10.21202/jdtl.2024.19

References

Abubakar, A. S., & Adebayo, F. O. (2014). Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects. *Mediterranean Journal of Social Sciences*, *5*(2), 215. https://doi.org/10.5901/mjss.2014.v5n2p215

Acha, I. A. (2008). Electronic Banking in Nigeria: Concept, Challenges and Prospects. *International Journal of Development and Management Review*, *3*(1), 23–45.

Adkomolede, T. (2008). Contemporary Legal Issues on Electronic Commerce in Nigeria. *Potchefstroom Electronic Law Journal*, *11*(3) 9–18. https://doi.org/10.4314/pelj.v11i3.42234

Adkwodimmah, C., & Ochei, A. I. (2019). Financial Technology and Liquidity in the Nigerian Banking Sector. *Journal of Association of Professional Bankers in Education*, *5*(1), 243–162.

Aguda, O. O. (2021). An Appraisal of the Legal Framework for Online Banking in Nigeria and South Africa. *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law*, *3*(1), 11–17.

Aidonojie, P. A., & Ong Argo, V. (2022). The Societal and Legal Missing Link in Protecting a Girl Child against abuse before and Amidst the Covid-19 Pandemic in Nigeria. *Jurnal Hukum UNISSULA*, *38*(1), 61–80. http://dx.doi.org/10.26532/jh.v38i1.18412

Dupas, P., Karlan, D., Robinson, J., & Ubfal, D. (2018). Banking the Unbanked? Evidence from Three Countries. *American Economic Journal: Applied Economics*, *10*(2), 257–297. https://doi.org/10.1257/app.20160597

Ezike, E. O. (2013). Online Contracts in Nigeria –An Overview. *The Nigerian Juridical Review*, *11*, 53–82.

Gabor, D., & Brooks, S. (2017). The Digital Revolution in Financial Inclusion: International Development in the Fintech Era. *New Political Economy*, *22*(4), 423–436. https://doi.org/10.1080/13563467.2017.1259298

Iriobe, G., & Akinyede, O. M. (2017). The Effect of Financial Technology Services on Banks Customers Satisfaction in Nigeria. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2984215

Jessah, J. E. (2019). E-Commerce in Nigeria: Liability for Loss or Damage to Goods Supplied by a Seller Pursuant to an Electronic Contract. *IJOCLLEP*, *1*(3), 105–114.

Laven, M., & Bruggink, G. (2016). How FinTech is transforming the way money moves around the world. *Journal of Payments Strategy & Systems*, *10*(1), 6–12.

Majekodunmi, T. A., Akintola, J. O., Aidonojie, P. A., Ikubbanni, O. O., & Oyebade, A. A. (2022). Legal Issues in Combating the Scourge of Terrorism; Its Impact on International Trade and Investment: Nigeria as a Case Study. *KIU Journal of Humanities*, *7*(3), 129–139.

Omoyajowo, K. (2021). Crowdfunding Regulatory Framework in Nigeria: An Appraisal of the Highlights of SEC Crowdfunding Regulation. *SSRN Electronic Journal*.

Sobehart, J. R. (2016). The FinTech revolution: Quantifying earnings uncertainty and credit risk in competitive business environments with disruptive technologies. *Journal of Risk Management in Financial Institutions*, *9*(2), 67–78.

Sokołowska, E. (2015). Innovations in the payment card market: The case of Poland. *Electronic Commerce Research and Applications*, *14*(5), 292–304. https://doi.org/10.1016/j.elerap.2015.07.005

Tasneem, F. (2014). Legal Effect of Electronic Contracts in Australia. *Global Research Journal of Engineering, Technology and Innovation*, *3*(1), 020–026.

Udobi-Owoloja, P. I., Ahigbe, B. E., Ubi, A. E., Gbajumo-Sheriff, M. A., & Umoru, B. (2020). Digital Banking and Bank Profitability in Nigeria. *Nigerian Journal of Management Studies*, *20*(2), 24–34.

Zhaohui, L. (2012). Motivation of Virtual Goods Transactions Based on the Theory of Gaming Motivations. *Journal of Theoretical and Applied Information Technology*, *43*(2), 254–260.

Authors informations

Ismaila Ozovehe Haruna – LLB, BL, LL.M, PGDE, Long Essay Coordinator Faculty of Law, Prince Abubakar Audu University, Anyigba – Nigeria
Address: P.M.B 1008 Anyigba, Kogi State, Nigeria
E-mail: Ozovehe.ih@ksu.edu.ng
ORCID ID: https://orcid.org/0009-0006-8773-768X
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=8xkClmoAAAAJ

Paul Atagamen Aidonojie – PhD, Associate Dean of Research Kampala International University, Uganda
Address: Box 20000, Ggaba Road, Kansanga, Kampala, Uganda
E-mail: paul.aidonojie@kiu.ac.ug
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Onivehu Julius Beida – PhD, Head of Department, Public & Private Law, Faculty of Law, Bingham University Karu, Nasarawa State
Address: Bingham University P.M.B 005, KM 26 Abuja- Keffi Expressway Kodope , Karu, Nassarawa State, Nigeria
E-mail: beida.onivehu@binghamuni.edu.ng
ORCID ID: https://orcid.org/0000-0002-6089-5059
Google Scholar ID: https://scholar.google.com/citations?user=fxTBqIMAAAAJ

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 – September 22, 2023
Date of approval – October 21, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.727:004.5
EDN: https://elibrary.ru/gbfhor
DOI: https://doi.org/10.21202/jdtl.2024.20

Социально-правовые риски шерентинга в процессе формирования цифровой идентичности ребенка в социальных сетях

Франциско Хосэ Аранда Серна

Католический университет Мурсии, Мурсия, Испания

Ключевые слова

веб-платформы,
неприкосновенность частной жизни,
персональные данные,
права ребенка,
право,
социальные сети,
цифровая идентичность,
цифровая конфиденциальность,
цифровые технологии,
шерентинг

Аннотация

Цель: определить правовые последствия шерентинга как деятельности, которая ставит под угрозу основные права несовершеннолетних, подвергая риску их частную жизнь.

Методы: проведенное исследование строится прежде всего на анализе европейского и американского опыта законодательного регулирования, который излагается в сравнительно-правовом аспекте с применением доктринальных подходов и концепций, получивших отражение в научных публикациях по данной теме. Это способствовало в том числе критическому осмыслению выявленных рисков, а также представлению существующих правовых подходов и формулированию предложений, направленных на защиту неприкосновенности частной жизни несовершеннолетних в социальных сетях.

Результаты: изучено влияние социальных сетей на права несовершеннолетних в части негативного их воздействия, возможных рисков и распространения социальных конфликтов. Осуществлен анализ основных положений законодательства Испании, Франции и США с целью выявления ключевых моментов относительно деятельности несовершеннолетних в социальных сетях и сети Интернет, необходимости выражения ими согласия на опубликование личной информации. Описаны наиболее распространенные конфликты, обусловленные шерентингом, и возможные гибкие законодательные решения споров, касающихся семейных отношений и связанных с деятельностью в социальных сетях. Сформулированы предложения по разрешению конфликтных ситуаций и проблемы цифровой идентичности, возникающих в процессе шерентинга в случае злоупотребления.

Научная новизна: представленное исследование обобщает различные научные точки зрения и правовые подходы к шерентингу как новому феномену, который быстро развивается в связи с широкой популярностью социальных сетей и интернет-активностью детей и их родителей, порождая социально-правовые конфликты.

Практическая значимость: представленное исследование показывает, что несовершеннолетние особенно уязвимы в информационно-телекоммуникационном пространстве. Во многих случаях чрезмерное раскрытие их личных данных происходит не только из-за их собственных действий, но и из-за действий членов их семей, как правило, родителей. Сравнительно-правовое исследование принятых законодательных мер и их интерпретаций в правовой доктрине позволяет охарактеризовать современную правовую ситуацию в отношении несовершеннолетних в цифровом пространстве как фрагментарную и предложить законодательные подходы и решения, позволяющие избежать или минимизировать возможные конфликтные ситуации и риски, такие как цифровое преследование или нарушение права на неприкосновенность частной жизни, которые могут возникать в процессе дальнейшего развития технологий и распространения шерентинга.

Для цитирования

Аранда Серна, Ф. Х. (2024). Социально-правовые риски шерентинга в процессе формирования цифровой идентичности ребенка в социальных сетях. *Journal of Digital Technologies and Law*, *2*(2), 394–407. https://doi.org/10.21202/jdtl.2024.20

Содержание

Введение

Несовершеннолетние пользуются социальными сетями, рассматривая их как возможные инструменты для реализации некоторых своих интересов, будь то личных или социальных. В отличие от взрослых для несовершеннолетних социальные сети имеют жизненно важное значение, поскольку подтверждают их собственное существование. Неучастие в этом виртуальном пространстве означает для них маргинализацию в социальных отношениях. Однако Интернет является относительно враждебной средой; хотя он также служит местом для построения и укрепления социальных отношений, в нем возникает множество социально-правовых конфликтов, среди которых цифровое преследование или нарушение права на неприкосновенность частной жизни (Marcelino Mercedes, 2015; Memedovich et al., 2024; Ahmed et al., 2023; Mola et al., 2023).

Одной из причин этих конфликтов является то, что, когда пользователь Интернета публикует свое изображение или какие-либо персональные данные, он автоматически теряет контроль над ними, поскольку другие пользователи могут получить

доступ к этой информации и затем поделиться ею. Во многих случаях сами родители игнорируют риски ненадлежащего использования Интернета их детьми, хотя весь контент, размещенный в Сети, может быть обращен против них (Durán Alonso, 2022).

Сложностей добавляет растущий феномен несовершеннолетних «инфлюенсеров», которые не только загружают контент в социальные сети, но и получают за это деньги. В последние годы они профессионализировались и стали рассматривать социальные сети как коммерческие и рекламные платформы, поэтому контент создается целенаправленно для привлечения подписчиков и коммерческих брендов (Jiménez-Iglesias et al., 2022).

Особого внимания заслуживает проблема, получившая название «шерентинг» (sharenting, от английских слов share – «делиться» и parenting – «родительство»). Это быстро развивающееся явление состоит в размещении в социальных сетях всевозможной информации о несовершеннолетних (особенно их фотографий и видеозаписей) их родителями, которые выступают в качестве цифровых менеджеров своих детей (Ferrara et al., 2023; Kopecky et al., 2020). Как и в случае с «инфлюенсерами», родители получают финансовую выгоду, выкладывая контент о своих детях (García García, 2021).

1. Понятие шерентинга и его причины

Шерентинг – это деятельность по распространению фотографий, видеозаписей и комментариев в социальных сетях, содержанием которых являются повседневные или интимные моменты жизни несовершеннолетних детей, их родителями или другими близкими родственниками. Это явление связано с широкой популярностью социальных сетей. Оно, очевидно, дает родителям много преимуществ, таких как получение одобрения (через комментарии или лайки), но может быть потенциально опасным, поскольку при этом происходит постоянная передача больших объемов информации, которая должна оставаться в сфере частной жизни (Ordoñez Pineda & Calva Jiménez, 2020; Aydogdu et al., 2023).

Причины, по которым родители выкладывают весь этот контент в Сеть, могут быть самыми разными: иногда – просто создать альбом с фотографиями и видеороликами, чтобы поделиться с родственниками. Учитывая природу социальных сетей, одним из мотивов может быть создание хорошего имиджа родителей или налаживание сотрудничества с другими семьями. В других случаях цель экономическая, поскольку в обмен на распространение контента родители получают денежное или натуральное вознаграждение (в виде спонсорской помощи, подарков и т. д.) (Azurmendi et al., 2021).

Последняя цель в наибольшей степени обращает на себя внимание закона, поскольку с психологической точки зрения шерентинг – это представление тревог и подавленных надежд родителей через детей в цифровой форме. Это становится очевидным, когда контент монетизируется, поскольку в этом случае образы детей оказываются связанными с профессиональным развитием родителей, и в еще большей степени – когда эта деятельность является единственным источником заработка в семье (Ranzini et al., 2020).

Родители как представители семьи и лица, несущие совместную ответственность за цифровую идентичность своих детей, обязаны защищать их права. В первую очередь следует различать особенности распространения контента на разных

платформах. Выложить фотографии в семейную группу в WhatsApp – совсем не то же самое, что выложить их на таких цифровых платформах, как Instagram* или YouTube**. Информация может публиковаться в частном режиме, когда доступ имеет ограниченная группа (семья), или в публичном режиме, с предоставлением доступа всем желающим (Montoro López, 2022).

Распространение видео и фотографий может иметь серьезные негативные последствия для личностного развития ребенка (Yiseul Choi & Lewallen, 2017).

2. Социальные сети как причина шерентинга

Социальные сети – важнейшее технологическое явление последних двадцати лет. Однако сама концепция не так нова, как можно подумать: хотя сегодня это понятие действительно относится к веб-платформам, на которых пользователи общаются друг с другом, ранее оно обозначало просто сообщества, которые были связаны каким-либо образом, например, дружбой, работой или другими ценностями (Oliva Marañón, 2012; Yang et al., 2022; Verswijvel, et al., 2019).

Все существующие социальные сети можно классифицировать по их направленности:

– социальные сети личного характера, например, Facebook*** и Twitter****.

– профессиональные социальные сети, например, LinkedIn*****.

– тематические социальные сети, например, YouTube** и Instagram*.

Можно было бы сказать, что первая категория является основной в плане «семейного» присутствия и распространения шеретинга, однако это нецелесообразно, поскольку границы между сетями в отношении их направленности очень размыты.

Так, на YouTube** есть тематические каналы (кино, фотография и т. д.), но также есть и «семейные» каналы, где выкладываются видео повседневной жизни несовершеннолетних, причем некоторые из них могут быть даже монетизированы.

Влияние YouTube** на несовершеннолетних очень велико, поэтому многие бренды заинтересованы в рекламе на каналах, где присутствуют дети. Это происходит по нескольким причинам; одна из них заключается в том, что семейные каналы и каналы с детьми вызывают большее доверие к демонстрируемой продукции, а это, в свою очередь, заставляет несовершеннолетних пользователей стремиться к ее потреблению (Durán Alonso 2022).

То же самое можно сказать и об Instagram*. Это приложение появилось в 2010 г. с единственной целью – делиться профессиональными фотографиями, однако в 2018 г. благодаря своим функциям (сториз, хэштеги, более эффективное распространение контента) стало крупной социальной сетью. В настоящее время она занимает первое место по количеству активных профилей среди других социальных сетей, особенно среди молодежи (Bard Wigdor & Magallanes Udovicih, 2021).

Эти социальные сети нельзя рассматривать как изолированные площадки; контент часто является мультиплатформенным, и гораздо чаще пользователи используют две или более социальных сетей одновременно, чем ограничиваются одной. В этой сфере несовершеннолетние – наиболее уязвимая группа, и достижение баланса между развитием технологий и защитой частной жизни представляет серьезную проблему.

3. Правовые подходы и меры по защите несовершеннолетних в социальных сетях

Несовершеннолетние пользуются особой защитой в области основных прав человека: по общему правилу, любое вмешательство в вопросы достоинства, частной жизни или идентичности требует явно выраженного согласия.

Несовершеннолетние обладают ограниченной дееспособностью, поэтому испанский Основной закон 1/1996 о правовой защите несовершеннолетних гласит, что их дееспособность толкуется ограничительно и всегда в интересах несовершеннолетнего. В нем также установлен критерий достаточной зрелости (достижение возраста четырнадцати лет), когда несовершеннолетний может самостоятельно осуществлять свои права (Durán Alonso, 2022).

Проблема заключается в том, что в отношении несовершеннолетних не существует единого режима: Основной закон о защите данных устанавливает возрастной критерий в отношении обработки данных, в то время как Гражданский кодекс Испании придает большее значение согласию по договоренности. Например, в случае с несовершеннолетним, достигшим возраста достаточной зрелости, такое согласие должен дать сам несовершеннолетний; однако, как мы увидим, большинство случаев шерентинга затрагивает детей очень раннего возраста (Toral Lara, 2020).

При этом многие правоведы понимают, что независимо от того, достиг несовершеннолетний возраста достаточной зрелости или нет, родители при осуществлении своих родительских прав должны всегда защищать личностные активы несовершеннолетнего. Прокуратура может инициировать официальные действия, если сочтет, что конфиденциальность частной жизни и другие права несовершеннолетнего были нарушены (De Lama Aymá, 2006).

Пионером в области защиты детей младше тринадцати лет стали Соединенные Штаты, приняв в 1998 г. Закон о защите частной жизни детей в Интернете (Children's Online Privacy Protection Act, COPPA Act), который обязал цифровые платформы использовать методы обеспечения согласия несовершеннолетних. Так, во исполнение этого закона платформа YouTube** классифицирует и идентифицирует контент, направленный на несовершеннолетних, и не собирает персональные данные этой аудитории (Durán Alonso, 2022).

Хорошим примером является также Франция, где в 2020 г. был принят Закон 2020/1266 о защите от коммерческого использования изображений несовершеннолетних в возрасте до шестнадцати лет. Он устанавливает ограничения в отношении графика совместимости между временем учебы и записи, а также предусматривает право на забвение, включая меры, регулирующие такое право несовершеннолетних. Последнее заключается в том, что социальные сети могут удалять контент несовершеннолетних по их просьбе, даже невзирая на разрешение родителей (Cremades García, 2021).

В Испании публикация изображений должна осуществляться с согласия несовершеннолетнего старше четырнадцати лет; до достижения этого возраста необходимо согласие обоих родителей. В случае открытия аккаунта в социальной сети несовершеннолетний обязательно должен быть старше 14 лет, поскольку создание аккаунта подразумевает официальное оформление договора и разрешение на обработку данных, которые могут противоречить требованиям защиты достоинства, частной жизни и идентичности (Santos Morón, 2011).

Согласие всегда должно быть конкретным и информированным; кроме того, необходимо понимать, с какой целью и как будут использоваться данные. Родители не должны вмешиваться в деятельность своих детей в социальных сетях, за исключением случаев, когда они обязаны делать это по закону для защиты интересов ребенка. В этом случае необходимо получить согласие, а судебное разрешение потребуется только в том случае, если речь идет о серьезном вмешательстве в основные права (Toral Lara, 2020).

4. Проблема переноса цифровой идентичности: злоупотребления в процессе шерентинга

Все больше и больше родителей практикуют шерентинг с целями, выходящими за рамки обмена информацией внутри семьи или круга друзей. Крупные виртуальные платформы облегчают существование каналов с семейным контентом и их использование с бизнес-целями. Это происходит отчасти потому, что это выгодно для спонсоров рекламы, а также потому, что создатели такого контента могут получать денежную прибыль (García García, 2023).

Иногда шерентинг предполагает участие несовершеннолетних в качестве главных героев или соавторов совместно с родителями в видео различного содержания. Некоторые исследователи определяют такую форму как злоупотребление. При этом согласие родителей в принципе не вызывает сомнений, поскольку в подавляющем большинстве случаев очевидна руководящая роль одного из них (Azurmendi et al., 2021).

Бизнес-модель в таких случаях может строиться различными способами:

– монетизация блога, аккаунта в социальной сети или семейного YouTube**-канала;

– оплата за размещение рекламы, получение спонсорской помощи или подарков от рекламодателей;

– профессиональное занятие какой-либо деятельностью в Интернете (например, ведение канала на YouTube**) (Azurmendi et al., 2021).

В отличие от других виртуальных видов деятельности, в которые вовлечены только взрослые, в случае шеретинга подразумевается, что цифровая идентичность родителей неразрывно связана с идентичностью их детей. Поэтому некоторые родители стремятся индивидуализировать свою цифровую идентичность и перенести ее на своих детей. Другие же придерживаются концепции родственной идентичности, когда личности родителя и ребенка сближаются между собой (Holiday et al., 2020).

Одной из целей активного и постоянного участия в социальных сетях является стремление к личностной значимости и одобрению со стороны других пользователей. Аналогично происходит в случае с родителями, однако при участии детей проблема заключается в том, что эта цифровая идентичность подвергается искажению. Можно привести множество примеров, когда личный бренд родителей накладывает свой отпечаток, будь то в силу экономической или иной мотивации. Это происходит потому, что в социальных сетях родители самопрезентуют себя через своих детей даже бессознательно.

Эта деятельность наносит вред детям, поскольку формирует их в качестве объекта для получения подтверждения «цифрового я» родителей или не более чем их продолжения. Более того, такая самопрезентация не ограничивается социальными сетями и цифровым пространством, а продолжается и за его пределами (Blum-Ross & Livingstone, 2017).

При этом дети выступают в качестве не более чем средства для достижения родительских чаяний, признания и успеха. Вредное воздействие проявляется, когда родители публикуют информацию, связанную со здоровьем детей, или другие личные данные, такие как местоположение, интимные подробности, или непосредственно занимаются продвижением и рекламой, что можно квалифицировать как эксплуатацию (Moser et al., 2017).

В ряде работ было показано, что в случаях значительного участия несовершеннолетних вступает в силу ряд факторов, которые усиливают или ослабляют шерентинг:

– другие члены семьи могут выступать в роли критиков родителей в отношении коммерциализации несовершеннолетних или усиливать шерентинг помимо участия родителей (Jiménez-Iglesias et al., 2022);

– существенным фактором могут стать комментарии потребителей такого рода контента, которые часто критически относятся к коммерциализации несовершеннолетних.

Широкое распространение злоупотреблений в процессе шерентинга позволяет предположить, что он будет оказывать значительное влияние на формирование цифровой идентичности несовершеннолетних, особенно если они становятся главными действующими лицами на таких семейных площадках с самого раннего возраста.

В настоящее время, даже если несовершеннолетний согласен на участие в этих видеороликах и доволен их реализацией, на самом деле он не может понимать их долгосрочных последствий. Большинство судебных споров обусловлено именно режимом монетизации шерентинга (Azurmendi et al., 2021).

Даже отдельные конфликты показывают, какой вред могут нанести злоупотребления в процессе шерентинга. Однако современная реальность такова, что многие родители привыкли почти автоматически выкладывать любые фотографиями и видеозаписи, что может негативно повлиять на отношения между родителями и детьми, а также на формирование цифровой идентичности ребенка. При монетизации такого контента возникает ощущение абсолютного отсутствия уважения к правам ребенка (Azurmendi et al., 2021).

Заключение

Интернет и социальные сети стали одним из величайших достижений современного общества, однако они также представляют собой одну из самых больших опасностей в отношении защиты персональных данных и прав человека, в частности, права на неприкосновенность частной жизни. Эта опасность еще более велика в отношении защиты данных и цифровой конфиденциальности несовершеннолетних, так как существование в цифровой среде требует определенной зрелости и знаний для обеспечения тайны личной жизни.

Представленное исследование показывает, что несовершеннолетние особенно уязвимы в пространстве социальных сетей. Во многих случаях чрезмерное раскрытие их личных данных происходит не только из-за их собственных действий, но и из-за действий членов их семей, как правило, родителей.

Современная правовая ситуация в отношении несовершеннолетних в Интернете несколько фрагментарна, но изучение законодательной базы позволяет обозначить ряд аспектов. Так, существует две категории несовершеннолетних: достигшие возраста достаточной зрелости и не достигшие его. Первые могут самостоятельно управлять своей деятельностью в социальных сетях и в целом имеют больше механизмов для выражения своего мнения в случае злоупотреблений в процессе шерентинга.

Ключом к разрешению этих конфликтов является необходимость обеспечить надлежащую подготовку не только несовершеннолетних, но и их родителей и опекунов, а также педагогов, поскольку во многих случаях их действия основаны на незнании возможных последствий необдуманной публикации контента в Интернете. Важно, чтобы и несовершеннолетние, и взрослые были должным образом подготовлены и знали о соответствующих рисках; это обеспечит ответственное и безопасное использование Интернета.

Необходимо, чтобы правовая база способствовала развитию, прежде всего на международном уровне. Это также предполагает ограничение опасной и выходящей за рамки общественной пользы деятельности, особенно в случаях, когда на первый план выступают экономические соображения и несовершеннолетний становится объектом использования.

Законы должны отражать все меры защиты, рекомендуемые общественными организациями, а также некоторые меры, которые уже применяются в других правовых системах, например в Соединенных Штатах. Это позволит создать правовой режим, обеспечивающий надлежащую и достаточную защиту такой уязвимой группы, как несовершеннолетние.

---

* Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.
** Иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации.
*** Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.
**** Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.
***** Социальная сеть, заблокированная на территории Российской Федерации.

Список литературы

Ahmed, H., Ekman, L., & Lind, N. (2023). Planned Behavior, Social Networks, and Perceived Risks: Understanding Farmers' Behavior toward Precision Dairy Technologies. *Journal of Dairy Science*. https://doi.org/10.3168/jds.2023-23861

Memedovich, A., Orr, T., Hollis, A., Salmon, C., Hu, J., Zinszer, K., Williamson, T., & Beall, R. F. (2024). Social network risk factors and COVID-19 vaccination: A cross-sectional survey study. *Vaccine*, *42*(4), 891–911. https://doi.org/10.1016/j.vaccine.2024.01.012

Aydoğdu, F., Güngör, B. Ş., & Öz, T. A. (2023). Does sharing bring happiness? Understanding the sharenting phenomenon. *Children and Youth Services Review*, *154*, 107122. https://doi.org/10.1016/j.childyouth.2023.107122

Azurmendi, A., Etayo, C. & Torrell, A. (2021). Sharenting y derechos digitales de los niños y adolescentes. *Elprofesional de la información*, *30*(4), 1–10. https://doi.org/10.3145/epi.2021.jul.07

Bard Widgor, G. & Magallanes Udovicich, M. L. (2021). Instagram*: La búsqueda de la felicidad desde la autopromoción de la imagen. *Culturales*, *9*, 1–29. https://doi.org/10.22234/recu.20210901.e519

Blum-Ross, A. & Livingstone, S. (2017). "Sharenting", parent blogging, and the boundaries of the digital self. *Popular Communication*, *15*(2), 110–125. https://doi.org/10.1080/15405702.2016.1223300

Cremades García, P. (2021). Futuro profesional de los menores y ejercicio de la patria potestad. *Revista Boliviana de Derecho*, *32*, 252–277.

De Lama Aymá, A. (2006). *La protección de los derechos de la personalidad del menor de edad*. Valencia: Tirant lo Blanch.

Durán Alonso, S. (2022). "Mom, I Want to Be a Youtuber": an Unregulated Reality. VISUAL REVIEW. *International Visual Culture Review Revista Internacional De Cultura Visual*, *10*(3), 1–14. https://doi.org/10.37467/revvisual.v9.3601

Ferrara, P., Cammisa, L., Corsello, G., Giardino, I., Vural, M., Pop, T. L., Pettoello-Mantovani, C., Indrio, F., & Pettoello-Mantovani, M. (2023). Online "Sharenting": The Dangers of Posting Sensitive Information About Children on Social Media. *The Journal of Pediatrics*, *257*. https://doi.org/10.1016/j.jpeds.2023.01.002

García García, A. (2021). La protección digital del menor: el fenómeno del sharenting a examen. *Revista de derecho UNED*, *27*, 455–492. https://doi.org/10.5944/rduned.27.2021.31094

García García, R. (2023). La responsabilidad social corporativa como herramienta para la consecución de la igualdad de género en cadenas globales de valor. *Temas Laborales: Revista andaluza de trabajo y bienestar social*, *167*, 209–246.

Holiday, S., Norman, M. S., & Densley, R. L. (2022). Sharenting and the extended self: Self-representation in parents' Instagram* presentations of their children. *Popular Communication*, *20*(1), 1–15. https://doi.org/10.1080/15405702.2020.1744610

Jiménez Iglesias, E., Elorriaga Illera, A., Monge Benito, S. & Olabarri Fernández, E. (2022). Exposición de menores en Instagram*: instamadres, presencia de marcas y vacío legal. *Revista Mediterránea de Comunicación*, *13*(1), 51–63. https://doi.org/10.14198/medcom.20767

Kopecky, K., Szotkowski, R., Aznar-Díaz, I., & Romero-Rodríguez, J.-M. (2020). The phenomenon of sharenting and its risks in the online environment. Experiences from Czech Republic and Spain. *Children and Youth Services Review*, *110*, 104812. https://doi.org/10.1016/j.childyouth.2020.104812

Marcelino Mercedes, G. V. (2015). Migración de los jóvenes españoles en redes sociales, de Tuenti a Facebook** y de Facebook** a Instagram*. La segunda migración. *Revista de Comunicación y Tecnologías Emergentes*, *13*(2), 48–78. https://doi.org/10.7195/ri14.v13i2.821

Mola, L., Kaminska, R., Richebé, N., & Carugati, A. (2023). Social strategies for information technology adoption: Social regulation process of mandated enterprise social network systems. *Technological Forecasting and Social Change*, *192*, 122570. https://doi.org/10.1016/j.techfore.2023.122570

Montoro López, A. (2022). Alcance de la fiscalidad como herramienta de la Política Ambiental de la Unión Europea: Los impuestos ambientales y su eficacia como instrumento de protección ambiental. Human Review. *International Humanities Review*, *2*(14), 1–15. https://doi.org/10.37467/revhuman.v11.4105

Moser, C., Chen, T., & Schoenebeck, S. Y. (2017). Parents' and children's preferences about parents sharing about children on social media. *Proceedings of the 2017 CHI Conference on Human Factos in Computing Systems*, 5221–5225. https://doi.org/10.1145/3025453.3025587

Oliva Marañon, C. (2012). Redes sociales y jóvenes: una intimidad cuestionada en Internet. *Aposta: Revista de ciencias sociales*, *54*, 1–16.

Ordoñez Pineda, L. & Calva Jimenez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. *Revista Chilena de Derecho y Tecnología*, *9*(2), 105–130. https://doi.org/10.5354/0719-2584.2020.55333

Ranzini, G., Newlands, G. & Lutz, C. (2020). Sharenting, Peer Influence, and Privacy Concerns, A Study of Instagram-Sharing Behaviors of Parents in the United Kingdom. *Social Media + Society*, *6*(4), 1–13. https://doi.org/10.1177/2056305120978376

Santos Morón, M. (2011). Menores y derechos de la personalidad. La autonomía del menor. *AFDUAM: Anuario de La Facultad de Derecho de la Universidad Autónoma de Madrid*, *15*, 63–93. http://hdl.handle.net/10486/662984

Toral Lara, E. (2020). Menores y redes sociales: consentimiento protección y autonomía. *Derecho Privado y Constitución*, *36*, 179–218. https://doi.org/10.18042/cepc/dpc.36.05

Verswijvel, K., Walrave, M., Hardies, K., & Heirman, W. (2019). Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review*, *104*, 104401. https://doi.org/10.1016/j.childyouth.2019.104401

Yang, M., Chen, H., Long, R., & Yang, J. (2022). The impact of different regulation policies on promoting green consumption behavior based on social network modeling. *Sustainable Production and Consumption*, *32*, 468–478. https://doi.org/10.1016/j.spc.2022.05.007

Yiseul Choi, G. & Lewallen, J. (2017). Say Instagram*, Kids!: examining Sharenting and Children Digital Representations on Instagram. *Howard Journal of Communications*, *29*(2), 144–164. https://doi.org/10.1080/10646175.2017.1327380

---

* Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

** Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Сведения об авторе

Аранда Серна Франциско Хосэ – PhD в области юриспруденции, доцент, факультет права, Католический университет Мурсии
Адрес: 30107, Испания, Мурсия, Гваделупа-де-Макиаскок, авеню де лос Херонимос, 135
E-mail: fjaranda@ucam.edu
ORCID ID: https://orcid.org/0000-0002-5768-2773
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=58097085200
Google Scholar ID: https://scholar.google.com/citations?user=zrndQAwAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 29 октября 2023 г.
Дата одобрения после рецензирования – 25 ноября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:342.727:004.5
EDN: https://elibrary.ru/gbfhor
DOI: https://doi.org/10.21202/jdtl.2024.20

Social and Legal Risks of Sharenting when Forming a Child's Digital Identity in Social Networks

Francisco José Aranda Serna
Catholic University of Murcia, Murcia, Spain

Keywords

children's rights,
digital identity,
digital privacy,
digital technologies,
law,
personal data,
privacy,
sharenting,
social networks,
web platforms

Abstract

Objective: to determine the legal consequences of sharenting as an activity that threatens the fundamental rights of minors, putting their privacy at risk.

Methods: the study is based primarily on the analysis of European and American experience of legislative regulation, which is presented in a comparative-legal aspect, using doctrinal approaches and concepts reflected in scientific publications on the topic. This contributed, among other things, to the critical understanding of the identified risks and helped to describe the existing legal approaches and formulate proposals aimed at protecting the minors' privacy in social networks.

Results: the impact of social networks on the rights of minors was studied, in terms of their negative influence, possible risks and the spread of social conflicts. The main provisions of the legislation of Spain, France and the USA were analyzed in order to identify the key points regarding the activities of minors in social networks and the Internet, the need for them to express their consent to the publication of personal information. The most common conflicts caused by sharenting were described, as well as possible flexible legislative solutions to disputes concerning family relations and social networking activities. Suggestions were formulated for resolving conflict situations and digital identity issues arising in abusive sharenting.

Scientific novelty: the study summarizes various scientific opinions and legal approaches to sharenting as a new phenomenon, which is rapidly developing due to the wide popularity of social networks and Internet activity of children and their parents, generating socio-legal conflicts.

Practical significance: the research shows that minors are particularly vulnerable in the information and telecommunication environment. In many cases, excessive disclosure of their personal data occurs not only because of their own actions, but also because of the actions of their family members, usually parents. A comparative legal study of the adopted legislative measures and their interpretations in the legal doctrine allows characterizing the current legal situation with regard to minors in the digital space as fragmentary and proposing legislative approaches and solutions to avoid or minimize possible conflict situations and risks, such as digital harassment or privacy violation, which may arise in the process of further technological development and the spread of sharenting.

For citation

Aranda Serna, F. J. (2024). Social and Legal Risks of Sharenting when Forming a Child's Digital Identity in Social Networks. *Journal of Digital Technologies and Law, 2*(2), 394–407. https://doi.org/10.21202/jdtl.2024.20

References

Ahmed, H., Ekman, L., & Lind, N. (2023). Planned Behavior, Social Networks, and Perceived Risks: Understanding Farmers' Behavior toward Precision Dairy Technologies. *Journal of Dairy Science*. https://doi.org/10.3168/jds.2023-23861

Memedovich, A., Orr, T., Hollis, A., Salmon, C., Hu, J., Zinszer, K., Williamson, T., & Beall, R. F. (2024). Social network risk factors and COVID-19 vaccination: A cross-sectional survey study. *Vaccine*, *42*(4), 891–911. https://doi.org/10.1016/j.vaccine.2024.01.012

Aydoğdu, F., Güngör, B. Ş., & Öz, T. A. (2023). Does sharing bring happiness? Understanding the sharenting phenomenon. *Children and Youth Services Review*, *154*, 107122. https://doi.org/10.1016/j.childyouth.2023.107122

Azurmendi, A., Etayo, C. & Torrell, A. (2021). Sharenting y derechos digitales de los niños y adolescentes. *Elprofesional de la información*, *30*(4), 1–10. (In Spanish). https://doi.org/10.3145/epi.2021.jul.07

Bard Widgor, G. & Magallanes Udovicich, M. L. (2021). Instagram*: La búsqueda de la felicidad desde la autopromoción de la imagen. *Culturales*, *9*, 1–29. (In Spanish). https://doi.org/10.22234/recu.20210901.e519

Blum-Ross, A. & Livingstone, S. (2017). "Sharenting", parent blogging, and the boundaries of the digital self. *Popular Communication*, *15*(2), 110–125. https://doi.org/10.1080/15405702.2016.1223300

Cremades García, P. (2021). Futuro profesional de los menores y ejercicio de la patria potestad. R*evista Boliviana de Derecho*, *32*, 252–277. (In Spanish).

De Lama Aymá, A. (2006). *La protección de los derechos de la personalidad del menor de edad*. Valencia: Tirant lo Blanch. (In Spanish)

Durán Alonso, S. (2022). "Mom, I Want to Be a Youtuber": an Unregulated Reality. VISUAL REVIEW. *International Visual Culture Review Revista Internacional De Cultura Visual*, *10*(3), 1–14. (In Spanish). https://doi.org/10.37467/revvisual.v9.3601

Ferrara, P., Cammisa, L., Corsello, G., Giardino, I., Vural, M., Pop, T. L., Pettoello-Mantovani, C., Indrio, F., & Pettoello-Mantovani, M. (2023). Online "Sharenting": The Dangers of Posting Sensitive Information About Children on Social Media. *The Journal of Pediatrics*, *257*. https://doi.org/10.1016/j.jpeds.2023.01.002

García García, A. (2021). La protección digital del menor: el fenómeno del sharenting a examen. *Revista de derecho UNED*, *27*, 455–492. (In Spanish). https://doi.org/10.5944/rduned.27.2021.31094

García García, R. (2023). La responsabilidad social corporativa como herramienta para la consecución de la igualdad de género en cadenas globales de valor. *Temas Laborales: Revista andaluza de trabajo y bienestar social*, *167*, 209–246. (In Spanish).

Holiday, S., Norman, M. S., & Densley, R. L. (2022). Sharenting and the extended self: Self-representation in parents' Instagram* presentations of their children. *Popular Communication*, *20*(1), 1–15. https://doi.org/10.1080/15405702.2020.1744610

Jiménez Iglesias, E., Elorriaga Illera, A., Monge Benito, S. & Olabarri Fernández, E. (2022). Exposición de menores en Instagram*: instamadres, presencia de marcas y vacío legal. *Revista Mediterránea de Comunicación*, *13*(1), 51–63. (In Spanish). https://doi.org/10.14198/medcom.20767

Kopecky, K., Szotkowski, R., Aznar-Díaz, I., & Romero-Rodríguez, J.-M. (2020). The phenomenon of sharenting and its risks in the online environment. Experiences from Czech Republic and Spain. *Children and Youth Services Review*, *110*, 104812. https://doi.org/10.1016/j.childyouth.2020.104812

Marcelino Mercedes, G. V. (2015). Migración de los jóvenes españoles en redes sociales, de Tuenti a Facebook** y de Facebook** a Instagram*. La segunda migración. *Revista de Comunicación y Tecnologías Emergentes*, *13*(2), 48–78. (In Spanish). https://doi.org/10.7195/ri14.v13i2.821

Mola, L., Kaminska, R., Richebé, N., & Carugati, A. (2023). Social strategies for information technology adoption: Social regulation process of mandated enterprise social network systems. *Technological Forecasting and Social Change*, *192*, 122570. (In Spanish). https://doi.org/10.1016/j.techfore.2023.122570

Montoro López, A. (2022). Alcance de la fiscalidad como herramienta de la Política Ambiental de la Unión Europea: Los impuestos ambientales y su eficacia como instrumento de protección ambiental. Human Review. *International Humanities Review*, *2*(14), 1–15. (In Spanish). https://doi.org/10.37467/revhuman.v11.4105

Moser, C., Chen, T., & Schoenebeck, S. Y. (2017). Parents' and children's preferences about parents sharing about children on social media. *Proceedings of the 2017 CHI Conference on Human Factos in Computing Systems*, 5221–5225. https://doi.org/10.1145/3025453.3025587

Oliva Marañon, C. (2012). Redes sociales y jóvenes: una intimidad cuestionada en Internet. *Aposta: Revista de ciencias sociales*, *54*, 1–16. (In Spanish).

Ordoñez Pineda, L. & Calva Jimenez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. *Revista Chilena de Derecho y Tecnología*, *9*(2), 105–130. (In Spanish). https://doi.org/10.5354/0719-2584.2020.55333

Ranzini, G., Newlands, G. & Lutz, C. (2020). Sharenting, Peer Influence, and Privacy Concerns, A Study of Instagram-Sharing Behaviors of Parents in the United Kingdom. *Social Media + Society*, *6*(4), 1–13. https://doi.org/10.1177/2056305120978376

Santos Morón, M. (2011). Menores y derechos de la personalidad. La autonomía del menor. *AFDUAM: Anuario de La Facultad de Derecho de la Universidad Autónoma de Madrid*, *15*, 63–93. (In Spanish). http://hdl.handle.net/10486/662984

Toral Lara, E. (2020). Menores y redes sociales: consentimiento protección y autonomía. *Derecho Privado y Constitución*, *36*, 179–218. (In Spanish). https://doi.org/10.18042/cepc/dpc.36.05

Verswijvel, K., Walrave, M., Hardies, K., & Heirman, W. (2019). Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review*, *104*, 104401. https://doi.org/10.1016/j.childyouth.2019.104401

Yang, M., Chen, H., Long, R., & Yang, J. (2022). The impact of different regulation policies on promoting green consumption behavior based on social network modeling. *Sustainable Production and Consumption*, *32*, 468–478. https://doi.org/10.1016/j.spc.2022.05.007

Yiseul Choi, G. & Lewallen, J. (2017). Say Instagram*, Kids!: examining Sharenting and Children Digital Representations on Instagram. *Howard Journal of Communications*, *29*(2), 144–164. https://doi.org/10.1080/10646175.2017.1327380

---

* The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

** The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

Author information

Francisco José Aranda Serna – PhD (Law), Associate Professor, Department of Law, Catholic University of Murcia
Address: Av. de los Jerónimos, 135, 30107 Guadalupe de Maciascoque, Murcia, Spain
E-mail: fjaranda@ucam.edu
ORCID ID: https://orcid.org/0000-0002-5768-2773
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=58097085200
Google Scholar ID: https://scholar.google.com/citations?user=zrndQAwAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – October 29, 2023
Date of approval – November 25, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:34.096:347.211
EDN: https://elibrary.ru/hiqzuj
DOI: https://doi.org/10.21202/jdtl.2024.21

Меры профилактики нарушений авторских прав на создание контента в цифровой среде: опыт Нигерии

Адетуту Дебора Айна-Пелемо ✉
Университет Искупителя, Эде, Нигерия

Итамар Басси
Университет Искупителя, Эде, Нигерия

Глориос Океоген Акподжаро
Университет Искупителя, Эде, Нигерия

Ключевые слова

авторское право,
интернет,
онлайн-контент,
право интеллектуальной собственности,
правовая защита,
профилактика нарушений авторских прав,
социальная сеть,
цифровая платформа,
цифровой маркетинг,
цифровые технологии

Аннотация

Цель: определить уровень защищенности прав авторов контента в социальных сетях и выработать меры профилактики правонарушений в данной области.

Методы: на достижение поставленной цели был направлен социологический и правовой познавательный инструментарий, включающий доктринальный метод исследования предметной области, с получением данных из «первых уст» с учетом воздействующих факторов и обстоятельств. Основные результаты получены при помощи социологического метода, используемого для сбора данных на основе разработанной анкеты, содержащей четыре исследовательских вопроса: (1) каковы представления и мнения третьих лиц или пользователей относительно роли создателя контента; (2) нарушаются ли права создателей контента на их произведения; (3) каковы способы защиты созданного контента от посягательств со стороны платформ; (4) как можно защитить права создателей контента. В основе полученных эмпирических данных и их обобщений находилась комбинация видов анализа, в том числе контент-анализ первичных и вторичных источников права.

Результаты: в последние годы создаваемый в социальных сетях контент превратился в сложную индустрию, которая меняет как традиционное понимание творческого самовыражения, так и реализацию прав интеллектуальной собственности. На примере опыта Нигерии

✉ Контактное лицо

предпринята попытка изучить права и меры защиты, предоставляемые создателям цифрового контента в соответствии с законодательством об интеллектуальной собственности. Как показало исследование, в настоящее время не существует достаточного количества научных работ в этой области или развитого законодательства по защите произведений в социальных сетях. Делается вывод о необходимости совершенствования законодательных актов по защите прав на контент в социальных сетях, в отсутствие которого авторам онлайн-произведений рекомендуется прибегать к более радикальным методам в обеспечении своих прав, чтобы уменьшить количество случаев незаконного присвоения интеллектуальной собственности. Создателям таких произведений предлагается обеспечивать защиту своих прав, основываясь на принципах доктрины добросовестного использования.

Научная новизна: исследование структурировано по исследовательским вопросам, касающимся нарушений и способов защиты прав создателей контента, адресованным респондентам из разных стран, значительная часть которых специализируется преимущественно на создании контента в разных социальных сферах посредством нескольких медиа-платформ и социальных сетей.

Практическая значимость: выводы и рекомендации позволят минимизировать риски нарушения прав интеллектуальной собственности создателей контента, которые могут возникнуть при широком использовании социальных сетей, а также повысить уровень защиты прав на созданное в виде онлайн-контента произведение.

Для цитирования

Айна-Пелемо, А. Д., Басси, И., Акподжаро, Г. О. (2024). Меры профилактики нарушений авторских прав на создание контента в цифровой среде: опыт Нигерии. *Journal of Digital Technologies and Law*, *2*(2), 408–429. https://doi.org/10.21202/jdtl.2024.21

Содержание

Введение

В условиях современного уникального и динамичного мира стремительно развивается сфера интеллектуальной собственности. Ее развитие в правовом поле продвинулось до уровня создания различных конвенций (Zhang & Xu, 2023). Наряду с этим международные организации, такие как Всемирная организация интеллектуальной собственности (ВОИС) и многие другие, внесли свой вклад в развитие права интеллектуальной собственности, углубив его понимание. Художественные, литературные, исполнительские и вещательные произведения также приобретают значительную ценность на рынке труда, поэтому было бы крайне неразумно игнорировать социально-правовые проблемы, которые возникают в связи с ними.

В последние несколько лет после пандемии COVID-19 многие были вынуждены работать удаленно; изменения норм затронули как частных предпринимателей, так и крупные компании (Liu & Zhang, 2024; Aina-Pelemo et al., 2021). В значительной степени возросло использование маркетинга в социальных сетях для достижения целевой аудитории. Это выдвинуло на первый план ту сферу интеллектуальной собственности, которая известна как «создание контента». Хотя создание контента существует так же давно, как и интеллектуальная собственность, новшеством стал формат, который это явление приняло на платформах социальных медиа. Сегодня творческие идеи и процессы распространяются через платформы, которые используются каждый день и являются преимущественно аудиовизуальными. С тех пор репутация производителей онлайн-контента и маркетологов значительно улучшилась, и, по прогнозам, мировой объем рынка инфлюенсер-маркетинга будет только расти (Alvarez-Monzocillo, 2022). В настоящее время на него приходится около 15 % от общего мирового дохода от рекламы.

При этом ожидается, что эта отрасль будет ежегодно расти на 25 % и к концу 2025 г. ее общая рыночная стоимость составит более 22 млрд индийских рупий (268,4 млн долларов США). До пандемии в Индии насчитывалось 400 млн пользователей социальных сетей, однако в результате пандемии их число значительно увеличилось (на 18 %) (Priyanshi, 2022). Эта стоимость оценивается гораздо выше в долларах США.

Создатели контента и агенты влияния помогают брендам охватить более широкую аудиторию. Согласно опросам пользователей Instagram* и других известных социальных сетей, каждый пользователь проводит на этих платформах в среднем два часа в день (Subair et al., 2019). Таким образом, агенты влияния в социальных сетях зарекомендовали себя как ценный инструмент в сфере маркетинга и вносят значительный вклад в расширение компаний, помогая им устанавливать связи с новой аудиторией.

1. Понятие интеллектуальной собственности и создания контента

Интеллектуальная собственность (ИС) – это юридические права, предоставляемые физическим или юридическим лицам на результаты интеллектуальной деятельности, такие как изобретения, литературные и художественные произведения, символы, имена, изображения и дизайны (Aina-Pelemo & Akpojaro, 2024; Saha & Bhattacharya, 2011). Эти права имеют решающее значение для стимулирования инноваций, творчества и экономического роста. В Нигерии законы об интеллектуальной собственности играют важную роль для защиты и развития инноваций и творчества (Owushi, 2020).

Объект интеллектуальной собственности обычно считается нематериальным и может быть воспринят только с помощью зрения или слуха. Исключительные права на использование или владение творческими произведениями, которые предоставляются их создателям, называются правами интеллектуальной собственности (Fatoba, 2019; Lei & Hui, 2023). Как правило, создателю дается исключительное право использовать свое произведение, продавать или отчуждать его по своему усмотрению или предоставлять использование этих прав другим лицам. Это результат интеллектуальной деятельности, и нематериальный носитель такой собственности является одной из причин его уникальности. Результат интеллектуальной деятельности зарождается в голове человека, а затем воплощается в реальные формы. Однако формирование этих идей является продуктом интеллекта. Интеллектуальные способности каждого человека различны, и в результате идеи, даже если они похожи, всегда будут иметь оттенок уникальности, который делает их исключительными.

Создание контента не является исключением; это выражение идей, сформированных интеллектом и мастерством человека, в аудио- и визуальных носителях[1]. Оно определяется как процесс производства и распространения информации через СМИ для достижения определенной аудитории с конкретной целью. В описательных целях создание контента включает также процесс исследования, выдвижения стратегических идей, превращения этих идей в высококачественные материалы и последующего продвижения этих материалов среди целевой аудитории. Этот процесс является продуктом интеллекта человека, называемого создателем. Создатель вкладывает в процесс свои знания и творчество, порождая новые ценности. Это показывает, что создание контента входит в сферу интеллектуальной собственности (Kupers et al., 2019). Обычно контент направлен на маркетинг, рекламу или обмен информацией.

Согласно Kupers et al. (2019), создание контента происходит в основном с помощью аудиовизуальных средств, таких как видеозаписи и фотографии. Внимание и интерес людей возбуждаются посредством слуха и зрения, поэтому аудиовизуальные произведения способны завладеть вниманием гораздо быстрее, чем через любой другой сенсорный механизм. Этим и пользуются создатели контента.

Благодаря социальным сетям мощный эффект от аудиовизуальных работ перешел в совершенно новое измерение. Они позволяют людям общаться друг с другом по всему миру в режиме реального времени. Это разрушает границы часовых поясов и другие препятствия. Фактически авторы могут делиться своими творениями в Интернете и любых социальных сетях по своему выбору; у них также есть возможность охватить тысячи и миллионы людей одновременно как в своих странах, так и за их пределами. Возьмем пример, когда художник проводит выставку в галерее, и ее посещают сто человек. Представьте, что он нанимает создателя контента для создания видеоролика, рассказывающего об экспонатах выставки и о том, почему для художников это отличная возможность посетить выставку и завязать знакомство. Такое видео размещается на странице в социальной сети и ориентировано на художников и любителей искусства. Несомненно, благодаря такому дополнению, продвижение и маркетинг видеоконтента охватит тысячи людей, а общее количество посетителей или зрителей может удвоиться или утроиться. В зависимости от масштаба продвижения результат может оказаться впечатляющим.

[1] Farrington, C. A., McBride, M. R. A., Puller, J., Weiss, E., Maurer, J., Nagaoka, J., Shewfelt, S., & Wright, L. (2019). Arts Education and Social-Emotional Learning Outcomes Among K-12 Students. Developing a theory of Action. UChicago Consortium on School Research.

Именно этим объясняется стремительное развитие индустрии создания контента. Компании, организации и всевозможные корпорации, нацеленные на получение прибыли, расширяются за счет маркетинга. В поисках лучших способов быстро и эффективно достичь своей целевой аудитории они могут нанять создателей контента, которые имеют влияние на определенном рынке, чтобы те продвигали продукт компании среди своей обширной, т. е. целевой, аудитории. Благодаря технологиям создание контента существует сейчас в очень больших масштабах. Кроме того, пандемия COVID-19 заставила предприятия и корпорации искать новые способы продвижения своих товаров и услуг, и рынок создания контента без труда заполнил этот пробел[2]. Исходя из этих объяснений, авторы могут с полным правом сказать, что создание контента – это основа современного цифрового маркетинга.

Ежедневно тысячи и миллионы публикаций распространяются в Интернете по всему миру. Чтобы контент произвел эффект, он должен быть качественным и ценным. Это означает, что автор должен приложить особые усилия для его создания и оформления. Сфера интеллектуальной собственности служит достижению двух основных целей (Afolayan, 2022): во-первых, защищать права создателей объектов интеллектуальной собственности, во-вторых – удовлетворять общественные интересы путем предоставления доступа к широкому спектру произведений и изобретений во многих областях, жизненно важных для благосостояния общества. Эта цель обеспечивает финансовую поддержку творческих проектов, которые приносят пользу обществу в целом.

В Нигерии авторское право в основном регулируется Законом об авторском праве Нигерии от 2022 г. (Nigerian Copyright Act, NCA), который отменил прежний Закон 1988 г. Он предоставляет владельцам авторских прав исключительные права, включая права на воспроизведение, распространение, исполнение и демонстрацию своих произведений. Защита авторских прав начинает действовать автоматически при создании произведения и распространяется на срок жизни автора плюс 70 лет после его смерти[3].

В новый закон были внесены важные изменения, которые призваны оказать влияние на авторов и значительно расширить возможности реализации их прав, особенно в цифровую эпоху. Комиссия по авторскому праву Нигерии (Nigerian Copyright Commission, NCC) получила больше полномочий для эффективного управления и обеспечения соблюдения положений Закона физическими и юридическими лицами (Majekolagbe, 2016). Теперь признано, что аудиовизуальные произведения подлежат охране авторским правом. Также теперь фотография и изобразительное искусство подлежат лицензированию, а моральные права – защите.

В Законе указано, что владелец аудиовизуального произведения должен дать свое согласие на тиражирование, передачу или коммерческое публичное распространение путем продажи или иной передачи права собственности (Nkwor, 2023). Закон также расширяет определение вещания, включая в это понятие распространение аудиовизуального произведения среди широкой публики с помощью проводных или беспроводных средств таким образом, чтобы обеспечить общий доступ с возможностью выбора потребителем места и времени этого доступа.

---

2 Smith, K. (2022). How Covid-19 Increased Influencer Marketing. https://clck.ru/3AQeFW

3 Oloruntade, G. (2023). What Does the New Copyright Law Mean for Nigerian Content Creators? Technext. https://clck.ru/3AQeG9

Под действие указанного Закона подпадает цифровая информация, поскольку он определяет копию как любой вид воспроизведения, включая цифровую копию. Это означает, что владельцы любого рода онлайн-контента, включая создателей контента в социальных сетях, аудио-, видео- и других материалов, защищены против нарушений авторских прав, поскольку их произведения не могут быть использованы без разрешения владельца или авторов (Jerameel, 2021).

Однако в результате расширения рынка социальных сетей творческие работники и агенты влияния на этих платформах сталкиваются с рисками в области прав интеллектуальной собственности. Их права на интеллектуальную собственность должны быть защищены, поскольку на создание оригинального материала затрачивается огромное количество времени и усилий, а на формирование соответствующей аудитории могут уйти годы.

В свете этого в данной работе на примере Нигерии предпринята попытка изучить права и меры защиты, предоставляемые создателям контента в соответствии с законодательством об интеллектуальной собственности. Исследование структурировано в виде ответов на четыре вопроса, которые рассмотрены в соответствующих разделах.

2. Права авторов на произведения, публикуемые на платформах социальных сетей

Права автора на его произведение, опубликованное на платформах социальных сетей, определяются различными факторами. Общее правило заключается в том, что как только творческое произведение публикуется в фиксированном формате, возникает авторское право (Oriakhogba, 2018). Прежде всего, авторские права принадлежат автору в момент создания, за исключением случаев, когда работодатель автора обладает полными или частичными правами на созданное произведение на основании соглашений между сторонами или условий найма (Garcia, 2022). Кроме того, объем прав автора может определяться условиями подписанного им контракта. В ситуации, когда создатель контента заключает соглашение с компанией, условия договора могут также определять объем предоставляемых прав на использование, лицензирование или совместное владение.

После того как автор загружает свою творческую работу в социальные сети, он сохраняет за собой авторские права. Платформа не претендует на право собственности на материал и не имеет права использовать его без согласия автора, но при использовании любой платформы социальных сетей считается, что пользователь соглашается с условиями предоставления услуг, которые часто предоставляют платформе разрешение на использование авторских работ. Это не означает, что сайт может использовать такие работы в своих целях, но он вправе оценивать, удалять или даже ограничивать контент, чтобы выполнять свои условия обслуживания (Reid, 2019). Согласно этим условиям, от пользователей может потребоваться разрешение на использование их работ в целях повышения качества услуг. Ни пользователи, ни веб-менеджер не осуществляют контроль над пользовательским контентом и не имеют права продавать его рекламным агентам. Еще важнее то, что, предоставляя другим пользователям сайта доступ к произведению, веб-менеджер обязан указать авторство его создателей.

По условиям ряда крупных социальных медиаплатформ (например, Instagram*, Twitter**, YouTube***, LinkedIn****, TikTok, Facebook*****, Snapchat, Pinterest и др.), пользователи сохраняют полное право собственности на публикуемый контент, тогда как

платформы лишь предоставляют им площадку для публикации[4]. Тем не менее нахождение произведения на публичном сайте не означает, что оно является общественным достоянием. По сути, в Интернете или в социальных сетях может произойти нарушение права интеллектуальной собственности на произведение, и за любое такое нарушение может быть присуждена компенсация (Fagundes & Perzanowski, 2020).

3. Представление и анализ данных

В этом разделе представлены и проанализированы данные, полученные с помощью анкетирования.

3.1. Выборка и методы исследования

В целях реализации принятой комплексной методологии исследования применялись как качественный, так и количественный подходы. В этой связи для сбора данных использовалась анкета, содержащая несколько исследовательских вопросов: 1. Каковы представления и мнения третьих лиц или пользователей относительно роли создателя контента? 2. Нарушаются ли права создателей контента на их произведения? 3. Каковы способы защиты созданного контента от посягательств со стороны платформ? 4. Как можно защитить права создателей контента?

Опрос проводился с января по март 2023 г. в электронном виде через Instagram*. На вопросы анкеты ответили более 50 авторов контента. Для отбора респондентов в исследовании использовался метод простой случайной выборки, который удачно сочетается с использованием гибридного подхода к правовым исследованиям, а также обладает преимуществами охвата наиболее разнородных группе респондентов и является свободным от предвзятости.

3.2. Анализ данных и результаты

Данные, полученные или сгенерированные на основе проведенного анкетирования, представлены ниже в таблицах.

Результаты социально-демографического исследования представлены в табл. 1. Распределение респондентов по полу показало, что почти все они женщины – 94,2 %, а 5,8 % – мужчины. Распределение респондентов по возрасту показало, что 17,3 % респондентов были в возрасте от 16 до 20 лет, 65,4 % – от 21 до 25 лет, 15,4 % – от 26 до 30 лет и лишь небольшая часть респондентов (1,9 %) были старше 30 лет. Что касается национальности респондентов, то большинство опрошенных (78,9 %) были нигерийцами, по 3,8 % – из Ганы и Албании, по 1,9 % – из Кении, Республики Гамбия, Тринидада, Бразилии и 5,9 % – из Великобритании.

Наибольшее количество респондентов (76,9 %) проживают в Нигерии, 3,8 % – в Гане, 1,9 % заявили, что живут в Сибири или Тринидаде, 3,8 % – в Италии или Соединенных Штатах Америки и 7,7 % – в Великобритании.

[4] Frost, N. (2023). Crediting Sources on Social Media: Why and How to Do It. https://clck.ru/3AQekF

Таблица 1. Социально-демографические характеристики респондентов

Характеристика	Варианты ответов		Количество	%
Пол	Мужской		3	5,8
	Женский		49	94,2
		Всего	52	100,0
Возраст	16–20 лет		9	17,3
	21–25 лет		34	65,4
	26–30 лет		8	15,4
	Старше 30 лет		1	1,9
		Всего	52	100,0
Национальность	Нигериец		41	78,9
	Уроженец Ганы		2	3,8
	Кениец		1	1,9
	Британец		3	5,9
	Тринидадец		1	1,9
	Албанец		2	3,8
	Уроженец Гамбии		1	1,9
	Бразилец		1	1,9
		Всего	52	100,0
Страна проживания	Нигерия		40	76,9
	Гана		2	3,8
	Россия		1	1,9
	Италия		2	3,8
	Тринидад		1	1,9
	Великобритания		4	7,7
	США		2	3,8
		Всего	52	100,0
Область создания контента	Красота		31	59,7
	Стиль жизни		3	5,9
	Мода, образование		1	1,9
	Красота, еда		1	1,9
	Красота/стиль жизни		2	3,8
	Стиль жизни, еда		1	1,9
	Мода, стиль жизни		2	3,8
	Красота, мода		2	3,8
	Стиль жизни, красота		1	1,9
	Красота, мода, стиль жизни		3	5,9
	Стиль жизни, красота, мода		1	1,9
	Красота, стиль жизни, развлечения		2	3,8
	Красота, стиль жизни, образование		1	1,9
	Красота, мода, здоровье, стиль жизни		1	1,9
		Всего	52	100,0

Окончание табл. 1

Характеристика	Варианты ответов	Количество	%
Платформы	YouTube***	2	3,8
	Instagram*	12	23,1
	TikTok	3	5,9
	WhatsApp, Tiktok	1	1,9
	Instagram*, Tiktok	18	34,6
	Instagram*, Tiktok, Facebook*****	5	9,6
	YouTube***, Instagram*, TikTok	4	7,7
	YouTube***, Facebook*****, Instagram*, Tiktok	2	3,8
	Instagram*, Tiktok, Pinterest, YouTube***	3	5,9
	Instagram*,TikTok, Pinterest	2	3,8
	Всего	52	100,0
Почему для вас важно создание контента?	Оно важно, так как занимает мое время и ресурсы.	27	51,9
	Оно важно, так как является источником дохода.	25	48,1
	Всего	52	100,0

Что касается творческих ниш респондентов, то значительная часть из них (59,7 %) специализируется на создании контента, связанного с красотой, 5,9 % пишут о стиле жизни, столько же – о красоте, моде и стиле жизни. Также сообщается, что 3,8 % сосредоточили свое творчество на красоте и стиле жизни, моде и стиле жизни, красоте и моде, а также красоте, стиле жизни и развлечениях. При этом 1,9 % специализировались на комбинированном контенте: о моде и образовании; о красоте и еде; о стиле жизни и еде; о стиле жизни и красоте; о красоте, стиле жизни и развлечениях; о красоте и моде; о здоровье и стиле жизни.

Что касается платформ для творчества, используемых респондентами, 3,8 % сообщили, что используют Youtube***; или одновременно Instagram*, TikTok и Pinterest; или одновременно YouTube***, Facebook*****, Instagram* и Tiktok. Об использовании TikTok сообщили 5,9 % респондентов, столько же используют одновременно Instagram*, Tiktok, Pinterest и YouTube***. Исключительно Instagram* используют 23,1 % респондентов. Небольшое число респондентов (1,9 %) пользуются WhatsApp и TikTok; 34,6 % также используют одновременно Instagram* и TikTok, 9,6 % размещают контент одновременно на платформах Instagram*, TikTok и Facebook*****, а 7,7 % – одновременно на YouTube***, Instagram* и TikTok. Наконец, мы выясняли, насколько актуально для респондентов создание контента. 51,9 % из них подтвердили, что создание контента помогает продуктивно использовать свое время и ресурсы, а 48,1 % согласились с тем, что создание контента является для них источником средств к существованию или дохода.

В таблице 2 представлены ответы респондентов на вопрос о об их отношении к роли создателя контента. Выяснилось, что 21,2 % респондентов принимали меры против тех, кто присвоил или использовал их работу без их согласия; некоторые (3,8 %) не беспокоятся, когда кто-то присваивает или использует их работу без их согласия, в то время как большинство ни разу не сталкивались с этой ситуацией. Также мы обнаружили, что 23,1 % респондентов не могут с уверенностью сказать,

присваивали ли они когда-либо творческие работы других авторов без их согласия или ссылались на них, когда черпали вдохновение в их произведениях или видоизменяли их. При этом большое число респондентов (76,9 %) утверждают, что никогда не присваивали творческие работы других авторов без их согласия или всегда ссылались на них, если вдохновлялись ими или видоизменяли чужие работы.

Таблица 2. Представления и мнения относительно роли создателя контента

Вопрос	Варианты ответов	Количество	%
Я боролся или подавал в суд против лица, присвоившего или видоизменившего мою работу без моего согласия	Нет	39	75,0
	Не знаю	2	3,8
	Да	11	21,2
	Всего	52	100,0
Я присваивал творческое произведение другого автора без его согласия или не ссылался на автора, если вдохновлялся его работой или видоизменял ее	Нет	40	76,9
	Не знаю	12	23,1
	Да	0	0,0
	Всего	52	100,0
Я всегда ссылаюсь на автора оригинальной работы или создателя дизайна и пр., если вдохновляюсь их контентом	Нет	1	1,9
	Мне все равно	12	23,1
	Да	39	75,0
	Всего	52	100,0
Я понимаю, что значит добросовестное использование контента	Нет	14	26,9
	Да	38	73,1
	Всего	52	100,0

Значительная доля респондентов (75 %) указывают, что они всегда ссылаются на создателя оригинального контента, 23,1 % не заботятся об этом, а несколько человек (1,9 %) не делают этого. Наконец, большинство респондентов (73,1 %) подтвердили, что они понимают, что означает добросовестное использование контента, хотя 26,9 % утверждают обратное.

Результаты, приведенные в табл. 3, показывают возможность посягательства на произведения создателей контента. Значительная часть респондентов (55,7 %) считают, что работы создателей контента могут быть присвоены в социальных сетях без каких-либо последствий, 21,2 % не уверены, есть ли какие-либо последствия для присвоения контента в социальных сетях или нет, а 23,1 % не верят, что авторские работы могут быть присвоены в социальных сетях без каких-либо последствий.

Наконец отметим, что значительная доля респондентов (55,8 %) не беспокоятся о том, были ли их работы присвоены и использованы без их согласия в прошлом, а 44,2 % отрицают такую возможность.

Таблица 3. Вероятность нарушения прав создателей контента на их произведения

Вопрос	Варианты ответов	Количество	%
Считаете ли Вы, что творческая работа в социальных сетях может быть присвоена безо всяких последствий?	Нет	12	23,1
	Не знаю	11	21,2
	Да	29	55,7
	Всего	52	100,0
В прошлом моя работа была присвоена или видоизменена без моего согласия	Нет	23	44,2
	Мне все равно	29	55,8
	Да	–	–
	Всего	52	100,0

В таблице 4 представлены ответы респондентов на вопрос о возможных способах защиты созданного контента от посягательств со стороны платформ. Большая часть респондентов (59,6 %) считают, что использование водяных знаков или наличие любой другой формы личного брендинга на творческом произведении, загруженном на платформы социальных медиа, является достаточным для защиты творческих прав на контент, однако 40,4 % придерживаются противоположного мнения.

Таблица 4. Возможные способы защиты контента от посягательств со стороны платформ

Вопрос	Варианты ответов	Количество	%
Считаете ли вы, что для защиты прав автора достаточно водяных знаков или другой формы обозначения личного бренда на произведениях, размещенных в социальной сети?	Нет	21	40,4
	Да	31	59,6
	Всего	52	100,0
Авторское право начинает действовать с момента публикации в фиксированном формате, поэтому регистрировать каждую работу необязательно, однако это обычно рекомендуется. Считаете ли вы, что можете зарегистрировать каждую свою работу?	Нет	21	40,4
	Не знаю	14	26,9
	Да	17	32,7
	Всего	52	100,0
Считаете ли вы, что «присвоения тега автора» достаточно для защиты его прав?	Нет	13	25,0
	Да	39	75,0
	Всего	52	100,0

Оказалось, что 40,4 % респондентов знают о необходимости регистрировать весь созданный ими контент, поскольку им было рекомендовано это делать. Поэтому они обязаны регистрировать свои творческие работы, чтобы обеспечить соблюдение авторских прав, поскольку эти права начинают действовать после того, как произведение опубликовано в фиксированном формате. 26,9 % респондентов не знают о необходимости и пользе регистрации созданных ими материалов, в то время как 32,7 % считают, что регистрация их материалов не является обязательной. Наконец, 75 % респондентов уверены, что «тега автора» достаточно для указания автора произведения, в то время как 25 % считают иначе.

Результаты относительно возможных шагов по защите прав создателей контента представлены в табл. 5. По мнению 42,3 % респондентов, добросовестное использование контента означает признание заслуг создателя произведения; 19,2 % объяснили это понятие как использование созданного создателем контента в первоначальном виде; 3,8 % считают, что добросовестный контент означает воспроизведение той же идеи в собственном контенте без ссылок; 34,6 % объяснили добросовестный контент как использование творческой работы или контента без ущерба для прав автора.

Таблица 5. Возможные шаги для защиты прав создателей контента

Вопрос	Варианты ответов	Количество	%
Что означает принцип добросовестного контента для вас лично как автора?	Признание авторства оригинальной работы	22	42,3
	Использование контента исключительно в том виде, в каком он был первоначально создан	10	19,2
	Использование идеи в моем контенте без ссылки на автора	2	3,8
	Использование произведения или контента без ущерба для его автора	18	34,6
	Всего	52	100,0
Известны ли вам какие-либо законные способы защиты своего контента в социальных сетях?	Нет	18	34,6
	Да	34	65,4
	Всего	52	100,0
Если да, то какие это способы?	Друзья	1	1,9
	Медиа (социальные сети, блоги, видео, статьи и т. д.)	26	50,0
	Формальное образование	7	13,5
	Всего	34	100,0
	Не релевантно	18	–
Знаете ли вы, что нельзя присваивать или видоизменять ваш контент без вашего согласия?	Нет	4	7,7
	Да	48	92,3
	Всего	52	100,0

Достаточно большое количество респондентов (65,4 %) подтвердили, что они знают о законных способах защиты своего контента в социальных сетях, в то время как 34,6 % сообщили, что не осведомлены об этом. Небольшое число респондентов (1,9 %) сообщили, что знают о законных способах защиты своего контента через своих друзей, а значительное число (50 %) указало на средства массовой информации, такие как блоги, видео и статьи в СМИ и другие медиа-платформы, а 13,5 % указали на формальное образование. Наконец, почти все респонденты (92,3 %) подтвердили свою осведомленность о том, что нельзя присваивать авторство на контент, однако 7,7 % не считают это незаконным.

3.3. Обсуждение результатов

Проведенное исследование показало, что создатели контента обладают достаточными знаниями о его добросовестном использовании и часто ссылаются на авторов материалов при их использовании в качестве источника вдохновения для своего собственного контента. Кроме того, создатели контента менее склонны к присвоению работ других авторов без их согласия и во многих случаях не противодействуют тем, кто присваивает созданный ими контент. Поэтому вполне логично, что они положительно относятся к необходимости ссылаться на источник своих идей.

Полученные результаты согласуются с исследованием, проведенным Frost[5] для рекламного агентства на платформе Facebook*****, которые показали, что важно ссылаться на творческие работы других авторов в социальных сетях, так как это создает целостность творческого произведения.

Постулат о том, что работы создателей контента подвергаются посягательствам, считается верным в разумных пределах, поскольку создатели контента знают о возможности присвоения созданного ими контента без каких-либо тяжелых последствий. Авторы также не всегда беспокоятся об этом, поскольку считают, что никаких действий против нарушителей не будет предпринято. Таким образом, можно сделать вывод, что создатели контента уверены в возможности нарушения прав на свои произведения через платформы социальных медиа. Этот вывод согласуется с исследованием, проведенным Nicdao и соавт. (2022), где было обнаружено, что из двадцати пяти создателей контента, столкнувшихся с нарушением авторских прав на свои работы, только двенадцать предприняли шаги, чтобы оспорить незаконное присвоение. Остальные тринадцать авторов не предприняли никаких действий, несмотря на негативный эффект от нарушения их прав. Это указывает на то, что вероятной причиной отказа защиты своих прав на произведения является неопределенность, связанная с их реализацией.

Большинство создателей контента понимают необходимость всегда указывать автора любых материалов, которые они используют как источник вдохновения. Кроме того, защитной мерой является использование водяных знаков и других форм персонального брендинга. Также становится необходимым регистрировать творческий контент, имеющий высокую ценность; это позволит избежать его незаконного присвоения на платформах социальных сетей. Таким образом, можно сделать вывод, что перечисленные меры позволят защитить созданный контент от посягательств на него на платформах социальных сетей.

Кроме того, исследование показало, что большинство создателей контента обладают достаточными знаниями о его добросовестном использовании и не занимаются незаконным присвоением материалов без согласия автора. Это показывает, что в разумных пределах создатели контента осведомлены о правовых шагах, которые можно предпринять для защиты авторских прав на свой контент, и подтверждает выводы, сделанные в работе Tobin (2013). В ней было показано ва ное значение того, что пользователи не могут просто присвоить произведение без учета прав автора. Если нарушаются моральные и экономические права автора, то это выходит за рамки принципа добросовестного использования, и такие нарушения влекут за собой юридические последствия. Создатели контента должны следить за соблюдением прав других авторов и всегда делать ссылки на них, а также принимать соответствующие меры для защиты своих собственных работ.

---

5 Frost, N. (2023). Crediting Sources on Social Media: Why and How to Do It. https://clck.ru/3AQekF

Заключение

В заключение следует отметить, что автору не нужно регистрировать свои работы до возникновения авторских прав, поскольку данные права начинают действовать с момента опубликования работы в художественной форме. Такое опубликование закрепляет право создателя контента на его творение без какой-либо регистрации. Кроме того, распространено заблуждение, что творческие работы создателей контента в Интернете или на платформах социальных сетей являются общественным достоянием, предназначенным для публичного использования. При этом неверно понимается термин «общественное достояние», который относится к произведениям, по ряду причин не находящимся под защитой законов об интеллектуальной собственности. Таким образом, широкое использование социальных сетей привело к свободному распространению различных творческих работ через эти платформы, которые превратились в огромный рынок для авторов и предпринимателей, нуждающихся в правовой защите. На этих платформах создаются рабочие места, появляются новые способы торговли и новые экономические отношения, и возможность нарушения прав становится неизбежной.

На этих платформах ежедневно взаимодействуют миллионы людей, и этот процесс растет в геометрической прогрессии. Следовательно, необходимо уделить внимание защите прав авторов контента с помощью соответствующего законодательства, чтобы искоренить возможности для заблуждений и ошибок.

На основе результатов данного исследования предлагаются следующие рекомендации:

– необходимо использовать видимые водяные знаки на работах, опубликованных в социальных сетях. Авторы должны рассмотреть различные варианты водяных знаков, которые будут уместны или совместимы с типом создаваемого контента;

– авторы, которые приобрели значительное влияние в определенных областях и относятся к категории агентов влияния (инфлюэнсеров), должны регистрировать свои работы, чтобы уменьшить количество случаев нарушения прав или недобросовестного использования;

– авторы также должны принимать дополнительные меры предосторожности, чтобы убедиться, что их контент не нарушает прав других авторов, поскольку это нарушит целостность их собственных работ;

– необходимо обеспечить надлежащее применение санкций к нарушителям прав интеллектуальной собственности;

– должны быть приняты специальные законы, направленные на защиту контента, созданного на платформах социальных сетей;

– создатели контента должны быть информированы об имеющихся возможностях правовой защиты своих работ с помощью тренингов, мастер-классов и семинаров.

---

* Instagram – Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

** Twitter – социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

*** YouTube – иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации.

**** LinkedIn – социальная сеть, заблокированная на территории Российской Федерации

***** Facebook – социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Список литературы

Afolayan, O. T. (2022). Intellectual Property Rights Protection in Nigeria: Issues and Perspectives. Information Impact: *Journal of Information and Knowledge Management*, *13*(1), 1–9, https://dx.doi.org/10.4314/iijikm.v13i1.1

Aina-Pelemo, A. D., Ayodeji, J. F., & Alade, I. T. (2021). Implications of Covid-19 on Intellectual Property Rights: Case study of Unfair Competition and Restraint to trade. *Carnelian Journal of Law & Politics*, *2*(2), 1–12.

Aina-Pelemo, A. D., & Akpojaro, G. O. (2024). Understanding Copyright and Fair Use in the Academic World: A Case Study of the Faculty of Law. Redeemer's University Nigeria. *University of Benin Journal of Business Law (UBJBL)*, *4*(2), 1–33.

Alvarez-Monzocillo, J. M. (2022). *The Dynamics of Influencer Marketing.* Routledge Publishers.

Fagundes, D., & Perzanowski, A. K. (2020). Abandoning Copyright. *Faculty Publications*. 2060.

Fatoba, K. (2019). *Intellectual Property Rights – An Overview of Nigerian Legal Framework*. http://dx.doi.org/10.2139/ssrn.3501898

García, K. (2022). The Emperor›s New Copyright. Boston University Law Review, 2023 Forthcoming. *Georgetown University Law Center Research Paper*, 2023/09. http://dx.doi.org/10.2139/ssrn.4048315

Jerameel, K. (2021). *The Law Meets Memes and Says Hello: Rise of Intellectual Property Rights; Kenyan Reflection*. http://dx.doi.org/10.2139/ssrn.3868440

Nicdao, J. D., Fat, A. L. T., Bolo, P. D., & Mactal, J. B. (2022). Context, Engagement and Impact of Copyright Infringement Among Selected Content Creators: A Brief Descriptive Survey Study. *International Journal of Academic and Practical Research*, *1*(1), 33–39. http://dx.doi.org/10.13140/RG.2.2.35834.98240

Kupers, E., Lehmann-Wermser, A., McPherson, G., & van Geert, P. (2019). Children's Creativity: A Theoretical Framework and Systematic Review. *Review of Educational Research*, *89*(1). https://doi.org/10.3102/0034654318815707

Lei, D., & Xue, P. (2023). Incentives or disincentives? Intellectual property protection and FinTech innovation – Evidence from Chinese cities. *Finance Research Letters*, *58*, 104451. https://doi.org/10.1016/j.frl.2023.104451

Liu, S., & Zhong, C. (2024). Green growth: Intellectual property conflicts and prospects in the extraction of natural resources for sustainable development. *Resources Policy*, *89*, 104588. https://doi.org/10.1016/j.resourpol.2023.104588

Majekolagbe, F. (2016). *A Critique of Right Management and Copyright Enforcement by Copyright Society of Nigeria (COSON)*. http://dx.doi.org/10.2139/ssrn.4349522

Nkwor, L. (2023). *Copyright in Audiovisual Works and Performers' Rights in Nigeria: a Clash Rather Than a Connection?* http://dx.doi.org/10.2139/ssrn.4430288

Oriakhogba, D. (2018). The Scope and Standard of Originality and Fixation in Nigerian and South African Copyright Law. *African Journal of Intellectual Property*, *2*(2), 119–135. https://ssrn.com/abstract=3260567

Owushi, E. (2020). Protecting Copyright Owners in Nigeria: A Panacea for Intellectual Development. *International Journal of Knowledge Content Development & Technology*, *10*(1), 21–34. https://doi.org/10.5865/IJKCT.2020.10.1.021

Priyanshi, V. (2022). IP Rights for Social Media Influencers and Content Creators.

Reid, A. (2019). Copyright Policy As Catalyst and Barrier to Innovation and Free Expression. *Catholic University Law Review*, *68*(1). http://dx.doi.org/10.2139/ssrn.3345684

Saha, C. N., & Bhattacharya, S. (2011). Intellectual Property Rights: An Overview and Implications in Pharmaceutical Industry. *Journal of Advanced Pharmaceutical Technology & Research*, *2*(2), 88–93. https://doi.org/10.4103/2231-4040.82952

Subair, S. T., Adebola, S., & Yahya, D. (2019). Social Media: Usage and Influence on Undergraduate Studies in Nigerian Universities. *IJEDICT*, *15*(3), 53–62.

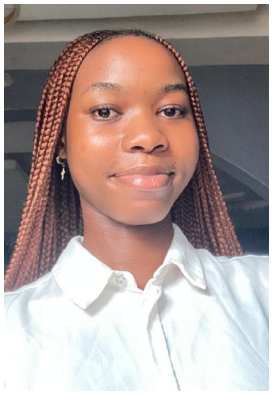
Tobin, J. (2013). *Earn It, Don't Buy It: The CMO's Guide to Social Media Marketing in a Post Facebook World Paperback*. Charles Pinot.

Zhang, C., & Xu, Y. (2023). Institutional innovation essence and knowledge innovation goal of intellectual property law in the big data era. *Journal of Innovation and Knowledge*, *8*(4), 100417. https://doi.org/10.1016/j.jik.2023.100417

Сведения об авторах

Айна-Пелемо Адетуту Дебора – PhD, старший преподаватель (доцент), кафедра юриспруденции и международного права, юридический факультет, Университет Искупителя
Адрес: Нигерия, штат Осун, Эде, P.M.B 230
E-mail: aina-pelemoa@run.edu.ng
ORCID ID: https://orcid.org/0000-0002-4063-3983
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57195309994
WoS ResearcherID: https://www.webofscience.com/wos/author/record/2345323
Google Scholar ID: https://scholar.google.com/citations?user=IX160Y8AAAAJ

Басси Итамар – бакалавр права, юридический факультет, Университет Искупителя
Адрес: Нигерия, штат Осун, Эде, P.M.B 230
E-mail: bassey7402@run.edu.ng
ORCID ID: https://orcid.org/0009-0004-9491-3392



Акподжаро Глориос Океоген – студент, юридический факультет, Университет Искупителя
Адрес: Нигерия, штат Осун, Эде, P.M.B 230
E-mail: akpojaro@run.edu.ng
ORCID ID: https://orcid.org/0009-0007-2918-5431
Google Scholar ID: https://scholar.google.com/citations?user=lu56_usAAAAJ

Вклад авторов

А. Д. Айна-Пелемо осуществляла общее руководство и постановку задач исследования; поиск и подбор научной литературы; критическую оценку интерпретации результатов исследования; формулировку ключевых выводов, предложений и рекомендаций; утверждение окончательного варианта статьи.

И. Басси осуществляла анализ национального законодательства; выполняла интерпретацию результатов исследования; организовала проведение социологического опроса и подготовку черновика рукописи.

Г. О. Акподжаро занималась сбором и анализом литературы и законодательства; проводила социологический опрос; выполняла интерпретацию результатов исследования; осуществляла подготовку чистовика рукописи.

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: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 5 февраля 2024 г.
Дата одобрения после рецензирования – 3 марта 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:34.096:347.211
EDN: https://elibrary.ru/hiqzuj
DOI: https://doi.org/10.21202/jdtl.2024.21

Measures to Prevent the Violation of the Rights of Content Creators in Digital Environment: Case Study of Nigeria

Adetutu Deborah Aina-Pelemo ✉
Redeemer's University, Ede, Nigeria

Ithamar Bassey
Redeemer's University, Ede, Nigeria

Glorious Okeoghene Akpojaro
Redeemer's University, Ede, Nigeria

Keywords

copyright,
Internet,
online content,
intellectual property rights,
legal protection,
prevention of copyright violation,
social network,
digital platform,
digital marketing,
digital technologies

Abstract

Objective: to determine the level of protection of the rights of content creators in social media and to develop measures to prevent offenses in this area.

Methods: to achieve the objective, the sociological and legal cognitive tools were used, including the doctrinal method of researching the subject area, obtaining "first-hand" data and taking into account the factors and circumstances of influence. The main results were obtained through the sociological method used to collect data based on a specially developed questionnaire with four research questions: (1) what are the perceptions and opinions of third parties or users regarding the role of a content creator? (2) are the rights of content creators regarding their works violated? (3) what are the ways to protect the created content from infringement by platforms? and (4) how can the rights of content creators be protected? The empirical findings and generalizations were based on a combination of analyses, including content analysis of primary and secondary legal sources.

Results: In recent years, the content generation in social media has evolved into a complex industry that is transforming both the traditional

✉ Corresponding author

understanding of creative expression and the implementation of intellectual property rights. Using the Nigerian experience as a case study, the authors examine the rights and protection measures provided to digital content creators under intellectual property law. The study shows that there is currently not enough scholarly work in this area or developed legislation to protect the social media content. It is concluded that there is a need for improved legislation on the protection of rights in the sphere of social media content. In the absence of such legislation, creators of online works should resort to more radical methods in enforcing their rights in order to reduce intellectual property misappropriation. Creators of such works are suggested to ensure the protection of their rights based on the fair use doctrine principles.

Scientific novelty: the study is structured around research questions concerning infringements and remedies for content creators. The questions were addressed to respondents from different countries, a large proportion of whom specialize mainly in content creation in various social spheres through several media platforms and social networks.

Practical significance: the article conclusions and recommendations may minimize the risks of infringement of intellectual property rights of content creators, which may arise with the widespread use of social networks, as well as increase the level of protection of rights to works created in the form of online content.

For citation

Aina-Pelemo, A. D., Bassey, I., & Akpojaro, G. O. (2024). Measures to Prevent the Violation of the Rights of Content Creators in Digital Environment: Case Study of Nigeria. *Journal of Digital Technologies and Law*, *2*(2), 408–429. https://doi.org/10.21202/jdtl.2024.21

References

Afolayan, O. T. (2022). Intellectual Property Rights Protection in Nigeria: Issues and Perspectives. Information Impact: *Journal of Information and Knowledge Management*, *13*(1), 1–9, https://dx.doi.org/10.4314/iijikm.v13i1.1

Aina-Pelemo, A. D., Ayodeji, J. F., & Alade, I. T. (2021). Implications of Covid-19 on Intellectual Property Rights: Case study of Unfair Competition and Restraint to trade. *Carnelian Journal of Law & Politics*, *2*(2), 1–12.

Aina-Pelemo, A. D., & Akpojaro, G. O. (2024). Understanding Copyright and Fair Use in the Academic World: A Case Study of the Faculty of Law. Redeemer's University Nigeria. *University of Benin Journal of Business Law (UBJBL)*, *4*(2), 1–33.

Alvarez-Monzocillo, J. M. (2022). *The Dynamics of Influencer Marketing.* Routledge Publishers.

Fagundes, D., & Perzanowski, A. K. (2020). Abandoning Copyright. *Faculty Publications*. 2060.

Fatoba, K. (2019). *Intellectual Property Rights – An Overview of Nigerian Legal Framework*. http://dx.doi.org/10.2139/ssrn.3501898

García, K. (2022). The Emperor›s New Copyright. Boston University Law Review, 2023 Forthcoming. *Georgetown University Law Center Research Paper*, 2023/09. http://dx.doi.org/10.2139/ssrn.4048315

Jerameel, K. (2021). *The Law Meets Memes and Says Hello: Rise of Intellectual Property Rights; Kenyan Reflection*. http://dx.doi.org/10.2139/ssrn.3868440

Nicdao, J. D., Fat, A. L. T., Bolo, P. D., & Mactal, J. B. (2022). Context, Engagement and Impact of Copyright Infringement Among Selected Content Creators: A Brief Descriptive Survey Study. *International Journal of Academic and Practical Research*, *1*(1), 33–39. http://dx.doi.org/10.13140/RG.2.2.35834.98240

Kupers, E., Lehmann-Wermser, A., McPherson, G., & van Geert, P. (2019). Children's Creativity: A Theoretical Framework and Systematic Review. *Review of Educational Research*, *89*(1). https://doi.org/10.3102/0034654318815707

Lei, D., & Xue, P. (2023). Incentives or disincentives? Intellectual property protection and FinTech innovation – Evidence from Chinese cities. *Finance Research Letters*, *58*, 104451. https://doi.org/10.1016/j.frl.2023.104451

Liu, S., & Zhong, C. (2024). Green growth: Intellectual property conflicts and prospects in the extraction of natural resources for sustainable development. *Resources Policy*, *89*, 104588. https://doi.org/10.1016/j.resourpol.2023.104588

Majekolagbe, F. (2016). *A Critique of Right Management and Copyright Enforcement by Copyright Society of Nigeria (COSON)*. http://dx.doi.org/10.2139/ssrn.4349522

Nkwor, L. (2023). *Copyright in Audiovisual Works and Performers' Rights in Nigeria: a Clash Rather Than a Connection?* http://dx.doi.org/10.2139/ssrn.4430288

Oriakhogba, D. (2018). The Scope and Standard of Originality and Fixation in Nigerian and South African Copyright Law. *African Journal of Intellectual Property*, *2*(2), 119–135. https://ssrn.com/abstract=3260567

Owushi, E. (2020). Protecting Copyright Owners in Nigeria: A Panacea for Intellectual Development. *International Journal of Knowledge Content Development & Technology*, *10*(1), 21–34. https://doi.org/10.5865/IJKCT.2020.10.1.021

Priyanshi, V. (2022). IP Rights for Social Media Influencers and Content Creators.

Reid, A. (2019). Copyright Policy As Catalyst and Barrier to Innovation and Free Expression. *Catholic University Law Review*, *68*(1). http://dx.doi.org/10.2139/ssrn.3345684

Saha, C. N., & Bhattacharya, S. (2011). Intellectual Property Rights: An Overview and Implications in Pharmaceutical Industry. *Journal of Advanced Pharmaceutical Technology & Research*, *2*(2), 88–93. https://doi.org/10.4103/2231-4040.82952

Subair, S. T., Adebola, S., & Yahya, D. (2019). Social Media: Usage and Influence on Undergraduate Studies in Nigerian Universities. *IJEDICT*, *15*(3), 53–62.

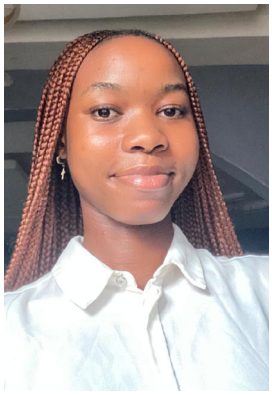
Tobin, J. (2013). *Earn It, Don't Buy It: The CMO's Guide to Social Media Marketing in a Post Facebook World Paperback*. Charles Pinot.

Zhang, C., & Xu, Y. (2023). Institutional innovation essence and knowledge innovation goal of intellectual property law in the big data era. *Journal of Innovation and Knowledge*, *8*(4), 100417. https://doi.org/10.1016/j.jik.2023.100417

Authors information

Adetutu Deborah Aina-Pelemo – PhD, Senior Lecturer (Assistant Professor), Department of Jurisprudence and International Law, Faculty of Law, Redeemer's University
Address: P.M.B 230, Ede, Osun-State, Nigeria
E-mail: aina-pelemoa@run.edu.ng
ORCID ID: https://orcid.org/0000-0002-4063-3983
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57195309994
WoS ResearcherID: https://www.webofscience.com/wos/author/record/2345323
Google Scholar ID: https://scholar.google.com/citations?user=IX160Y8AAAAJ

Ithamar Bassey – LL.B, Law Graduate, Faculty of Law, Redeemer's University
Address: P.M.B 230, Ede, Osun-State, Nigeria
E-mail: bassey7402@run.edu.ng
ORCID ID: https://orcid.org/0009-0004-9491-3392



Glorious Okeoghene Akpojaro – student, Faculty of Law, Redeemer's University
Address: P.M.B 230, Ede, Osun-State, Nigeria
E-mail: akpojaro@run.edu.ng
ORCID ID: https://orcid.org/0009-0007-2918-5431
Google Scholar ID: https://scholar.google.com/citations?user=lu56_usAAAAJ

Authors' contributions

Aina-Pelemo A. D. provided general guidance and set the study objectives; searched and selected scientific literature; critically evaluated the interpretation of the study results; formulated key conclusions, suggestions and recommendations; approved the final version of the article.

Bassey I. analyzed the national legislation; interpreted the study results; organized the sociological survey and drafted the manuscript.

Akpojaro G. O. collected and analyzed literature and legislation; conducted the sociological survey; interpreted the study results; organized the sociological survey and drafted the manuscript.

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 5, 2023
Date of approval – March 3, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:347.4:004.4
EDN: https://elibrary.ru/lvpigr
DOI: https://doi.org/10.21202/jdtl.2024.22

Соглашение о государственно-частном партнерстве в контексте матрицы оценки их юридических параметров и цифровизации

Доминик Т. Молинтас

Колледж аэронавтики PATTS, Параньяк, Филиппины;
Университет Гриффита, Квинсленд, Австралия

Ключевые слова

государственно-частное партнерство,
контракт,
конфликт интересов,
ограничение конкуренции,
право,
соглашение,
управление рисками,
цифровые технологии,
цифровизация,
юридическая оценка

Аннотация

Цель: путем рассмотрения юридических аспектов соглашений о государственно-частном партнерстве синтезировать их основные положения в общую матрицу, которую при переводе в цифровой формат можно использовать в интересах стандартизации и упрощения формулирования параметров соглашения.

Методы: автор опирался на сравнительно-правовой анализ научной литературы, законодательства и интернет-источников по государственно-частному партнерству, дополненный рассмотрением соглашений о государственно-частном партнерстве различной социально-политической направленности, что позволило создать научно-обоснованную и практико-ориентированную матрицу, которая может послужить инструментом при составлении соглашений о государственно-частном партнерстве.

Результаты: выделены национальные аспекты в правовом регулировании обозначенных отношений в различных странах и описан ряд особенностей, встречающихся в соглашениях о государственно-частном партнерстве.

Научная новизна: с учетом важнейших правовых особенностей, характерных для разных стран, представлена матрица для составления соглашений о государственно-частном партнерстве, включающая восемь основных параметров: 1 – полученную стоимость, масштаб, выгоды и риски, 2 – выход на рынок, 3 – ограничение конкуренции, 4 – конфликт интересов/закупки, 5 – полномочия, одобрение, юридическая оценка, 6 – обязательства, разрешение споров, 7 – структуру собственности, управление и уровень автономии, 8 – стратегии выхода. В зависимости от обозначенных приоритетов ее можно модифицировать, учитывая, что приоритеты определяют и формируют конкретные параметры каждого отдельного партнерства.

Практическая значимость: полученная в результате исследования матричная схема может стать инструментом планирования, используемым для анализа и понимания взаимосвязей между восемью юридическими параметрами, необходимыми для формирования отношений в сфере государственно-частного партнерства. Она послужит юридическим ориентиром для формулирования соглашений о государственно-частном партнерстве, используемых во всем мире, и будет способствовать не только активизации государственно-частного партнерства, но и правильному пониманию обязательств, объемов ответственности и ограничений. Приведенные в исследовании рекомендации задают направление для оценки государственно-частного партнерства, позволяя сделать четкие выводы о партнерстве. При условии цифровой доступности предложенная матрица будет представлять определенный интерес для многих организаций, использующих государственно-частное партнерство в своей профессиональной деятельности.

Для цитирования

Молинтас, Д. Т. (2024). Соглашение о государственно-частном партнерстве в контексте матрицы оценки их юридических параметров и цифровизации. *Journal of Digital Technologies and Law*, *2*(2), 430–449. https://doi.org/10.21202/jdtl.2024.22

Содержание

Введение

Инвестиции в строительство способствуют значительному экономическому прогрессу и социальному развитию. Обустроенная среда стимулирует торговлю, что приводит к росту производства, повышению микроэкономической эффективности и снижению транзакционных издержек (Jayachandran, 2021). В бедных странах, где государственные бюджеты уже полностью распределены, государственно-частное партнерство (далее – ГЧП) является основной платформой для закупок в строительной сфере (Moffatt & Kohler, 2008). Разработаны многочисленные варианты контрактов по модели ГЧП в качестве механизма повышения устойчивости к рискам и продления срока действия проектов[1].

В данном исследовании представлен обзор важнейших правовых особенностей, характерных для разных стран с целью формирования матрицы для цифровизации юридических аспектов ГЧП. В сфере ГЧП назрела необходимость в создании инструмента для фиксации договоренностей между сторонами предполагаемого предприятия (Leigland, 2018). Такой договор должен содержать указания на вкладываемые средства, предполагаемые результаты, обязательства, права, обязанности и ответственность сторон. Договор должен определять такие ключевые элементы, как механизм распределения прибылей и обязательств, чтобы избежать споров (González-Ruiz et al., 2018).

Для определения наиболее подходящего контракта в сфере ГЧП нами был разработан инструмент оценки с использованием матрицы, представленный в настоящем исследовании. Кроме того, мы выделили некоторые правовые аспекты различных стран в этой области деятельности и описали ряд особенно интересных положений, встречающихся в контрактах ГЧП.

1. Полученная стоимость (масштаб, выгоды и риски)

1.1. Полномочия, одобрение, юридическая оценка

Законодательство Китая позволяет гибко подходить как к определению состава совета директоров, так и разграничению полномочий по ведению деятельности. По законодательству Индонезии государство может заключать договоры ГЧП с частными компаниями для реализации инфраструктурных проектов[2]. Процесс заключения таких контрактов регулируется законами и нормативными актами о ГЧП, а также Указом Президента № 38 от 2015 г. о сотрудничестве между государством и хозяйствующими субъектами в целях развития инфраструктуры (Rybnicek et al., 2020; Buso et al., 2021).

Контракты ГЧП в штате Квинсленд (Австралия) не предусматривают гарантий государства по обязательствам и исполнению партнерства. В Соединенном Королевстве главной задачей при создании специальных инструментов для обеспечения деятельности являются централизация и формализация. Согласно австралийскому законодательству, ГЧП создается при наличии значительного

---

1 The World Bank. (2017, April 27). PPP Reference Guide 3.0 (Full version). https://clck.ru/3AgJNx

2 Eddymurthy, I., & Mooduto, N. (2017). Joint ventures in Indonesia: overview. Jakarta: SSEK Indonesian Legal Consultants. https://clck.ru/3AgJS8

синергетического эффекта, подтверждением которого может служить увеличение экспортных поступлений или удешевление товаров (Jokar et al., 2021). ГЧП должно продемонстрировать эффективность или снижение затрат благодаря осуществлению проекта или программы группой в целом, а не отдельными ее членами[3].

1.2. Структура собственности, управление и уровень автономии

Японское законодательство не регулирует ГЧП непосредственно. Партнерские контракты регулируются Законом № 89 Гражданского кодекса от 1896 г. и Законом о компаниях № 86 от 2005 г.[4] В соответствии с законодательством Бельгии участник ГЧП должен внести 25 % уставного капитала. Минимальный размер капитала для создания ГЧП с государственной компанией составляет 61,5 тысячи евро. Индонезийское законодательство предусматривает создание ГЧП с участием юридического лица, имеющего статус компании с ограниченной ответственностью, в соответствии с Законом о корпорациях[5] (Chen & Hubbard, 2012).

К структурам управления ГЧП, активно выполняющим политические функции, относятся: во Франции – Миссия по содействию в реализации государственно-частных партнерств (Mission d'appui à la réalisation des partenariats public–privé, MAPPP)[6] как орган управления; в Греции – Специальный секретариат по распространению информации о ГЧП как орган управления; в Италии – техническое подразделение по финансированию проектов (Unita Tecnicà Finanza di Progetto, UTFP)[7]; в Португалии – Комиссия по ГЧП; в Великобритании – инфраструктурное подразделение по вопросам партнерства на местном уровне (Demirag et al., 2011; Rybnicek et al., 2020; Ito, 2020).

1.3. Обязательства, разрешение споров

Согласно законодательству Индонезии, совокупный выпущенный и оплаченный акционерный капитал должен составлять не менее 25 % от уставного капитала ГЧП. Постановлением Правительства № 29 от 2016 г. сделано исключение для микро-, малых и средних предприятий с уставным капиталом менее IDR 50 млн, при этом оплата за акции может производиться как наличными, так и в натуральной форме. Бразильское законодательство[8] предусматривает, что корпорации и общества с огра-

---

3 Government of Australia. (2016). National Guidelines for Infrastructure Project Delivery. Canberra: The Department of Infrastructure, Transport, Regional Development, Communications and the Arts. https://goo.su/9k38lH

4 Association of Southeast Asian Nations. (1980). Supplementary Agreement to the Basic Agreement on Asean urea project. Indonesia. Jakarta. https://clck.ru/3AgJbY

5 Government of the Republic of Indonesia. (1979). Agreement between the Government of the Republic of Indonesia and the United Nations High Commissioner for Refugees regarding the Establishment of the Office of the UNHCR representative for Indonesia. Jakarta: Government of the Republic of Indonesia. https://goo.su/kUK0k

6 MAPPP – Mission to support the implementation of public-private partnership contracts. (In French). https://clck.ru/3AgJhn

7 Presidenza del Consiglio dei Ministri. (2010). Unita Tecnica Finanza di Progetto (UTPF). (In Italian). https://clck.ru/3AgJim

8 National Congress. (2004). Brazil's Public-Private Partnership Law. Brasilia: Lei de Licitações e Contratos Administrativos. (In Portuguese). https://goo.su/yOEZc5

ниченной ответственностью должны обеспечивать акционерам защиту от ограниченной ответственности, за исключением ответственности согласно экологическому и антимонопольному законодательству, законам о борьбе со взяточничеством, трудовому общему праву и законам о защите прав потребителей, где акционер может нести личную ответственность (Kurniawan et al., 2015; Wang, 2003).

В штате Квинсленд ГЧП имеют возможность обратиться в суд для получения приказа во исполнение статута при возникновении споров относительно траста, продажи или раздела имущества. В то же время совет директоров головной компании несет ответственность за соблюдение руководящих принципов такого партнерства. В частности, в Китае от иностранного участника государственно-частного партнерства требуется подтвердить обязательство не посягать на суверенитет страны и не эксплуатировать ее ресурсы (Salem, 1981). Законодательство о разрешении споров, связанных с ГЧП[9], должно исключать длительные периоды подготовки до начала разбирательства; также нежелательно менять юрисдикцию с целью ускорить вынесение промежуточного или окончательного судебного решения.

1.4. Стратегии выхода

Законодательство Таиланда, а именно Закон о частных инвестициях в государственные предприятия (Private investment in state undertaking, PISU) содержит заметное упущение в вопросе досрочного расторжения договора, хотя в законодательстве ЕЭС и в новом Законе о ГЧП оно предусмотрено. В случае если досрочное расторжение договора происходит не по вине частного предприятия, государство должно выплатить соответствующую компенсацию, используя надлежащий механизм расчета. Это соответствует концепции партнерства и обеспечивает тщательную проработку роли частного партнера. В случаях, когда досрочное расторжение происходит из-за действий частной организации, государство имеет право возместить свои убытки, возникшие в результате такого нарушения (Garg & Garg, 2016, Wegrich et al., 2017; Hart, 2003).

Британское законодательство допускает прекращение деятельности ГЧП по взаимному согласию сторон либо при нарушении, допущенном одной из сторон, или при форс-мажорных обстоятельствах. В Корее предприятия с иностранными инвестициями и активы, вложенные иностранными инвесторами, не подлежат национализации или конфискации государством. Иностранному инвестору разрешается реинвестировать часть прибыли или всю прибыль на территории КНДР (Lee, 2003).

Китайский закон о налогообложении поощряет депонирование средств в Банке Китая, разрешая возврат налога на реинвестированную сумму. Таким образом, можно вернуть подоходный налог, уплаченный с реинвестированной суммы, или его часть. В случае национализации или конфискации государством предприятий и активов должна быть выплачена справедливая компенсация (Jin & Huang, 2021).

[9] US Security Exchange and Commission. (2008). Sino-Foreign Joint Venture Contract by and between Sun Far East Limited and Zibo Bao Kai Trading Company, LTD. for establishing Taixing Zhongneng Far East Silicon Co., LtD. USA: SEC. https://clck.ru/3AgJsr

2. Выход на рынок

2.1. Полномочия, одобрение, юридическая оценка

В Испании в интересах ГЧП действует временный консорциум Unión Temporal de Empresas (UTE). В США вопросы ответственности и распределения рисков, положения о защите и возмещении ущерба определяет специальный орган Special Purpose Vehicle (DoD NASA, 2020; Noring, 2019). В штате Квинсленд в случае принятия решения о полном или частичном отчуждении доли в ГЧП между действующими сторонами и новым участником заключается особое соглашение. В Австралии действует механизм AusTrade PPP Grant – особый вид государственно-частного партнерства, в рамках которого правительство выдает малому или среднему предприятию грант с целью осуществления конкретной экспортной деятельности. Максимальный размер гранта – 150 тысяч австралийских долларов в год[10].

2.2. Структура собственности, управление и уровень автономии

Ряд структур государственно-частного партнерства при министерствах и ведомствах, выполнявших политические функции, показали очень низкую или среднюю эффективность и некоторые из них были закрыты: в Австрии – PPP Kompetenzzentrum; в Чехии – PPP Centrum; в Дании – PPP knowledge unit; в Нидерландах – PPS support; в Сербии – Odbor partnerských projektov; в Словакии – Sektor za upravljanje javnega premoženja.

По законодательству Таиланда, органом, утверждающим окончательный выбор частной компании и проект контракта ГЧП на этапе закупок является кабинет министров (Hennessey, 2021). Однако, согласно новому законопроекту о ГЧП, роль кабинета министров на этапе закупок может быть уменьшена с целью повышения эффективности и гибкости осуществления процесса партнерства (Mirzaee & Sardroud, 2022). К числу объектов национальной инфраструктуры, созданных в рамках ГЧП, относятся международный аэропорт У-Тапао, высокоскоростное железнодорожное сообщение с тремя крупнейшими аэропортами, промышленный порт Мап Та Пхут Фаза III, порт Лаем Чабанг Фаза III и цифровой парк Таиланда[11]. Законодательство Индии[12] предусматривает, что государственная структура, намеревающаяся вступить в партнерские отношения с частным сектором, должна сначала изучить возможность достижения целей с помощью альтернативных средств, отличных от ГЧП (Selim & ElGohary, 2020). В Европе структура ГЧП должна быть в первую очередь совместима с внутренним рынком, чтобы способствовать экономическому развитию, особенно в регионах, где уровень жизни аномально низок или существует неполная занятость (Yurdakul et al., 2022). Ввиду структурной, экономической и социальной ситуации к ним относятся регионы ЕС, упомянутые в ст. 349[13].

---

10 Austrade Export Market Development Grants Canberra. (2020). https://goo.su/rnYK

11 Ponte, J. de. (2021). Delivering Thailand's Infrastructure Pipeline – The PPP push. Melbourne: DLA Piper Global Services LLP. https://clck.ru/3AgK8V

12 Ministry of Finance. (2009). Joint Ventures: a guidance note for public sector bodies forming joint ventures with the private sector. New Delhi: Government of India. https://clck.ru/3AgK9j

13 Hatton, C., Cardwell, D., & Botts, B. (2020, July 8). European Union: Joint Ventures. Global Competition Review. https://clck.ru/3AgKCF

2.3. Обязательства, разрешение споров

В соответствии с законодательством Кипра, арбитраж не практикуется, а компетентными органами для разрешения споров являются окружные суды[14]. В Индии ответственность за все действия и решения партнерства несут члены совета директоров ГЧП со стороны правительства (Liu et al., 2016a; Ma et al., 2023; Liu et al., 2016b; Rufín & Rivera-Santos, 2012).

В Европе таким советом является Европейская группа по экономическим интересам (European Economic Interest Group, EEIG). Структура партнерства определяется договором, заключенным между участниками, которые несут солидарную ответственность по долгам и обязательствам EEIG. Если не определено иное, EEIG также назначает руководителей ГЧП (Whiteside, 2020).

В штате Квинсленд договор ГЧП включает право доступа его членов и аудиторов к бухгалтерской отчетности и счетам партнерства. Законодательство Китая предоставляет ГЧП значительно большую степень гибкости в определении состава контролирующего органа совместного предприятия, чем в ряде других социалистических стран (Wang et al., 2019).

2.4. Стратегии выхода

Согласно британскому законодательству, прекращение ГЧП может быть осуществлено по взаимному соглашению сторон; либо в результате нарушения, допущенного одной из сторон; либо в результате форс-мажорных обстоятельств.

Законодательство о ГЧП в Великобритании допускает возможность выхода акционеров через опционы на покупку акций или через предложение акций с преимущественным правом покупки. В европейском антимонопольном законодательстве и законах о конкуренции обращается особое внимание на структуру предприятия и цель его деятельности. В работе ГЧП необходимо учитывать условия конкуренции на соответствующем рынке и ограничения, которые способны снизить эффективность партнерства; используются и антиконкурентные ограничения, такие как фиксация цен или раздел рынка (Owen Liu, Xiong & Zhu, 2007).

Нормы в отношении ГЧП, предусмотренные законодательством ОАЭ[15], носят преимущественно ограничительный характер. Среди них положения о конфиденциальности, запрет недобросовестного найма сотрудников противоположной стороны, а также правила отчуждения и приобретения акций в случае их продажи третьим лицам по моделям «прицеп», «присоединение» или «понуждение к совместной продаже», например, в фармацевтической или нефтехимической промышленности и т. д. (Sharma, 2022).

---

[14] The Private Sector Participation Governing Rules. https://clck.ru/3AgKRH

[15] Mohammed bin Rashid Al Maktoum, Ruler of Dubai (2017). Law No. (22) of 2015 Regulating Partnership between the Public Sector and the Private Sector in the Emirate of Dubai. Dubai: The Supreme Legislation Committee in the Emirate of Dubai. https://clck.ru/3AgKKF

3. Ограничение конкуренции

3.1. Полномочия, одобрение, юридическая оценка

Европейское законодательство в области ГЧП[16] запрещает получение субсидий или ресурсов, которые угрожают свободной конкуренции; при этом отдается предпочтение определенным предприятиям и производствам на внутреннем европейском рынке (Rossi & Civitillo, 2014). Законы штата Квинсленд[17] требуют, чтобы ГЧП обеспечивало стратегические преимущества, особенно в высокорегулируемых секторах. В качестве примера можно привести договор ГЧП с сингапурскими фирмами, в котором четко указано, что арбитраж будет проводиться в Сингапуре. Законодательство Кореи[18] определяет конкретные сектора для ГЧП, включая промышленность, сельское хозяйство, строительство, транспорт, телекоммуникации, науку и технологии, туризм и финансовые услуги. Запрещены или ограничены инвестиции, препятствующие развитию национальной экономики и угрожающие национальной безопасности, а также технически устаревшие и наносящие вред окружающей среде (Hurk et al., 2016; Soomro & Yuhui, 2023; Liu et al., 2014).

3.2. Структура собственности, управление и уровень автономии

В Африке Закон о ГЧП запрещает соглашения между конкурентами, которые приводят к установлению цен и распределению рынков, сговору при проведении тендеров и установлению минимальных и перепродажных цен. В соответствии с законодательством Малайзии, условия участия в ГЧП варьируются от варианта концессии и приватизации до партнерства (Biygautane et al., 2020). В странах Азии сотрудничество местных компаний касается в основном стандартных инфраструктурных проектов. В Австралии Закон о конкуренции и защите прав потребителей 2010 г. запрещает и криминализирует картельные сговоры в сфере ГЧП. Согласно немецкому законодательству, нарушение запрета на картельные сговоры является уголовно наказуемым (Outhuijse, 2020).

Если в рамках ГЧП происходит концентрация собственности независимых участников рынка, это может быть чревато нарушением запрета на картели. В противном случае, когда обе партнерские компании остаются активными на данном рынке, существует риск, что характер ГЧП будет расценен как кооперация, а игроки нарушат запрет на картели. В Германии ГЧП может быть организовано по-разному в зависимости от глубины сотрудничества. Это может быть корпорация ГЧП (Aktiengesellschaft); общество с ограниченной ответственностью (Gesellschaft mit beschränkter Haftung); «тихие» товарищества (stille Gesellschaft); субучастие, или присоединение (Unterbeteiligung). Все это формы ГЧП, предусмотренные немецким законодательством (Darko et al., 2023).

---

16 Hatton, C., Cardwell, D., & Botts, B. (2020, July 8). European Union: Joint Ventures. Global Competition Review. https://clck.ru/3AgKYR

17 Queensland Treasury and Trade. (2013). Government Owned Corporations Guidelines for Joint Venture Agreements. Queensland Treasury. https://goo.su/v45h3t

18 Standing Committee of the Supreme People's Assembly. (1992). The law of the Democratic People's Republic of Korea on foreign investment. Seoul: Fourth Session of the Ninth Supreme People's.

3.3. Обязательства, разрешение споров

По австралийскому законодательству нельзя избежать длительных процедур разрешения споров или изменить юрисдикцию судов с целью добиться срочного судебного решения, промежуточного или окончательного[19]. Британское венчурное законодательство для разрешения споров, возникающих в работе предприятия, предусматривает (в порядке предпочтительности) консультации, мировое соглашение, арбитраж и судебную процедуру (Khallaf et al., 2021). Индонезийское законодательство запрещает практики, направленные на несправедливое ограничение конкуренции, в соответствии с антимонопольным законодательством и Законом о запрете монополистической практики и несправедливой деловой конкуренции. Например, субъекту, занимающему доминирующее положение на рынке, запрещается злоупотреблять своим положением, несправедливо ограничивая деятельность своих конкурентов. Положение об отсутствии конкуренции, заявленное доминирующим в отрасли предприятием, может не пройти проверку в индонезийском Агентстве по надзору за конкуренцией.

Согласно законодательству Японии[20], к закрытым относятся отрасли, затрагивающие значимые общественные интересы, например, гидротехнические работы, железные дороги, банковское дело и морские перевозки (Bradshaw, 1963).

3.4. Стратегии выхода

По законам ОАЭ арбитраж проводится в Дубайском международном арбитражном центре (DIAC), либо в Лондонском международном арбитражном суде (London Court of International Arbitration, LCIA), либо в совместном органе DIFC-LCIA. Согласно регламенту DIFC-LCIA, рекомендуется определять конкретное место проведения арбитража на начальном этапе сотрудничества[21]. Согласно корейскому законодательству, на ГЧП распространяются основные положения, регулирующие вопросы антимонопольного регулирования и справедливой конкуренции, предусмотренные Законом о регулировании монополий и честной торговле[22]. Кроме того, в аспектах слияния и поглощения государственно-частного партнерства может касаться корейское законодательство о контроле за слияниями, если общая сумма активов или оборот компании по всему миру равны или превышают 300 млрд южнокорейских вон, или 257,1 млн UR. В Австралии отчуждение и переуступка доли в ГЧП со стороны государственного партнера не требуют согласия ГЧП. Согласно индийскому законодательству, государственная организация обязана оценить возможные способы возврата инвестиций в случае неудачи ГЧП.

---

19 Seungwoo Son. (2012). Legal analysis on Public-Private Partnerships regarding Model PPP Rules. https://clck.ru/3AgKta

20 Matsuura, M., Niunoya, M., & Hamasu, Sh. (2023). A structured guide to public private partnerships in Japan. Atsumi & Saka. https://clck.ru/3AgKue

21 HM Treasury. (2010, March). Joint Ventures: a guidance note for public sector bodies forming joint ventures with the private sector. London: Government of UK. https://clck.ru/3AgKva

22 Tae Hee Lee. (2020). International Joint Ventures in Korea. Seoul: Lee & Ko. https://clck.ru/3AgKwa

4. Конфликт интересов/закупки

4.1. Полномочия, одобрение, юридическая оценка

Согласно австралийскому законодательству, ГЧП пользуется неквалифицированным правом на раскрытие конфиденциальной информации и, наоборот, правом на раскрытие квалифицированной информации. На Кипре арбитраж не практикуется и роль компетентных органов выполняют окружные суды (Caperchione et al., 2017). По законам Кореи, к нарушениям добросовестной конкуренции относятся дискриминация и злоупотребление преимущественным положением; ложная, обманная или вводящая в заблуждение реклама. Законодательство Малайзии ввело меры по ускорению процесса утверждения проектов ГЧП, в результате чего сроки такого утверждения сократились до 8–10 месяцев. Эти положения применяются к тем инвестиционным проектам, которые были признаны особо важными Комитетом по политике ЕЭС и требуют рассмотрения перед утверждением. В соответствии с китайским законодательством, создание ГЧП включает в себя четыре основных этапа: получение согласия Китайской международной трастовой и инвестиционной корпорации; согласование правовой базы совместного предприятия; получение разрешения Комиссии по иностранным инвестициям КНР; регистрация в Главном управлении промышленности и торговли (Liyanapathirana et al., 2023).

4.2. Структура собственности, управление и уровень автономии

В КНДР законодательство по ГЧП разрешает совместным предприятиям с долевым участием и на договорной основе создавать и управлять предприятиями, полностью принадлежащими иностранному капиталу, в свободной торгово-экономической зоне. По законам Австралии[23] ГЧП должно допускать неквалифицированное право на раскрытие конфиденциальной информации государственным партнером ГЧП и, наоборот, раскрытие квалифицированной информации (Azarian et al., 2023). В Словакии[24] ответственность регулируется коммерческим кодексом, но между партнерами существует большая договорная свобода, поскольку непосредственно закон о ГЧП отсутствует. Согласно индийскому законодательству[25], ГЧП создается как автономная уставная организация на принципах, схожих с таковыми группы предприятий. В Европе при создании совместного предприятия предусмотрено подписание соглашения о неконкуренции, когда стороны соглашаются не конкурировать за пределами совместного предприятия[26].

4.3. Обязательства, разрешение споров

В штате Квинсленд партнер ГЧП не может предоставлять гарантии или брать на себя какие-либо обязательства ГЧП, если это специально не одобрено представителями

---

[23] Griffiths, A., & Carney, N. (2023). An introduction to public-private partnerships in Australia. Lexology. https://clck.ru/3AgLab

[24] Ministry of Finance of the Slovak Republic. Public Private Partnership (PPP). https://clck.ru/3AgLbZ

[25] Government of India. Public Private Partnership In India. https://goo.su/qlmvkUI

[26] Giguère, S. (2001). Local governance and partnerships. A summary of the findings of the OECD study on local partnerships. Paris: Organisation for Economic Co-operation and Development. https://goo.su/G5ctv

акционеров и не оговорено в Руководстве по инвестициям (Ojelabi & Noone, 2020). Согласно корейскому законодательству, любые разногласия, касающиеся иностранных инвестиций, должны решаться путем консультаций. Споры рассматриваются и разрешаются судом или арбитражным органом, в противном случае разногласия могут быть переданы для разрешения в арбитражное агентство в третьих странах[27]. По законодательству Новой Зеландии, при возникновении спора все действия должны происходить в рамках закона независимо от структуры ГЧП; место и процедура разрешения спора могут оговариваться отдельно; при отсутствии конкуренции остается только одна заинтересованная сторона (Chou & Lin, 2012).

В немецком законодательстве важную роль играют положения о контроле за слияниями. Существенным критерием является доминирующее положение на рынке: если оно создается, то ГЧП должно быть запрещено. Однако если партнеры докажут, что, несмотря на создание или укрепление доминирующего положения на рынке, ГЧП улучшает конкурентные условия на том же или другом рынке и это перевешивает негативное влияние доминирующего положения, то они могут получить разрешение на слияние. В американском праве ГЧП определяет ответственность, структура которой включает защиту, возмещение убытков и оговорку о непричинении вреда.

4.4. Стратегии выхода

Согласно британскому законодательству, деятельность ГЧП может быть прекращена по взаимному соглашению сторон, в результате нарушения, допущенного одной из сторон, или форс-мажорных обстоятельств (Marques, 2021). По законам Кореи[28] стороны вправе обратиться в любой суд соответствующей юрисдикции внутри страны или за ее пределами для разрешения споров, возникающих в рамках ГЧП. Возможные средства правовой защиты включают денежные компенсации за ущерб или убытки, соответствующие предварительные аресты, а также средства правовой защиты по праву справедливости в виде исполнения конкретных обязательств, временного и постоянного судебного запрета (Lemley & McCreary, 2020).

Согласно законодательству Новой Зеландии, акционеры ГЧП не несут фидуциарных обязательств друг перед другом. По индийскому законодательству, типичными являются следующие стратегии выхода из международных проектов: продажа, перепродажа, слияние, объединение или ликвидация; требование по страховке или гарантии; перемещение или уход с рынка; судебное или арбитражное разбирательство.

Заключение

Любой юридический аспект соглашения о партнерстве рассматривается с точки зрения четырех различных юридических аргументов, что является признаком хорошо продуманного соглашения. Приведенные ниже рекомендации задают направление оценки ГЧП, позволяют сделать четкие выводы о партнерстве.

---

27 Mirza & Associates. (2023, May 23). The pros and cons of arbitration vs. litigation: What's the best option for your Business? Mondaq. https://clck.ru/3AgLhv

28 Standing Committee of the Supreme People's Assembly. (1992). The law of the Democratic People's Republic of Korea on foreign investment. Seoul: Fourth Session of the Ninth Supreme People's. https://clck.ru/3AgLjY

Рекомендации для оценки ГЧП

Матрица механизмов		Полномочия, одобрение, юридическая оценка	Структура собственности (управление и уровень автономии)	Обязательства, разрешение споров	Стратегии выхода
	Полученная стоимость (масштаб, выгоды и риски)	Совместное предприятие создается, когда прогнозируется значительный синергетический эффект, который приведет к увеличению экспортной выручки или удешевлению потребительских услуг и товаров	На местном рынке ГЧП содействует экономическому развитию, особенно там, где наблюдался аномально низкий уровень жизни или неполная занятость	ГЧП в форме компании специального назначения может обеспечить акционерам защиту от ограниченной ответственности, за исключением экологического и антимонопольного законодательства	Какое-либо агентство или государственная компания не должны предоставлять гарантии или брать на себя какие-либо обязательства по ГЧП, если это специально не одобрено руководством и не соответствует законодательству по инвестициям
	Выход на рынок	ГЧП предусматривает заключение соглашения между существующими участниками в разумные и определенные сроки	Руководящие принципы ГЧП ограничивают отрасли, затрагивающие общественные интересы, такие как транспорт, энергетика или образование. Роль правительства заключается в защите активов национальной инфраструктуры	Представители государства в правлении ГЧП несут ответственность и подотчетны за определенные действия и решения ГЧП и за любые неудачи	Арбитражный суд должен быть определен с самого начала, например, Лондонский международный арбитражный суд и соответствующие правила
	Ограничение конкуренции	ГЧП должно прямо запрещать и криминализировать картельные сговоры. Роль государства заключается в защите воздействия на экономику, а не в обеспечении прибыльности ГЧП	Государство может заключать соглашения о ГЧП с частными компаниями для реализации инфраструктурных проектов при условии, что вхождение или поглощение может осуществляется исключительно суверенным государством	На ГЧП распространяются основные правила антимонопольного регулирования и добросовестной конкуренции: монополия и честная торговля	Соглашения о ГЧП не должны позволять частному сектору полностью брать на себя ответственность за реализацию проектов после их завершения
	Конфликт интересов (закупки)	ГЧП не должно наносить ущерб добросовестной конкуренции: запрещены дискриминация, злоупотребление преимущественным положением на переговорах, включая ложную, обманную или вводящую в заблуждение рекламу	При создании ГЧП утверждаются Соглашения о неконкуренции когда стороны соглашаются не конкурировать за пределами совместного предприятия	В рамках ГЧП недопустимо предоставление грантов или финансовых ресурсов, которые искажают или угрожают конкуренции, отдавая предпочтение определенным предприятиям	

Список литературы

Azarian, M., Shiferaw, A. T., Lædre, O., Wondimu, P. A., & Stevik, T. K. (2023). Project ownership in public-private partnership (PPP) projects of Norway. *Procedia Computer Science*, *219*, 1838–1846. https://doi.org/10.1016/j.procs.2023.01.481

Biygautane, Mh., Neesham, C., & Al-Yahya, Kh. O. (2020). Institutional entrepreneurship and infrastructure public-private partnership (PPP): Unpacking the role of social actors in implementing PPP projects. *International Journal of Project Management*, *37*(1), 192–219. https://doi.org/10.1016/j.ijproman.2018.12.005

Bradshaw, C. (1963). Joint Ventures in Japan. *Washington Law Review*, *38*(1), 58–104.

Buso, M., Dosi, C., & Moretto, M. (2021). Do exit options increase the value for money of public–private partnerships? *Journal of Economics & Management Strategy*, *30*(4), 721–742. https://doi.org/10.1111/jems.12440

Caperchione, E., Demirag, I., & Grossi, G. (2017). Public sector reforms and public private partnerships: Overview and research agenda. *Accounting Forum*, *41*(1), 1–7. https://doi.org/10.1016/j.accfor.2017.01.003

Chen, Ch., & Hubbard, M. (2012). Power relations and risk allocation in the governance of public private partnerships: A case study from China. *Policy and Society*, *31*(1), 39–49. https://doi.org/10.1016/j.polsoc.2012.01.003

Chou, J.-Sh., & Lin, Ch. (2012). Predicting disputes in Public-Private Partnership projects: Classification and ensemble models. *Journal of Computing in Civil Engineering*, *27*(1). https://doi.org/10.1061/(ASCE)CP.1943-5487.0000197

Darko, D., Zhu, D., Quayson, M., Hossin, M. A., Omoruyi, O., & Bediako, A. K. (2023). A multicriteria decision framework for governance of PPP projects towards sustainable development. *Socio-Economic Planning Sciences*, *87*(B), 101580. https://doi.org/10.1016/j.seps.2023.101580

Demirag, I., Khadaroo, I., Stapleton, P., & Stevenson, C. (2011). Risks and the financing of PPP: Perspectives from the financiers. *The British Accounting Review*, *43*(4), 294–310. https://doi.org/10.1016/j.bar.2011.08.006

DoD NASA. (2020). *Proposed Rules. Federal Register*, *85*(109), 34561–34569.

Garg, S., & Garg, S. (2016). Rethinking Public-Private Partnerships: An unbundling approach. *Transportation Research Procedia* (Vol. 25, pp. 3789–3807). https://doi.org/10.1016/j.trpro.2017.05.241

González-Ruiz, Ju. D., Botero-Botero, S., & Duque-Grisales, E. (2018). Financial eco-innovation as a mechanism for fostering the development of sustainable infrastructure systems. *Sustainability*, *10*(12), 4463. https://doi.org/10.3390/su10124463

Hart, O. (2003). Incomplete contracts and public ownership: Remarks, and an application to public-private partnerships. *The Economic Journal*, *113*(486), C69–C76. https://doi.org/10.1111/1468-0297.00119

Hennessey, K. (2021). Comment on «When and how to use Public-Private Partnerships in infrastructure: Lessons from the international experience». In E. Glaeser, & J. Poterba (Eds.), *Economic Analysis and Infrastructure Investment* (pp. 365–368). Cambridge: National Bureau of Economic Research.

Hurk, M. van den, Brogaard, L., Lember, V., Petersen, O. H., & Witz, P. (2016). National varieties of Public-Private Partnerships (PPPs): A comparative analysis of PPP-supporting units in 19 European Countries. *Journal of Comparative Policy Analysis: Research and Practice*, *18*(1), 1–20. https://doi.org/10.1080/13876988.2015.1006814

Ito, S. (2020). *Infrastructure Development and Public-Private Partnership.* Singapore: Springer Nature Singapore Pte Ltd.

Jayachandran, S. (2021). *How economic development influences the environment*. Cambridge: National Bureau of Economic Research. https://doi.org/10.3386/w29191

Jin, Zh., & Huang, Ch. (2021). Tax enforcement and corporate donations: evidence from Chinese 'Golden Tax Phase III'. *China Journal of Accounting Studies*, *9*(4), 526–548. https://doi.org/10.1080/21697213.2022.2053375.

Jokar, E., Aminnejad, B., & Lork, A. (2021). Assessing and prioritizing risks in Public-Private Partnership (PPP) projects using the integration of fuzzy multi-criteria decision-making methods. *Operations Research Perspectives*, *8*, 100190. https://doi.org/10.1016/j.orp.2021.100190

Khallaf, R., Naderpajouh, N., & Hastak, M. (2021). Robust decision-making for multiparty renegotiations in Public-Private Partnerships. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *13*(3). https://doi.org/10.1061/(ASCE)LA.1943-4170.0000473

Kurniawan, F., Mudjanarko, S. W., & Ogunlana, S. O. (2015). Best practice for financial models of PPP projects. In *Procedia Engineering* (Vol. 125, pp. 124–132). https://doi.org/10.1016/j.proeng.2015.11.019

Lee, E. Y.-J. (2003). The Special Economic Zones and North Korean economic Reformation with a viewpoint of international law. *Fordham International Law Journal*, *27*(4), 1343–1378.

Leigland, J. (2018). Public-Private partnerships in developing countries: The emerging evidence-based critique. *The World Bank Research Observer*, *33*(1), 103–134. https://doi.org/10.1093/wbro/lkx008

Lemley, M., & McCreary, A. (2019, December 19). Exit strategy. *Stanford Law and Economics Olin Working Paper*, 542.

Liu, J., Gao, R., Cheah, Ch., & Luo, J. (2016a). Incentive mechanism for inhibiting investors' opportunistic behavior in PPP projects. *International Journal of Project Management*, *34*(7), 1102–1111. https://doi.org/10.1016/j.ijproman.2016.05.013

Liu, J., Yu, X., & Cheah, Ch. Yu. J. (2014). Evaluation of restrictive competition in PPP projects using real option approach. *International Journal of Project Management*, *32*(3), 473–481. https://doi.org/10.1016/j.ijproman.2013.07.007

Liu, T., Wang, Y., & Wilkinson, S. (2016b). Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public-Private Partnerships (PPPs): A comparative analysis of Australia and China. *International Journal of Project Management*, *34*(4), 701–716. https://doi.org/10.1016/j.ijproman.2016.01.004

Liyanapathirana, D., Adeniyi, O., & Rathnasiri, P. (2023). Tactical conflict prevention strategies in Public-Private Partnerships: Lessons from experts. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *16*(1). https://doi.org/10.1061/jladah.ladr-996

Ma, L., Hu, Ya., Zhu, L., & Ke, Y. (2023). Are public-private partnerships still an answer for social infrastructure? A systematic literature review. *Frontiers of Engineering Management*, *10*(3), 467–482. https://doi.org/10.1007/s42524-023-0249-1

Marques, R. C. (2021). Public interest and early termination of PPP contracts. Can fair and reasonable compensations be determined? *Utilities Policy*, *73*, 101301. https://doi.org/10.1016/j.jup.2021.101301

Mirzaee, A. M., & Sardroud, J. M. (2022). Public-private-partnerships /PPP enabled smart city funding and financing. In J. R. Vacca (Ed.), *Smart Cities Policies and Financing. Approaches and Solutions* (Chapter 9, pp. 117–131). https://doi.org/10.1016/B978-0-12-819130-9.00011-5

Moffatt, S., & Kohler, N. (2008). Conceptualizing the built environment as a social–ecological system. *Building Research & Information: Developing theories of the built environment*, *36*(3), 248–268. https://doi.org/10.1080/09613210801928131

Noring, L. (2019). Public asset corporation: A new vehicle for urban regeneration and infrastructure finance. *Cities*, *88*, 125–135. https://doi.org/10.1016/j.cities.2019.01.002

Ojelabi, L. A., & Noone, M. A. (2020). Jurisdictional perspectives on alternative dispute resolution and access to justice: introduction. *International Journal of Law in Context*, *16*(2), 103–107. https://doi.org/10.1017/S1744552320000087

Outhuijse, A. (2020). The effective public enforcement of the prohibition of anti-competitive agreements: Which factors influence the high percentage of annulments of Dutch cartel fines? *Journal of Antitrust Enforcement*, *8*(1), 124–164. https://doi.org/10.1093/jaenfo/jnz020

Owen, B., Sun, S., & Zheng, W. (2007). China's competition policy reforms: The anti-monopoly law and beyond. *Stanford Law and Economics Olin Working Paper*, *339*. https://doi.org/10.2139/ssrn.978810

Rossi, M., & Civitillo, R. (2014). Public Private Partnerships: A general overview in Italy. *Procedia-Social and Behavioral Sciences*, *109*, 140–149. https://doi.org/10.1016/j.sbspro.2013.12.434

Rufín, C., & Rivera-Santos, M. (2012). Between commonweal and competition: Understanding the governance of public-private partnerships. *Journal of Management*, *38*(5), 1634–1654. https://doi.org/10.1177/0149206310373948

Rybnicek, R., Plakolm, Ju., & Baumgartner, L. (2020). Risks in Public-Private Partnerships: A systematic literature review of risk factors, their impact and risk mitigation. *Public Performance & Management Review*, *43*(5), 1174–1208. https://doi.org/10.1080/15309576.2020.1741406

Salem, D. (1981). The Joint Venture Law of the Peoples' Republic of China: Business and Legal Perspective. *Maryland Journal of International Law*, *7*(1), 73–118

Selim, A., & ElGohary, A. S. (2020). Public-private partnerships (PPPs) in smart infrastructure projects: the role of stakeholders. *HBRC Journal*, *16*(1), 317–333. https://doi.org/10.1080/16874048.2020.1825038

Sharma, Ch. (2022). Who does it better and why? Empirical analysis of public-private partnership in infrastructure in Asia-Pacific. *Property Management*, *41*(3), 309–335. https://doi.org/10.1108/PM-07-2022-0050

Soomro, N.-E-H., & Yuhui, W. (2023). Appraisal of existing evidences of competition law and policy: Bilateral legislative developments of Sino-Pak. *Heliyon*, *9*(8). https://doi.org/10.1016/j.heliyon.2023.e18935

Wang, H., Liu, Yu., Xiong, W., & Zhu, D. (2019). Government support programs and private investments in PPP Markets. *International Public Management Journal*, *22*(3), 499–523. https://doi.org/10.1080/10967494.2018.1538025

Wang, Y. (2003). A broken fantasy of Public-Private Partnerships. *Public Administration Review*, *69*(4), 779–782. https://doi.org/10.1111/j.1540-6210.2009.02025.x

Wegrich, K., Kostka, G., & Hammerschmid, G. (Eds.) (2017). *The governance of infrastructure*: Hertie Governance Report. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198787310.001.0001

Whiteside, H. (2020). Public-private partnerships: market development through management reform. *Review of International Political Economy*, *27*(4), 880–902. https://doi.org/10.1080/09692290.2019.1635514

Yurdakul, H., Kamaşak, R., & Öztürk, T. Ya. (2022). Macroeconomic drivers of Public Private Partnership (PPP) projects in low income and developing countries: A panel data analysis. *Borsa Istanbul Review*, *22*(1), 37–46. https://doi.org/10.1016/j.bir.2021.01.002

Сведения об авторе

Молинтас Доминик Т. – научный сотрудник, Колледж аэронавтики PATTS; магистр, Университет Гриффита
Адрес: Филиппины, Параньяк, авеню Ломбос, Сан Исидро 1700; Австралия, Квинсленд, Натан, QLD 4111
E-mail: dmolintas@asia.com
ORCID ID: https://orcid.org/0000-0002-4063-3983
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KHE-0949-2024
Google Scholar ID: https://scholar.google.com/citations?user=G8imOMYAAAAJ

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

История статьи

Дата поступления – 16 января 2024 г.
Дата одобрения после рецензирования – 12 февраля 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:347.4:004.4
EDN: https://elibrary.ru/lvpigr
DOI: https://doi.org/10.21202/jdtl.2024.22

Public-Private Partnership Agreement in the Context of the Matrix for Assessing their Legal Parameters and Digitalization

Dominique T. Molintas

PATTS College of Aeronautics, Paranaque, Philippines;
Griffith University, Queensland, Australia

Keywords

agreement,
conflict of interest,
contract,
digital technologies,
digitalization,
law,
legal assessment,
public-private partnership,
restraint of competition,
risk management

Abstract

Objective: by reviewing the legal aspects of public-private partnership agreements, to synthesize their main provisions into a common matrix, which, when digitized, can be used to standardize and simplify the formulation of agreement parameters.

Methods: the author relied on comparative-legal analysis of scientific literature, legislation and Internet sources on public-private partnership, supplemented by a review of public-private partnership agreements in various socio-political spheres, which made it possible to create a science-based and practice-oriented matrix that can serve as a tool for drafting public-private partnership agreements.

Results: national aspects in the legal regulation of the said relations in different countries were highlighted; a number of peculiarities encountered in public-private partnership agreements were described.

Scientific novelty: taking into account the most important legal peculiarities characteristic of different countries, a matrix for drafting public-private partnership agreements is presented, including eight main parameters: 1 – value received, scope, benefits and risks, 2 – route to market, 3 – restraint of competition, 4 – conflict of interest and procurement issues, 5 – powers, approvals, legal assessment, 6 – liabilities, dispute resolution, 7 – ownership structure, governance and level of autonomy, 8 – exit strategies. Depending on the priorities identified, the matrix can be modified, taking into account that priorities define and shape the specific parameters of each individual partnership.

Practical significance: the matrix obtained can become a planning tool used to analyze and understand the relationships between the eight legal parameters necessary for the formation of relations in the sphere of public-private partnership. It may serve as a legal reference point for the formulation of public-private partnership agreements around the world, and will contribute not only to the revitalization of public-private partnerships, but also to a proper understanding of obligations, responsibilities and limitations. The recommendations provided in the study show direction for the evaluation of public-private partnerships, allowing clear conclusions to be drawn about the partnership. Digital accessibility provided, the proposed matrix will be of interest to many organizations that use public-private partnerships in their professional activities.

For citation

Molintas, D. T. (2024). Public-Private Partnership Agreement in the Context of the Matrix for Assessing their Legal Parameters and Digitalization. *Journal of Digital Technologies and Law, 2*(2), 430–449. https://doi.org/10.21202/jdtl.2024.22

References

Azarian, M., Shiferaw, A. T., Lædre, O., Wondimu, P. A., & Stevik, T. K. (2023). Project ownership in public-private partnership (PPP) projects of Norway. *Procedia Computer Science*, *219*, 1838–1846. https://doi.org/10.1016/j.procs.2023.01.481

Biygautane, Mh., Neesham, C., & Al-Yahya, Kh. O. (2020). Institutional entrepreneurship and infrastructure public-private partnership (PPP): Unpacking the role of social actors in implementing PPP projects. *International Journal of Project Management*, *37*(1), 192–219. https://doi.org/10.1016/j.ijproman.2018.12.005

Bradshaw, C. (1963). Joint Ventures in Japan. *Washington Law Review*, *38*(1), 58–104.

Buso, M., Dosi, C., & Moretto, M. (2021). Do exit options increase the value for money of public–private partnerships? *Journal of Economics & Management Strategy*, *30*(4), 721–742. https://doi.org/10.1111/jems.12440

Caperchione, E., Demirag, I., & Grossi, G. (2017). Public sector reforms and public private partnerships: Overview and research agenda. *Accounting Forum*, *41*(1), 1–7. https://doi.org/10.1016/j.accfor.2017.01.003

Chen, Ch., & Hubbard, M. (2012). Power relations and risk allocation in the governance of public private partnerships: A case study from China. *Policy and Society*, *31*(1), 39–49. https://doi.org/10.1016/j.polsoc.2012.01.003

Chou, J.-Sh., & Lin, Ch. (2012). Predicting disputes in Public-Private Partnership projects: Classification and ensemble models. *Journal of Computing in Civil Engineering*, *27*(1). https://doi.org/10.1061/(ASCE)CP.1943-5487.0000197

Darko, D., Zhu, D., Quayson, M., Hossin, M. A., Omoruyi, O., & Bediako, A. K. (2023). A multicriteria decision framework for governance of PPP projects towards sustainable development. *Socio-Economic Planning Sciences*, *87*(B), 101580. https://doi.org/10.1016/j.seps.2023.101580

Demirag, I., Khadaroo, I., Stapleton, P., & Stevenson, C. (2011). Risks and the financing of PPP: Perspectives from the financiers. *The British Accounting Review*, *43*(4), 294–310. https://doi.org/10.1016/j.bar.2011.08.006

DoD NASA. (2020). *Proposed Rules. Federal Register*, *85*(109), 34561–34569.

Garg, S., & Garg, S. (2016). Rethinking Public-Private Partnerships: An unbundling approach. *Transportation Research Procedia* (Vol. 25, pp. 3789–3807). https://doi.org/10.1016/j.trpro.2017.05.241

González-Ruiz, Ju. D., Botero-Botero, S., & Duque-Grisales, E. (2018). Financial eco-innovation as a mechanism for fostering the development of sustainable infrastructure systems. *Sustainability*, *10*(12), 4463. https://doi.org/10.3390/su10124463

Hart, O. (2003). Incomplete contracts and public ownership: Remarks, and an application to public-private partnerships. *The Economic Journal*, *113*(486), C69–C76. https://doi.org/10.1111/1468-0297.00119

Hennessey, K. (2021). Comment on «When and how to use Public-Private Partnerships in infrastructure: Lessons from the international experience». In E. Glaeser, & J. Poterba (Eds.), *Economic Analysis and Infrastructure Investment* (pp. 365–368). Cambridge: National Bureau of Economic Research.

Hurk, M. van den, Brogaard, L., Lember, V., Petersen, O. H., & Witz, P. (2016). National varieties of Public-Private Partnerships (PPPs): A comparative analysis of PPP-supporting units in 19 European Countries. *Journal of Comparative Policy Analysis: Research and Practice*, *18*(1), 1–20. https://doi.org/10.1080/13876988.2015.1006814

Ito, S. (2020). *Infrastructure Development and Public-Private Partnership.* Singapore: Springer Nature Singapore Pte Ltd.

Jayachandran, S. (2021). *How economic development influences the environment*. Cambridge: National Bureau of Economic Research. https://doi.org/10.3386/w29191

Jin, Zh., & Huang, Ch. (2021). Tax enforcement and corporate donations: evidence from Chinese 'Golden Tax Phase III'. *China Journal of Accounting Studies*, *9*(4), 526–548. https://doi.org/10.1080/21697213.2022.2053375.

Jokar, E., Aminnejad, B., & Lork, A. (2021). Assessing and prioritizing risks in Public-Private Partnership (PPP) projects using the integration of fuzzy multi-criteria decision-making methods. *Operations Research Perspectives*, *8*, 100190. https://doi.org/10.1016/j.orp.2021.100190

Khallaf, R., Naderpajouh, N., & Hastak, M. (2021). Robust decision-making for multiparty renegotiations in Public-Private Partnerships. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *13*(3). https://doi.org/10.1061/(ASCE)LA.1943-4170.0000473

Kurniawan, F., Mudjanarko, S. W., & Ogunlana, S. O. (2015). Best practice for financial models of PPP projects. In *Procedia Engineering* (Vol. 125, pp. 124–132). https://doi.org/10.1016/j.proeng.2015.11.019

Lee, E. Y.-J. (2003). The Special Economic Zones and North Korean economic Reformation with a viewpoint of international law. *Fordham International Law Journal*, *27*(4), 1343–1378.

Leigland, J. (2018). Public-Private partnerships in developing countries: The emerging evidence-based critique. *The World Bank Research Observer*, *33*(1), 103–134. https://doi.org/10.1093/wbro/lkx008

Lemley, M., & McCreary, A. (2019, December 19). Exit strategy. *Stanford Law and Economics Olin Working Paper*, 542.

Liu, J., Gao, R., Cheah, Ch., & Luo, J. (2016). Incentive mechanism for inhibiting investors' opportunistic behavior in PPP projects. *International Journal of Project Management*, *34*(7), 1102–1111. https://doi.org/10.1016/j.ijproman.2016.05.013

Liu, J., Yu, X., & Cheah, Ch. Yu. J. (2014). Evaluation of restrictive competition in PPP projects using real option approach. *International Journal of Project Management*, *32*(3), 473–481. https://doi.org/10.1016/j.ijproman.2013.07.007

Liu, T., Wang, Y., & Wilkinson, S. (2016). Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public-Private Partnerships (PPPs): A comparative analysis of Australia and China. *International Journal of Project Management*, *34*(4), 701–716. https://doi.org/10.1016/j.ijproman.2016.01.004

Liyanapathirana, D., Adeniyi, O., & Rathnasiri, P. (2023). Tactical conflict prevention strategies in Public-Private Partnerships: Lessons from experts. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *16*(1). https://doi.org/10.1061/jladah.ladr-996

Ma, L., Hu, Ya., Zhu, L., & Ke, Y. (2023). Are public-private partnerships still an answer for social infrastructure? A systematic literature review. *Frontiers of Engineering Management*, *10*(3), 467–482. https://doi.org/10.1007/s42524-023-0249-1

Marques, R. C. (2021). Public interest and early termination of PPP contracts. Can fair and reasonable compensations be determined? *Utilities Policy*, *73*, 101301. https://doi.org/10.1016/j.jup.2021.101301

Mirzaee, A. M., & Sardroud, J. M. (2022). Public-private-partnerships /PPP enabled smart city funding and financing. In J. R. Vacca (Ed.), *Smart Cities Policies and Financing. Approaches and Solutions* (Chapter 9, pp. 117–131). https://doi.org/10.1016/B978-0-12-819130-9.00011-5

Moffatt, S., & Kohler, N. (2008). Conceptualizing the built environment as a social–ecological system. *Building Research & Information: Developing theories of the built environment*, *36*(3), 248–268. https://doi.org/10.1080/09613210801928131

Noring, L. (2019). Public asset corporation: A new vehicle for urban regeneration and infrastructure finance. *Cities*, *88*, 125–135. https://doi.org/10.1016/j.cities.2019.01.002

Ojelabi, L. A., & Noone, M. A. (2020). Jurisdictional perspectives on alternative dispute resolution and access to justice: introduction. *International Journal of Law in Context*, *16*(2), 103–107. https://doi.org/10.1017/S1744552320000087

Outhuijse, A. (2020). The effective public enforcement of the prohibition of anti-competitive agreements: Which factors influence the high percentage of annulments of Dutch cartel fines? *Journal of Antitrust Enforcement*, *8*(1), 124–164. https://doi.org/10.1093/jaenfo/jnz020

Owen, B., Sun, S., & Zheng, W. (2007). China's competition policy reforms: The anti-monopoly law and beyond. *Stanford Law and Economics Olin Working Paper*, *339*. https://doi.org/10.2139/ssrn.978810

Rossi, M., & Civitillo, R. (2014). Public Private Partnerships: A general overview in Italy. *Procedia-Social and Behavioral Sciences*, *109*, 140–149. https://doi.org/10.1016/j.sbspro.2013.12.434

Rufín, C., & Rivera-Santos, M. (2012). Between commonweal and competition: Understanding the governance of public-private partnerships. *Journal of Management*, *38*(5), 1634–1654. https://doi.org/10.1177/0149206310373948

Rybnicek, R., Plakolm, Ju., & Baumgartner, L. (2020). Risks in Public-Private Partnerships: A systematic literature review of risk factors, their impact and risk mitigation. *Public Performance & Management Review*, *43*(5), 1174–1208. https://doi.org/10.1080/15309576.2020.1741406

Salem, D. (1981). The Joint Venture Law of the Peoples' Republic of China: Business and Legal Perspective. *Maryland Journal of International Law*, *7*(1), 73–118

Selim, A., & ElGohary, A. S. (2020). Public-private partnerships (PPPs) in smart infrastructure projects: the role of stakeholders. *HBRC Journal*, *16*(1), 317–333. https://doi.org/10.1080/16874048.2020.1825038

Sharma, Ch. (2022). Who does it better and why? Empirical analysis of public-private partnership in infrastructure in Asia-Pacific. *Property Management*, *41*(3), 309–335. https://doi.org/10.1108/PM-07-2022-0050

Soomro, N.-E-H., & Yuhui, W. (2023). Appraisal of existing evidences of competition law and policy: Bilateral legislative developments of Sino-Pak. *Heliyon*, *9*(8). https://doi.org/10.1016/j.heliyon.2023.e18935

Wang, H., Liu, Yu., Xiong, W., & Zhu, D. (2019). Government support programs and private investments in PPP Markets. *International Public Management Journal*, *22*(3), 499–523. https://doi.org/10.1080/10967494.2018.1538025

Wang, Y. (2003). A broken fantasy of Public-Private Partnerships. *Public Administration Review*, *69*(4), 779–782. https://doi.org/10.1111/j.1540-6210.2009.02025.x

Wegrich, K., Kostka, G., & Hammerschmid, G. (Eds.) (2017). *The governance of infrastructure*: Hertie Governance Report. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198787310.001.0001

Whiteside, H. (2020). Public-private partnerships: market development through management reform. *Review of International Political Economy*, *27*(4), 880–902. https://doi.org/10.1080/09692290.2019.1635514

Yurdakul, H., Kamaşak, R., & Öztürk, T. Ya. (2022). Macroeconomic drivers of Public Private Partnership (PPP) projects in low income and developing countries: A panel data analysis. *Borsa Istanbul Review*, *22*(1), 37–46. https://doi.org/10.1016/j.bir.2021.01.002

Author information

Dominique T. Molintas – Researcher, PATTS College of Aeronautics; Graduate Student, Griffith Graduate Research School, Griffith University
Address: Nathan, QLD 4111, Queensland, Australia; Lombos Avenue, San Isidro 1700, Paranaque, Philippines
E-mail: dmolintas@asia.com
ORCID ID: https://orcid.org/0000-0002-4063-3983
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KHE-0949-2024
Google Scholar ID: https://scholar.google.com/citations?user=G8imOMYAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – January 16, 2024
Date of approval – February 12, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:17:004.8
EDN: https://elibrary.ru/fsfsnq
DOI: https://doi.org/10.21202/jdtl.2024.23

Этическое и правовое регулирование использования искусственного интеллекта в Марокко

Хамза Джабир ✉
Университет Ибн Зохр, Агадир, Марокко

Камаль Лагтати
Университет Ибн Зохр, Агадир, Марокко

Денис Поэ-Токпа
Университет Бордо, Пессак, Франция

Ключевые слова

«жесткое право», законодательство Марокко, искусственный интеллект, моральные ценности, «мягкое право», принцип технологической реальности, правовое регулирование, правовые риски, цифровые технологии, этические принципы

Аннотация

Цель: поиск и определение проблем и возможностей этического и правового регулирования искусственного интеллекта на примере опыта цифровых преобразований в Марокко.

Методы: исследование проведено с использованием аналитического и сравнительного подходов к решению возникающих юридических вопросов, обусловленных развитием искусственного интеллекта. За основу традиционного научного метода в праве взят правовой анализ, который применялся к изучению юридических текстов, научной литературы, диагностике состояний и условий изучаемой области на национальном и международном уровне. Наряду с этим использовался сравнительный подход в праве, позволивший рассмотреть законодательство Марокко в сопоставлении с законодательством других стран.

Результаты: осуществлен обзор научной литературы, посвященной правовым и этическим вопросам использования искусственного интеллекта. Проведен обзор юридических текстов и директив, разработанных на национальном и международном уровне и имеющих прямую или косвенную связь с использованием искусственного интеллекта. Приводится сравнение законодательства Марокко с соответствующими правовыми актами других стран. Полученные выводы свидетельствуют о том, что в отсутствие специальной правовой базы для систем искусственного интеллекта предпочтительным является

✉ Контактное лицо

принятие этических стандартов в виде руководящих принципов, руководства по передовой практике и этических хартий. Эти механизмы представляются жизнеспособной альтернативой правовому регулированию. В этом смысле было предпринято несколько инициатив по продвижению «мягкого права», которое направлено на поощрение надлежащего поведения технологических агентов.

Научная новизна: анализ цифровых преобразований в Марокко позволил представить комплексный взгляд на роль этических аспектов и обеспечение достаточности закона для реагирования на изменения современного общества, трансформирующегося в свете развития искусственного интеллекта.

Практическая значимость: проведенное исследование позволяет обозначить пути поиска более гибкого баланса между «мягким» и «жестким» правом в регулировании отношений с учетом технологической реальности, что должно поощрять надлежащее поведение технологических агентов и положительно влиять на специфику современной ситуации, когда «жесткое право» медленно осознает и решает проблемы, связанные с регулированием цифровых технологий, а также медленно учитывает возможные риски, которые несет в себе искусственный интеллект и недостаточность регулирования связанных с ним отношений.

Для цитирования

Джабир, Х., Лагтати, К., Поэ-Токпа, Д. (2024). Этическое и правовое регулирование использования искусственного интеллекта в Марокко. *Journal of Digital Technologies and Law*, *2*(2), 450–472. https://doi.org/10.21202/jdtl.2024.23

Содержание

Введение

В последние годы искусственный интеллект (далее – ИИ) находится в центре всеобщего внимания, так как все больше компаний используют его интенсивно и разнообразно. ИИ – это «компьютерная система, которая работает на основе дублирования или имитации принципов мышления, интеллекта или, другими словами, определенных действий человека» (Bertrand, 2010). С увеличением разнообразия средств связи, новых возможностей сбора и алгоритмической обработки данных

в настоящее время наблюдается появление технологий, связанных с Big Data, подключенными объектами, алгоритмами, блокчейном и искусственным интеллектом. Этот многогранный цифровой феномен объединяет различные вселенные; растут скорость, синхронность работы и другие возможности цифровых технологий. Вместе с объектами, связанными с этими технологиями, это явление получило название «новые информационные и коммуникационные технологии» (НИКТ) (Soulez, 2018).

Действительно, искусственный интеллект развивается чрезвычайно быстрыми темпами, и компании все чаще оказываются в положении, когда они вынуждены, с одной стороны, приобретать эти технологии, чтобы оставаться конкурентоспособными, а с другой – учиться работать с ними, чтобы избежать различных предубеждений, которые могут оказаться вредными. Искусственный интеллект таит в себе большой потенциал, но также вызывает и сильные опасения. Последние связаны с теми рисками, которые необходимо устранить или ограничить, чтобы гарантировать внедрение технологий, соответствующее правовым нормам, моральным ценностям и этическим принципам, а также способствующее всеобщему благу.

По данным ЮНЕСКО, риски, связанные с искусственным интеллектом, имеют три составляющих[1]: нехватку работ, выполняемых машинами вместо людей; последствия для независимости человека, в частности его свободы и безопасности; отчуждение человечества, которое в катастрофическом антиутопическом сценарии может совсем исчезнуть, будучи замененным интеллектуальными машинами (Franchomme & Jazottes, 2021). Более того, использование технологий искусственного интеллекта уже создало новые проблемы. Оно подразумевает трансформацию общества, что создает необходимость переосмысления этических аспектов и обеспечения достаточности закона для реагирования на эти изменения.

Многочисленные инициативы по регулированию искусственного интеллекта сходятся на важности этики в этой области, даже при ее слабом влиянии на функционал ИИ (Merabet, 2018). Этические вопросы стали приниматься во внимание лишь недавно, потому что право медленно осознает проблемы, связанные с цифровыми технологиями, и принимает законодательные меры по их решению. Прежде чем рассматривать практику регулирования, необходимо признать, что права человека применимы к цифровому миру. Этому помогает то, что этические вопросы «мягкого права» рассматриваются на глобальном уровне и границы не являются реальным препятствием, как в случае с созданием нормативной базы «жесткого права» (Cath, 2018).

Поэтому необходимо включить этические вопросы в цифровые проекты, связанные с искусственным интеллектом (Cath, 2018). Так, профессиональными ассоциациями, частными компаниями и рядом международных организаций были разработаны стандарты, хартии и руководства, касающиеся вопросов алгоритмических систем, прозрачности, неприкосновенности частной жизни, конфиденциальности, беспристрастности и в целом разработки этических систем (Bensamoun & Loiseau, 2017a).

Марокко стала одной из первых стран, присоединившихся к рекомендациям ЮНЕСКО по этике искусственного интеллекта (Rochd et al., 2021). Это первый

[1] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, adopted on the sidelines of the 41st session of the UNESCO General Conference held in November 2021 in Paris.

глобальный нормативный документ в данной области. Об этом заявил министр национального образования, дошкольного воспитания и спорта в кулуарах подписания соглашения с ЮНЕСКО в рамках CONFINTEA VII, проходившей в Марракеше в июне 2022 г. Королевство Марокко официально внедрило рекомендации ЮНЕСКО об этике искусственного интеллекта, принятые в рамках 41-й сессии Генеральной конференции ЮНЕСКО, состоявшейся в ноябре 2021 г. в Париже (Benhanou, 2017).

Функционал искусственного интеллекта в деятельности компании сложно описать исчерпывающим образом, так как он расширяется с каждым днем. В настоящее время ИИ дает возможность организациям все больше автоматизировать и оптимизировать определенные задачи, тем самым играя важную роль в изменении профессиональной деятельности, создавая ее новые формы и организационные решения (Benhanou, 2017). Искусственный интеллект уже стал неотъемлемой частью повседневной жизни и в ближайшие годы должен еще более интегрироваться в нее. Это порождает ряд проблем, но также открывает новые перспективы для отдельных лиц, организаций и структур. Использование искусственного интеллекта в повседневной жизни поднимает множество этических вопросов, тесно связанных с правовой сферой, поскольку закон является гарантом защиты основных прав и только он может ограничить или запретить определенные практики. Например, если говорить о вреде для окружающей среды, то в 2020 г. цифровые технологии стали причиной от 1,8 до 6,3 % выбросов углекислого газа в мире.

В свете особенностей искусственного интеллекта крайне важно рассмотреть правовые последствия его применения. При этом необходимо обеспечить подотчетность всех заинтересованных сторон и предотвратить возможные злоупотребления. Нельзя мириться с правовым вакуумом в сфере искусственного интеллекта. Поэтому представляется необходимым задуматься о роли этики в создании правовых норм при использовании искусственного интеллекта в компаниях.

При проведении данного исследования были использованы традиционные научные методы: анализ юридических текстов, научной литературы, диагностика состояния и условий изучаемой области на национальном и международном уровнях. Для изучения проблемы нашего исследования был осуществлен обзор научной литературы, посвященной правовым и этическим вопросам использования искусственного интеллекта. Кроме того, мы провели обзор юридических текстов и директив, разработанных на национальном и международном уровнях и имеющих прямую или косвенную связь с использованием искусственного интеллекта, а также сравнили законодательство Марокко с соответствующими правовыми актами других стран. На международном уровне мы изучили директивы и резолюции, принятые различными организациями или международными органами.

1. Появление искусственного интеллекта: возможность или угроза?

Искусственный интеллект уже оказывает влияние практически на все сферы повседневной жизни. В его основе лежит процесс имитации человеческого интеллекта, который базируется на создании и применении алгоритмов. Искусственный интеллект таит в себе огромный потенциал и предоставляет множество возможностей для всех стран мира. С другой стороны, использование этой технологии уже создало новые проблемы и вызывает опасения по поводу рисков, которые она представляет для функционирования организаций (1.2), сферы трудовых отношений и основных прав и свобод (1.1).

1.1. Искусственный интеллект и защита основных прав и свобод

Действительно, искусственный интеллект предоставляет все больше возможностей для создания новых решений, направленных на улучшение жизни людей, укрепление гарантий здоровья и благополучия человечества (Soulez, 2018). Эти интеллектуальные технологии содержат риски для осуществления основных прав и свобод. Именно в этом смысле комиссия Европейского совета заявила, что «использование алгоритмических систем с возможностями автоматизированного сбора данных, анализа решений, оптимизации или машинного обучения может иметь негативные последствия для осуществления, реализации и защиты основных прав и свобод человека»[2].

Дело в том, что искусственный интеллект позволяет собирать и обрабатывать огромное количество данных. Они собираются с помощью приложений (электронный пропуск, геолокация, видеонаблюдение и т. д.) и могут использоваться для назначения и выплаты вознаграждения, управления режимом труда и отдыха сотрудников, контроля исполнения задач и соблюдения дисциплины[3]. Различные технологии, используемые на рабочем месте, могут оказывать влияние на права и свободы сотрудников (Desbarats, 2020) и даже затрагивать права кандидатов в процессе найма, организованного компанией (Desbarats, 2020).

Поскольку искусственный интеллект в процессе своей работы опирается на данные, проблема персональных данных является одной из самых важных в этой сфере. Она заключается в том, что алгоритмам необходимо обработать огромное количество данных, чтобы принять решение. Такая ситуация может противоречить принципам сбора и использования данных, установленным действующим законодательством Марокко. Фактически это принципы минимизации данных и установления ограничений в зависимости от целей сбора данных, которые предусмотрены Законом 09-08 о защите физических лиц в отношении обработки персональных данных.

Важно отметить, что использование приложений искусственного интеллекта уже давно обосновано технологической природой этих приложений, поскольку они позволяют избежать любых предрассудков и ненамеренной дискриминации со стороны человека. Таким образом, искусственный интеллект может подорвать человеческие ценности и принципы, лежащие в основе Всеобщей декларации прав человека. Он также может привести к нарушению основных прав и свобод, таких как свобода выражения мнений и собраний, путем фильтрации и удаления контента. Это относится к таким аспектам, как человеческое достоинство, дискриминация по признаку пола, расы или этнического происхождения, религии или убеждений и, в зависимости от обстоятельств, защита персональных данных, уважение частной жизни или право на эффективную судебную защиту и справедливое судебное разбирательство, а также защита прав потребителей.

Следует также отметить, что искусственный интеллект породил новые вопросы и проблемы с точки зрения этики и защиты данных, которые необходимо решать на политическом уровне с помощью тщательной разработки мер для достижения

---

2 Counsil of Europe. (2018, November 12). Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems. https://clck.ru/3B46zf

3 (Michaud, 2021); usages et régulations, conférence de l'université de Toulouse à titre de "l'année universitaire" 2019–2020.

баланса и соответствия нормативным положениям. Обрабатываемые данные часто носят личный характер, могут описывать поведение человека и быть конфиденциальными; это, например, информация о здоровье и биометрические данные. Они могут иметь потенциальные последствия для неприкосновенности частной жизни и этики, осложняя проблему защиты личной информации в будущем, когда появится искусственный интеллект. Действительно, если персональные данные – это новое Эльдорадо, то их эксплуатация с помощью сверхсложных и идеологически предвзятых алгоритмов может привести к созданию новых форм рабства или, по крайней мере, дистанционного контроля над коллективным и индивидуальным поведением (Barraud, 2019). Это технологическое регулирование, угрожающее свободе воли каждого индивида, и алгоритмы могут нести в себе грозные, хотя поначалу неощутимые нормативные последствия (Marique & Stronwel, 2017).

Учитывая возможности искусственного интеллекта, его интеграция в правовую сферу может послужить катализатором социального и технического прогресса, выгодного как профессионалам в области права, так и участникам судебных процессов. «Нет сомнений в том, что некоторые приложения искусственного интеллекта, которые в настоящее время разрабатываются или находятся на стадии эксперимента (например, направленные на ускорение правовых исследований), могут быть очень полезными и сделать судебную работу более быстрой и эффективной. Необходимо поддерживать использование искусственного интеллекта, который, с одной стороны, находится на службе у профессионалов системы правосудия и соответствует их потребностям, а с другой – уважает права личности, гарантированные Всеобщей декларацией» (Boy, Racine, & Siiriaien, 2009). Искусственный интеллект не просто инструмент для повышения эффективности судебной сферы, он должен укреплять, а не снижать гарантии верховенства закона и качество государственной системы правосудия.

1.2. Искусственный интеллект: инструмент для компаний

Технологический прогресс придает деловой среде новый динамизм, ставя перед компаниями все более сложные задачи. В ходе промышленной революции новые технологии существенно повлияли на организацию и управление компаниями, что привело к их цифровой трансформации и оптимизации операционных моделей с приоритетным использованием ИТ-ресурсов для улучшения продуктов и услуг, создания более тесных партнерств нового поколения и немедленного реагирования на ожидания клиентов.

Действительно, искусственный интеллект заставил мир бизнеса бурно развиваться[4]. Масштабы этих изменений доходят даже до «запрограммированного» исчезновения некоторых видов деятельности во многих отраслях (промышленность, банковское дело, финансы, торговля и т. д.). Речь идет также о том, что роботы должны более или менее ощутимым образом «увеличить» физический и когнитивный потенциал человека на рабочем месте, одновременно снижая монотонность труда и помогая ему. С появлением приложений искусственного интеллекта ряд

[4] N. Le Ru. (2016). l'effet de l'automatisation sur l'emploi: ce qu'on sait et ce qu'on ignore, France stratégie. La note d'analyse, no 49 juillet 2016: conseil d'orientations sur l'emploi, Automatisation, numérisation et emploi, t, 1, les impacts sur le volume, la structure et la localisation de l'emploi, janvier 2017.

профессий особенно сильно изменится; роботы постепенно будут интегрированы в датчики на основе искусственного интеллекта. Последний все чаще позволяет осуществлять «мягкое» взаимодействие между людьми и роботами. Эта революция должна благоприятно сказаться как на компаниях, так и на отдельных сотрудниках, которые смогут гораздо проще взаимодействовать с машиной, способной помочь им в решении сложных задач (Zouinar, 2020). Помогающие роботы приносят пользу компании, повышают производительность и гибкость, а также могут способствовать улучшению условий труда, снижению количества нарушений и обеспечению гибкой координации при выполнении задач внутри компании[5].

Отметим, что приложения, оснащенные искусственным интеллектом, специально разрабатываются для обеспечения удаленной и командной работы с использованием новых коммуникационных технологий; так работа может стать мобильной и дистанционной. Они также позволяют улучшить коммуникацию внутри компании, повысить уровень профессиональных и человеческих отношений, делая более доступной информацию о жизни в компании. Эти различные инструменты искусственного интеллекта дают новые возможности, позволяют оптимизировать рабочее время, выполнять новые задачи, снижать вероятность ошибки, а также снимать возможный стресс (Marique & Stronwel, 2017). Однако не менее велик риск изоляции работника, вторжения в его личную жизнь вездесущих информационных потоков и отношений, которые становятся исключительно цифровыми в ущерб человеческим.

В Марокко, как и в целом ряде других развивающихся стран, «большие данные» и алгоритмы открывают новые горизонты. Действительно, искусственный интеллект уже очень широко присутствует в нашей жизни через смартфоны, GPS и другие софты и все больше и больше через наши автомобили (Naim et al., 2021). То же самое можно сказать и о компаниях, где часто используется множество других инструментов, таких как автоматический перевод или чат-боты[6] для ответа клиентам через Интернет. Кроме того, технология преобразования речи в текст, основанная сразу на нескольких свойствах искусственного интеллекта, способна превратить любой аудиоконтент в письменный текст. Это позволяет компаниям экономить время, избавляя их от необходимости вручную набирать текст на клавиатуре. Таким образом, искусственный интеллект способствует разработке нового поколения продуктов и услуг с меньшими затратами.

Важно отметить, что в Марокко не все отрасли в одинаковой степени готовы к применению этого вида технологий. Мы все еще не можем говорить об использовании искусственного интеллекта в Марокко, по крайней мере, для большинства компаний (Ait El Bour & Lebzar, 2020). Сегодня компании работают с данными, пытаясь собрать их, оцифровать, сделать доступными и проанализировать (Bouanba et al., 2022; Mohamed-Amine et al., 2024). Это первый шаг к внедрению систем искусственного интеллекта. В настоящее время наиболее подвержены эволюции в сфере технологий такие секторы, как банковское дело, фондовый рынок, страхование, телекоммуникации и частично промышленность.

---

5 Atain-Kouadio, J. J., & Sghaier, A. (2017). Les robots et dispositifs d'assistance physique: état des lieux et enjeux pour la prévention. INRS, Note Scientifique et technique, NS 354. (In French).

6 Это персональный помощник, который быстро и верно отвечает на запросы тысяч клиентов, ищущих информацию или услугу. Чат-бот беседует с клиентом, соблюдая культуру и имидж компании или человека, который его использует.

В государственном секторе искусственный интеллект дает возможность улучшить качество обслуживания населения. Он позволяет предоставлять гражданам практическую информацию, тем самым облегчая их жизнь, модернизируя управление и государственные услуги. Системы с ИИ также способствуют участию в общественной жизни и стимулируют экономическое развитие за счет более эффективного предоставления и распространения информации. Они также позволяют развивать информационные технологии и создавать цифровую экономику, преодолевая консерватизм органов управления, и формировать экосистему для обеспечения сбалансированного общества знаний, в которое могут внести свой вклад различные стороны (Boubker, 2024).

Наконец, внедрение технологий искусственного интеллекта оказывает значительное влияние на производительность компаний, стимулирует их развитие и интернализацию, повышает эффективность и экономические результаты деятельности. Современные технологии искусственного интеллекта основаны на методах машинного обучения, который представляет собой математический инструмент самообучения алгоритмов. Компании все чаще инвестируют в технологии искусственного интеллекта, чтобы автоматизировать бизнес-процессы, улучшить процесс принятия решений и получать более точные рекомендации.

2. Регулирование искусственного интеллекта: моральная и правовая необходимость

Ускоренное развитие искусственного интеллекта в последние годы и возможность его внедрения во все отрасли и практически во все виды человеческой деятельности заставили задуматься о его правовых основах. Однако человечество еще только осваивается в этом мире без территории, поэтому защита цифровых прав и свобод должна основываться на определенных и четко установленных правовых принципах, а также на широком спектре инструментов регулирования.

Осознавая потенциал технологий в перспективе постковидной экономики, государства, однако, в равной степени осознают и их опасности. Кроме того, в каждой области применения (в самом широком смысле) использование искусственного интеллекта может вызвать вопросы и поставить под сомнение его этический и правовой характер. Ввиду сложности и разнообразия сфер применения искусственного интеллекта, а также их изменчивого и постоянного эволюционирующего характера необходимо принять гибкие инструменты «мягкого права» в виде руководящих принципов, этических хартий, кодексов поведения и других этических стандартов (2.1), прежде чем создавать правовые рамки для использования искусственного интеллекта (2.2).

2.1. Этические рамки для искусственного интеллекта

Относительная анархия в области развития искусственного интеллекта побудила участников процесса предложить нормативные рамки, чтобы снизить риски, которые несет в себе эта технология, и в то же время оптимизировать ее преимущества. Однако, осознавая важность норм, а также необходимость не ограничивать себя созданием корпуса правил, субъекты искусственного интеллекта призвали установить этические правила разработки и использования систем искусственного интеллекта на основе принципов, соответствующих конкретным интересам. В то же время государственные и частные субъекты во всем мире, осознавая риски неупорядоченной

и необъективной стандартизации, включились в гонку стандартов как на национальном, так и на международном уровнях (Thibout, 2019).

Такая динамика привела к появлению множества нормативных и этических кодексов при отсутствии международного консенсуса по созданию общих нормативных инструментов. Цель этих инициатив – реагировать на очевидную и явную обеспокоенность в связи с появлением искусственного интеллекта и его реальными или предполагаемыми опасностями. Идея заключается в том, что искусственный интеллект должен быть, от замысла до использования, «совместимым с этикой», т. е. соответствовать гуманистическим ценностям, присущим обществу. Другими словами, настало время воплотить в текстах хартий, этических кодексов, руководств по надлежащей практике, руководящих принципов этику использования приложений искусственного интеллекта (Jobin et al., 2019). В этом смысле внедрение искусственного интеллекта в общественную жизнь потребует разработки правил в виде гибкого закона, с активным вовлечением заинтересованных сторон в его создание (Bostrom & Yudkowsky, 2018).

Действительно, идея этики искусственного интеллекта состоит в том, что разработчики должны уважать человеческое достоинство и личную независимость в процессе исследования и разработки систем искусственного интеллекта. Например, они должны принимать необходимые меры, чтобы не вызывать дискриминацию, обусловленную предрассудками, которые могут проникнуть в обучающие данные для систем искусственного интеллекта. В контексте конкуренции на международном уровне и рисков искусственного интеллекта множатся инициативы по его регулированию, так как в значимости этики в этой области нет сомнений (Bufflier, 2020).

Этика, применяемая к искусственному интеллекту, находится в процессе разработки; существуют определенные международные стандарты, но они имеют значение «мягкого права». Таким образом, этика изначально имеет логику «мягкого права» и постепенно формулируется вокруг соблюдения норм.

Что касается международного уровня, то на Генеральной конференции ЮНЕСКО были приняты рекомендации по этике искусственного интеллекта. Их разработка основывалась на предварительном исследовании Всемирной комиссии по научным знаниям и технологиям (World Commission on Scientific Knowledge and Technology, COMEST) при ЮНЕСКО. Это первый международный нормативный документ по этике ИИ в форме рекомендаций, охватывающих все области ИИ путем разработки ключевых принципов и направляющих развитие и применение ИИ с учетом интересов человека. В тексте Рекомендаций говорится, что ЮНЕСКО «также убеждена в том, что всемирно признанные этические стандарты для технологий ИИ, полностью соответствующие международному праву, в частности законодательству о правах человека, могут сыграть ключевую роль в развитии норм, связанных с ИИ, во всем мире»[7].

Важно отметить, что в этой простой рекомендации, не имеющей обязательного характера, ЮНЕСКО вводит механизмы соблюдения норм, называемые «стратегическими механизмами» этики, и призывает государства-члены создать «стратегические рамки или механизмы» для оценки воздействия искусственного интеллекта на права человека, верховенство закона, демократию, этику, а также создать инструменты комплексной юридической оценки на основе Руководящих принципов

[7] The Preamble of the UNESCO Recommendation on the Ethics of Artificial Intelligence.

предпринимательской деятельности в аспекте прав человека, которые были разработаны ООН (Bostrom & Yudkowsky, 2018).

На европейском уровне начиная с 2018 г. работает комиссия Европейского совета, которая рассматривает искусственный интеллект в глобальном масштабе. Задача комиссии – обеспечить адекватные этические и правовые рамки в отношении ценностей ст. 2 Договора о Европейском союзе и Хартии основных прав Европейского союза. С этой целью комиссия предложила разработать проект этического руководства в области искусственного интеллекта. Эти руководящие принципы были опубликованы в 2019 г. и представляют собой надежную основу, из которой следуют этические принципы, которых должны придерживаться специалисты в области искусственного интеллекта. Это четыре этических принципа: уважение автономии человека, предотвращение вреда, справедливость и объяснимость.

Кроме того, в 2017 г. Европейский парламент принял резолюцию, содержащую «рекомендации по нормам гражданского права в области робототехники»[8]. Приложением к ней стала «Хартия по робототехнике», которая, по мнению специалистов, сводится к этическому «кодексу поведения» для инженеров-робототехников, «кодексу этики» для комитетов по этике и исследованиям, «лицензий» для разработчиков и пользователей. В этом же ключе Европейская комиссия разработала текст в виде «Европейской этической хартии по использованию искусственного интеллекта в судебных и сопутствующих им системах» (Bensoussan & Bensoussan, 2019). Она касается автоматизированной обработки судебных решений и судебных данных (с помощью машинного обучения). Хартия содержит целый ряд принципов, направленных на решение этических проблем искусственного интеллекта. Эти принципы нацелены на уважение фундаментальных ценностей, в частности принцип недискриминации и права на неприкосновенность частной жизни. Особое внимание в хартии уделяется также безопасности и прозрачности[9].

Осознавая риски, которые несет в себе искусственный интеллект, Марокко, со своей стороны, предприняло ряд инициатив в области цифровых преобразований. В 2011 г. в стране было создано Главное управление по безопасности информационных систем (General Directorate of Information Systems Security, DGSSI), задача которого – обеспечить поддержку и безопасность цифрового развития. Этот орган разработал стратегию, призванную сопровождать распространение коммуникационных и информационных технологий. Данная стратегия отвечает на новые вызовы, возникающие в связи с развитием цифровых пользователей и угрозами, связанными с этими технологиями[10].

---

8 Resolution of February 16, 2017 with recommendations to the Commission on civil law rules on robotics (2015/2103(INL)), Liability, item AF.

9 В 2020 г. Европейский парламент принял и другие резолюции: Резолюция Европейского парламента от 20 октября 2020 г. с рекомендациями для комиссии о правовых основах этики искусственного интеллекта и робототехники и связанных с ними технологий; Резолюция Европейского парламента от 20 октября 2020 г. с рекомендациями для комиссии о режиме гражданской ответственности для искусственного интеллекта. Voir, Y. Meneceur. (2019). Les enseignements des éthiques européennes de l'intelligence artificielle. La Semaine Juridique, 12, 552–558. (In French).

10 General Directorate for Information Systems Security. Stratégie Nationale en matière de cyber sécurité. https://clck.ru/3B49Gf

В 2017 г. в Марокко было также учреждено Агентство цифрового развития, занимающееся вопросами отношения человека к цифровым технологиям. Агентство готовит отчеты и организует широкие консультации с участием государственных и частных структур, чтобы внести вклад в создание более творческого и инновационного общества, а также выстроить новый баланс между экономическими и социальными вопросами, связанными с цифровыми технологиями. С принятием Закона 09-08 о защите физических лиц при обработке персональных данных в Марокко также была создана национальная комиссия по контролю над защитой персональных данных. Она отвечает за обеспечение защиты персональных данных, содержащихся в компьютерных файлах и на бумажных носителях, как в государственной, так и в частной сфере (Jaldi, 2022).

Отчеты этих учреждений служат источником справочной информации для регулирования использования технологий в Марокко (Ait El Bour & Lebzar, 2020). Королевство также присоединилось к рекомендациям ЮНЕСКО по этике искусственного интеллекта. Теперь предстоит создать комиссию, которая будет отвечать за вопросы искусственного интеллекта и его вызовы, безусловно следуя рекомендациям ЮНЕСКО, а также этическим хартиям и руководящим принципам, разработанным международными организациями.

Частные инициативы также играют ключевую роль в создании этических рамок использования искусственного интеллекта. В них участвуют все крупные игроки цифровой экономики. К примеру, партнерство «Partnership on AI»[11] было основано крупнейшими транснациональными компаниями – Google, Microsoft, Facebook[12], Amazon и Apple – для изучения и развития передового опыта в области технологий искусственного интеллекта, для углубления понимания общественностью сути ИИ и в качестве открытой платформы для обсуждения и взаимодействия в этой области и влияния ИИ на человека и общество (Bensamoun & Loiseau, 2017a).

Трудность, которую мы наблюдаем сегодня, заключается в том, что на практике этика, применяемая к искусственному интеллекту, сложна в своей реализации. Действительно, большое количество компаний, правительств, ассоциаций, государственных и частных организаций разрабатывают руководства по передовому опыту, рекомендации или просто дискутируют об этичности и ответственности искусственного интеллекта. Однако можно заметить, что эти субъекты испытывают трудности с внедрением указанных принципов в своей практике. В этом смысле актуальным решением может стать саморегулирование операторов, но только в том случае, если оно предполагает обязательность действий на более высоком уровне, согласно модели соответствия или подотчетности (Cath, 2018).

2.2. Необходимость правового режима, адаптированного к искусственному интеллекту

Проблема искусственного интеллекта стала стратегической, поскольку она касается практически всех сфер деятельности человека, от финансов до обороны, образования, логистики, здравоохранения и правосудия. В некоторых регионах мира ИИ уже

[11] Partnership on AI (PAI). www.Partnershiponai.org

[12] Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

стал необходимостью, и он стремится распространиться на всю планету. Это побуждает заинтересованных игроков разрабатывать нормативные рамки, чтобы ограничить риски, связанные с этой технологией, и оптимизировать ее преимущества. Однако внедрение правовой базы, которая бы строго регулировала разработку и использование систем искусственного интеллекта, сопряжено с рядом проблем. Во-первых, она не всегда желательна для определенных заинтересованных сторон, поскольку может противоречить их интересам, ограничивая их свободу действий. Во-вторых, она требует консенсуса, основанного на длительной дипломатической работе и сложных переговорах с различными государственными и частными субъектами. Такое регулирование должно оставлять как можно больше возможностей для развития и использования алгоритмических систем, которые несут много преимуществ человечеству. При этом необходимо гарантировать, что использование этих систем не навредит отдельным людям и обществу в целом.

Кроме того, если проблемы, создаваемые системами искусственного интеллекта, не будут регулироваться общим «законодательством об искусственном интеллекте» или «законодательством об алгоритмах», тогда гораздо более уместным будет сочетание общих и отраслевых стандартов. Действительно, можно наблюдать, что возможность надлежащим образом отвечать на новые вызовы, вероятно, потребует адаптации толкования и применения существующих стандартов.

Особо следует отметить, что законодательство Марокко не предусматривает специального регулирования искусственного интеллекта, как это происходит в большинстве развитых стран. Однако использование систем искусственного интеллекта связано с обработкой данных, к которым применяется Закон о защите персональных данных. Таким образом, представляется возможным принципиально решить проблемы, связанные с защитой частной жизни и защитой данных, с помощью уже имеющегося средства – законодательства о защите данных (Jaldi, 2022). Далее каждый раз, когда системы искусственного интеллекта задействуют персональные данные и информацию, находит свое применение Закон 09-08 о защите физических лиц в отношении обработки персональных данных.

Однако использование систем искусственного интеллекта приводит и к другим проблемам. Например, часто заинтересованные лица не осознают, что, имеют дело с применением этих систем и не понимают сути их функционирования. Кроме того, такие системы могут привести к дискриминации и манипулированию действиями людей. Вместе с тем, внедрение систем искусственного интеллекта ставит новые вопросы в области законодательства об ответственности. Во всех этих областях по-прежнему существует необходимость в регулировании, и это касается обеспечения безопасности автономных систем и определенных процедур авторизации.

Несомненно, в области систем искусственного интеллекта крайне важно наличие правовой базы, не препятствующей развитию технологии и предоставляющей гарантии при возможном ущербе. Для этого некоторые авторы предлагают создать электронную личность, наделив системы искусственного интеллекта юридическим статусом. Эта концепция электронной личности была очень быстро подвергнута критике на том основании, что такое решение может разрушить границы между человеком и машиной (Merabet, 2018). Очевидно, что вменить машине юридическую ответственность сложно; при этом решение, заключающееся в создании правосубъектности систем искусственного интеллекта, является чрезмерным и его необходимо отклонить. Такое решение может ограничить платежеспособность «робота-должника» и снизить ответственность его производителей (Bensamoun & Loiseau, 2017b).

С другой стороны, представляется разумным и обоснованным возложить ответственность на разработчика, производителя, владельца и пользователя искусственного интеллекта. Отметим, что одна из сложностей в области искусственного интеллекта заключается в том, что в его функционирование могут вмешиваться многие субъекты[13]. Таким образом, ответственность может лежать на уровне выбора, сбора и организации данных для обучения, разработки алгоритмов, реализации программного обеспечения, интерфейса и даже аппаратной части (Courtois, 2016). Другие участники могут нарушить работу систем, будь то злонамеренный пользователь или даже третья сторона, действующая недобросовестно. Представляется, что некоторые из этих субъектов могут нести определенную долю ответственности или даже что различные аспекты ответственности могут быть возложены на них совместно или раздельно.

Сегодня интеллектуальные машины наделены способностью принимать решения автономно и в отсутствие эффективного контроля со стороны человека. Это делает неприменимыми традиционные нормы ответственности, предусмотренные статьей 88 Кодекса обязательственного и договорного права Марокко[14]. Ведь даже если человек отвечает за устройство, наделенное искусственным интеллектом, оно может выйти из-под контроля из-за сложности эффективного управления ею. Кроме того, при таком режиме потенциальным жертвам сложно определить, кто будет нести ответственность – разработчик или пользователь искусственного интеллекта. Например, если пользователь обладает техническими навыками, он может модифицировать исходный код, что приведет к изменению работы ИИ. Кроме того, пользователь может выбирать параметры функционирования, также изменяя его работу. Такой сценарий значительно затрудняет идентификацию лица, реально управляющего устройством с искусственным интеллектом. С учетом всех вышеперечисленных проблем становится непросто установить, был ли вред нанесен в результате дефектов структуры или действий искусственного интеллекта, что порождает проблему доказывания.

В самом деле в большинстве доктрин отмечается, что ответственность за действия устройств не вполне адаптирована к факту автономности искусственного интеллекта (Shushanik, 2019). Однако к этому факту могут быть адаптированы другие режимы, когда ответственность наступает при отсутствии вины. Так происходит в случае ответственности за качество продукции; этот режим может оказаться эффективным для работы с автономными системами искусственного интеллекта (Courtois, 2016). Понятия продукта и дефекта хорошо совместимы с нематериальным и автономным характером этих систем. Это механизм ответственности полного права, как предусмотрено в п. 1 ст. 106 Кодекса обязательственного и договорного

[13] Множественность участников процесса использования или программирования системы не позволяет применить традиционные составляющие гражданской ответственности: понятий вины, ущерба и причинной связи.

[14] Статья 88 Кодекса обязательственного и договорного права гласит: «Физические лица несут ответственность за вред, причиненный находящимися в их ведении объектами, при условии, что эти объекты непосредственно причинили вред, если они не докажут: 1) что приняли все необходимые меры предосторожности для предотвращения вреда и 2) что вред возник вследствие непредвиденных обстоятельств, непреодолимой силы или по вине потерпевшего».

права Марокко: «Производитель несет ответственность за ущерб, вызванный дефектом его продукции»[15].

В действительности интеллектуальные машины не являются обычными продуктами. Необходимо учитывать, в частности для определения происхождения дефекта, их сложность, сочетание нематериальных и при необходимости материальных элементов, а также участие многочисленных сторон в их производстве, от разработчика алгоритмов и программ до изготовителя робота. Широкое понятие производителя, будь то изготовитель конечного продукта или его компонентов, а также солидарная ответственность обоих позволяют обеспечить необходимый режим ответственности без применения других норм (Courtois, 2016). Возникает вопрос, в каком случае производитель может воспользоваться основанием для освобождения от ответственности. Ответ на этот вопрос содержится в п. 9 ст. 106 Кодекса обязательственного и договорного права: «Производитель не несет ответственности, если будет доказано, что дефект, вызвавший ущерб, не существовал в момент выпуска товара в обращение или что этот дефект возник впоследствии». Согласно этой статье, производитель не может быть привлечен к ответственности, если с учетом обстоятельств есть основания полагать, что дефект, причинивший вред, не существовал в момент выпуска товара в обращение или что этот дефект возник позже.

Однако в отношении систем искусственного интеллекта традиционные нормы выпуска товара на рынок можно поставить под сомнение. В некоторых случаях роль производителя не ограничивается таким выпуском. Иногда программное обеспечение обновляется для обеспечения его надлежащего функционирования и адаптации к окружающей среде. Кроме того, производитель может предоставить новые данные для обработки автономным программным обеспечением. Тогда речь идет о том, можно ли учесть роль производителя при определении ответственности. Для ответа на этот вопрос можно предположить, что если производитель сохраняет контроль над созданной им системой для последующих обновлений, то он должен нести ответственность за дефекты этой системы, даже если они появляются после выпуска данного продукта. Наконец, следует отметить, что данный режим ответственности, по-видимому, адаптирован к системам искусственного интеллекта, однако его применение в этой области все еще остается неопределенным из-за отсутствия общепризнанной судебной практики, и вопрос о согласовании этих различных режимов ответственности может стать серьезной проблемой.

Заключение

Искусственный интеллект и темпы его развития породили новые экономические, социальные и этические проблемы. Область права не является исключением. Хотя искусственный интеллект помогает компаниям адаптироваться и осваивать все

[15] Термин «продукт» означает любой продукт, предлагаемый на рынке в контексте профессиональной, коммерческой или ремесленной деятельности, за плату или бесплатно, новый или бывший в употреблении, подвергавшийся или не подвергавшийся обработке или упаковке, либо встроенный в другой объект или в здание. Электроэнергия также считается продуктом. См. п. 2 ст. 106 Кодекса обязательственного и договорного права Марокко.

более динамичную бизнес-среду, он также создает риски для реализации основных прав и свобод. Поэтому необходимо найти баланс между использованием искусственного интеллекта для развития сферы бизнеса и человека в целом и защитой основных прав и свобод.

Технологии и их использование, а в XX в. это прежде всего Интернет, являются трансграничными и ставят под сомнение множество правовых границ, национальных и даже международного законов. Однако, чтобы оставаться эффективным, право должно придерживаться принципа «технологической реальности», который является фактором дифференциации и усложнения нормы, и применять его к искусственному интеллекту. Проблема выбора нормативных актов, применимых к искусственному интеллекту, остается актуальной, поскольку искусственный интеллект находится на пересечении нескольких самых передовых областей человеческой деятельности.

В отсутствие специальной правовой базы для искусственного интеллекта этика естественным образом становится временным решением проблемы выбора мягкого права. Это непростой для большинства людей выбор, так как мягкое право необязательно к исполнению; однако его легко применить к искусственному интеллекту. Этика оказывается удобным инструментом, который можно использовать вместо права. Правовое регулирование систем искусственного интеллекта требует работы на пересечении множества общих и специальных юридических дисциплин, создавая новые, сквозные отношения. Тем самым право получает возможность отразить специфику этих новых субъектов и выполнить свои нормативные и регулятивные функции.

Список литературы

Ait El Bour, D., & Lebzar, B. (2020). L'intelligence artificielle face aux entreprises marocaines, quels défis? *Revue Internationale d'Economie Numérique, 2*(1). (In French).

Al-Ajmi, F. (2011). *Civil Protection for the Consumer in the Electronic Contract*. (Unpublished Master dissertation). University of the Middle East.

Barraud. (2019). Le droit en datas: comment l'intelligence artificielle redessine le monde juridique. *Revue Lamy droit de l'immatériel*, *164*. (In French).

Benhanou, S. (2017). *Imaginer l'avenir de travail – Quatre types d'organisations à l'horizon 2030*, France Stratégie, Document de travail n°2017-05. (In French).

Bensamoun, A., & Loiseau, G. (2017a). La gestion des risques de l'intelligence artificielle – de l'éthique à la responsabilité. *La Semaine juridique*, *12*. (In French).

Bensamoun, A., & Loiseau, G. (2017b). *L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun: questions de temps*. Dalloz IP/IT, 239. (In French).

Bensoussan, A., &, Bensoussan, J. (2019). *IA, robots et droit*. Bruxelles: Bruylant. (In French).

Bertrand, André R. (2010). *Conditions de la protection par le droit d'auteur. Deux cas particuliers: intelligence artificielle et réalité virtuelle*, Dalloz, 103.27. (In French).

Bostrom, N., & Yudkowsky, E. (2018). The Ethics of Artificial Intelligence. In *Artificial Intelligence Safety and Security* (pp. 57–69). Chapman and Hall/CRC. https://doi.org/10.1201/9781351251389-4

Bouanba, N., Barakat, O., & Bendou, A. (2022). Artificial Intelligence & Agile Innovation: Case of Moroccan Logistics Companies. *Procedia Computer Science*, *203*, 444–449. https://doi.org/10.1016/j.procs.2022.07.059

Boubker, O. (2024). From chatting to self-educating: Can AI tools boost student learning outcomes? *Expert Systems with Applications*, *238*(A), 121820–121820. https://doi.org/10.1016/j.eswa.2023.121820

Boy, L., Racine, J.-B., & Siiriaien, F. (2009). *Droit économique et Droit de l'homme*. Bruxelles, Larcier. (In French).

Bufflier, I. (2020). Intelligence artificielle et éthique d'entreprise. *Cahiers de droit de l'entreprise*, *3*, dossier 19, 45. (In French).

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080.

Courtois, G. (2016). *Robots intelligents et responsabilité : quels régimes, quelles perspectives*. Dalloz IP/IT, 287. (In French).
Desbarats, I. (2020). Quelle protection sociale pour les travailleurs des plateformes? *Revue de droit du travail*, *10*, 592–601. (In French).
Franchomme, M.-P., & Jazottes, G. (2021). Le défi d'une IA inclusive et responsable. *Droit social*, *2*, 100–108. (In French).
Jacquemin, H., & de Streel, A. (2017). *L'Intelligence artificielle et le droit*, Bruxelles, Larcier. (In French).
Jaldi, A. S. (2022). l'intelligence artificielle au Maroc: entre encadrement réglementaire et stratégie économique. *Policy Centre for the New South*, PB-59/22. (In French).
Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature machine intelligence*, 1(9), 389–399.
Marique, E., & Stronwel, A. (2017). *Gouverner par la loi ou les algorithmes: de la norme générale de comportement au guidage rapproché des conduites*. Dalloz IP/IT, 10, 517. (In French).
Merabet, S. (2018). *Vers un droit de l'intelligence artificielle: thèse pour le doctorat en droit privé*. Université d'Aix-Marseille. (In French).
Michaud, O. (2021). La protection des travailleurs à l'heure de l'intelligence artificielle. *Dossier droit social*, *2*, Fév., 124–132. (In French).
Mohamed-Amine, N., Abdellatif, M., & Belaid, B. (2024). Artificial intelligence for forecasting sales of agricultural products: A case study of a moroccan agricultural company. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(1), 100189. https://doi.org/10.1016/j.joitmc.2023.100189
Naim, A., Aaroud, A., Akodadi, K., & El Hachimi, C. (2021). A fully AI-based system to automate water meter data collection in Morocco country. *Array*, *10*, 100056. https://doi.org/10.1016/j.array.2021.100056
Rochd, A., Benazzouz, A., Ait Abdelmoula, I., Raihani, A., Ghennioui, A., Naimi, Z., & Ikken, B. (2021). Design and implementation of an AI-based & IoT-enabled Home Energy Management System: A case study in Benguerir – Morocco. *Energy Reports*, *7*, 699–719. https://doi.org/10.1016/j.egyr.2021.07.084
Shushanik, G. (2019). *Les problèmes de la réparation du dommage pour les produits et services défectueux dans la législation civile: thèse pour le doctorat en droit privé*. l'UEE. (In French).
Soulez, M. (2018). Questions juridiques au sujet de l'IA. *Enjeux numériques*, *1*, 83. (In French).
Thibout, Ch. (2019). La compétition mondiale de l'intelligence artificielle. *Pouvoirs – Revue française d'études constitutionnelles et politiques*, *170*, 131–142. (In French).
Vassileva-Hadjitchoneva, J. (2020). L'IA au service de la prise de décisions plus efficace. *Pour une recherche économique efficace: 61° Congrès International AIELF*. Santiago, Chili. (In French).
Zouinar, M. (2020). Evolutions de l'intelligence artificielle: Quels enjeux pour l'activité humaine et la relation humain-machine au travail? *Activités*, 17-1. (In French). https://doi.org/10.4000/activites.4941

Сведения об авторах

Джабир Хамза – соискатель степени PhD; исследовательская лаборатория частного права, юридических наук и устойчивого развития; факультет права, экономики и общественных наук; Университет Ибн Зохр
Адрес: Марокко, Агадир, BP 32/S, Риад Салам, CP 80000
E-mail: hamza.jabir@edu.uiz.ac.ma
ORCID ID: https://orcid.org/0000-0003-3534-8982
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HMP-6781-2023
Google Scholar ID: https://scholar.google.com/citations?user=Lka-pbUAAAAJ

Лагтати Камаль – профессор-исследователь, почетный доктор, исследовательская лаборатория частного права, юридических наук и устойчивого развития; факультет права, экономики и общественных наук; Университет Ибн Зохр; член Центра Мишель де л'госпиталь, Университет Клермон-Овернь (EA 4232).
Адрес: Марокко, Агадир, BP 32/S, Риад Салам, CP 80000
E-mail: k.lagtati@uiz.ac.ma
ORCID ID: https://orcid.org/0009-0004-9198-2712
Google Scholar ID: https://scholar.google.com/citations?user=W-X93ewAAAAJ

Поэ-Токпа Денис – профессор-исследователь, почетный доктор частного права, факультет права и политологии, Университет Бордо
Адрес: Франция, Пессак, 33608, авеню Леона Дюгуи, 16
E-mail: denis.pohe-tokpa@u-bordeaux.fr
ORCID ID: https://orcid.org/0009-0007-2678-1430

Вклад авторов

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

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 14 декабря 2023 г.
Дата одобрения после рецензирования – 12 января 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:17:004.8
EDN: https://elibrary.ru/fsfsnq
DOI: https://doi.org/10.21202/jdtl.2024.23

Ethical and Legal Regulation of Using Artificial Intelligence in Morocco

Hamza Jabir ✉
Ibn Zohr University, Agadir, Morocco

Kamal Lagtati
Ibn Zohr University, Agadir, Morocco

Denis Pohe-Tokpa
University of Bordeaux, Pessac, France

Keywords

"hard law",
Moroccan legislation,
artificial intelligence,
moral values,
"soft law",
principle of technological reality,
legal regulation,
legal risks,
digital technologies,
ethical principle

Abstract

Objective: to explore and identify the issues and opportunities for the ethical and legal regulation of artificial intelligence by the example of digital transformation in Morocco.

Methods: the study was conducted using analytical and comparative approaches to address the emerging legal issues arising from the development of artificial intelligence. The traditional scientific method in law is based on legal analysis, which was applied to the study of legal texts, scientific literature, diagnosis of the condition of the study field at the national and international level. Along with this, the comparative approach in law was used, which made it possible to examine the Moroccan legislation comparison with that of other countries.

Results: the article presents a review of scientific literature on the legal and ethical issues of using artificial intelligence. Legal texts and decrees developed at national and international level, directly or indirectly linked to the use of artificial intelligence, were reviewed. Moroccan legislation was compared with that of other countries. The findings suggest that, in the absence of a specific legal framework for artificial intelligence systems, the adoption of ethical standards in the form of guidelines, best

✉ Corresponding author

practices and ethical charters is preferable. These mechanisms appear to be a viable alternative to legal regulation. In this sense, several initiatives were taken to promote "soft law", which aims to encourage appropriate behavior of technological agents.

Scientific novelty: the analysis of digital transformations in Morocco made it possible to present a comprehensive view on the role of ethical aspects and on the sufficiency of law to respond to the changes in the modern society, transformed by the development of artificial intelligence.

Practical significance: the study allows identifying ways to find a more flexible balance between "soft" and "hard" law in the regulation of relations, taking into account the technological reality. This should encourage the appropriate behavior of technological agents and positively affect the specificity of the current situation. Today, the "hard law" slowly recognizes and addresses the problems associated with the digital technologies' regulation and slowly takes into account the possible risks posed by artificial intelligence and the insufficiency of its regulation.

For citation

Jabir, H., Lagtati, K., & Pohe-Tokpa, D. (2024). Ethical and Legal Regulation of Using Artificial Intelligence in Morocco. *Journal of Digital Technologies and Law, 2*(2), 450–472. https://doi.org/10.21202/jdtl.2024.23

References

Ait El Bour, D., & Lebzar, B. (2020). L'intelligence artificielle face aux entreprises marocaines, quels défis? *Revue Internationale d'Economie Numérique*, *2*(1). (In French).

Al-Ajmi, F. (2011). *Civil Protection for the Consumer in the Electronic Contract*. (Unpublished Master dissertation). University of the Middle East.

Barraud. (2019). Le droit en datas: comment l'intelligence artificielle redessine le monde juridique. *Revue Lamy droit de l'immatériel*, *164.* (In French).

Benhanou, S. (2017). *Imaginer l'avenir de travail – Quatre types d'organisations à l'horizon 2030*, France Stratégie, Document de travail n°2017-05. (In French).

Bensamoun, A., & Loiseau, G. (2017a). La gestion des risques de l'intelligence artificielle – de l'éthique à la responsabilité. *La Semaine juridique*, *12*. (In French).

Bensamoun, A., & Loiseau, G. (2017b). *L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun: questions de temps*. Dalloz IP/IT, 239. (In French).

Bensoussan, A., &, Bensoussan, J. (2019). *IA, robots et droit*. Bruxelles: Bruylant. (In French).

Bertrand, André R. (2010). C*onditions de la protection par le droit d'auteur. Deux cas particuliers: intelligence artificielle et réalité virtuelle*, Dalloz, 103.27. (In French).

Bostrom, N., & Yudkowsky, E. (2018). The Ethics of Artificial Intelligence. In *Artificial Intelligence Safety and Security* (pp. 57–69). Chapman and Hall/CRC. https://doi.org/10.1201/9781351251389-4

Bouanba, N., Barakat, O., & Bendou, A. (2022). Artificial Intelligence & Agile Innovation: Case of Moroccan Logistics Companies. *Procedia Computer Science*, *203*, 444–449. https://doi.org/10.1016/j.procs.2022.07.059

Boubker, O. (2024). From chatting to self-educating: Can AI tools boost student learning outcomes? Expert *Systems with Applications*, *238*(A), 121820–121820. https://doi.org/10.1016/j.eswa.2023.121820

Boy, L., Racine, J.-B., & Siiriaien, F. (2009). *Droit économique et Droit de l'homme*. Bruxelles, Larcier. (In French).

Bufflier, I. (2020). Intelligence artificielle et éthique d'entreprise. *Cahiers de droit de l'entreprise*, *3*, dossier 19, 45. (In French).

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080.

Courtois, G. (2016). *Robots intelligents et responsabilité : quels régimes, quelles perspectives*. Dalloz IP/IT, 287. (In French).

Desbarats, I. (2020). Quelle protection sociale pour les travailleurs des plateformes? *Revue de droit du travail*, *10*, 592–601. (In French).

Franchomme, M.-P., & Jazottes, G. (2021). Le défi d'une IA inclusive et responsable. *Droit social*, *2*, 100–108. (In French).

Jacquemin, H., & de Streel, A. (2017). *L'Intelligence artificielle et le droit*, Bruxelles, Larcier. (In French).

Jaldi, A. S. (2022). l'intelligence artificielle au Maroc: entre encadrement réglementaire et stratégie économique. *Policy Centre for the New South*, PB-59/22. (In French).

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature machine intelligence*, *1*(9), 389–399.

Marique, E., & Stronwel, A. (2017). *Gouverner par la loi ou les algorithmes: de la norme générale de comportement au guidage rapproché des conduites*. Dalloz IP/IT, 10, 517. (In French).

Merabet, S. (2018). *Vers un droit de l'intelligence artificielle: thèse pour le doctorat en droit privé*. Université d'Aix-Marseille. (In French).

Michaud, O. (2021). La protection des travailleurs à l'heure de l'intelligence artificielle. *Dossier droit social, 2*, Fév., 124–132. (In French).

Mohamed-Amine, N., Abdellatif, M., & Belaid, B. (2024). Artificial intelligence for forecasting sales of agricultural products: A case study of a moroccan agricultural company. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(1), 100189. https://doi.org/10.1016/j.joitmc.2023.100189

Naim, A., Aaroud, A., Akodadi, K., & El Hachimi, C. (2021). A fully AI-based system to automate water meter data collection in Morocco country. *Array*, *10*, 100056. https://doi.org/10.1016/j.array.2021.100056

Rochd, A., Benazzouz, A., Ait Abdelmoula, I., Raihani, A., Ghennioui, A., Naimi, Z., & Ikken, B. (2021). Design and implementation of an AI-based & IoT-enabled Home Energy Management System: A case study in Benguerir – Morocco. *Energy Reports*, *7*, 699–719. https://doi.org/10.1016/j.egyr.2021.07.084

Shushanik, G. (2019). *Les problèmes de la réparation du dommage pour les produits et services défectueux dans la législation civile: thèse pour le doctorat en droit privé*. l'UEE. (In French).

Soulez, M. (2018). Questions juridiques au sujet de l'IA. *Enjeux numériques*, *1*, 83. (In French).

Thibout, Ch. (2019). La compétition mondiale de l'intelligence artificielle. Pouvoirs – *Revue française d'études constitutionnelles et politiques*, 170, 131–142. (In French).

Vassileva-Hadjitchoneva, J. (2020). L'IA au service de la prise de décisions plus efficace. *Pour une recherche économique efficace: 61° Congrès International AIELF*. Santiago, Chili. (In French).

Zouinar, M. (2020). Evolutions de l'intelligence artificielle: Quels enjeux pour l'activité humaine et la relation humain-machine au travail? *Activités*, 17-1. (In French). https://doi.org/10.4000/activites.4941

Authors information

Hamza Jabir – PhD Student in Private Law, Legal Sciences and Sustainable Development Research Laboratory, Faculty of Law, Economics, and Social Sciences, Ibn Zohr University
E-mail: hamza.jabir@edu.uiz.ac.ma
ORCID ID: https://orcid.org/0000-0003-3534-8982
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HMP-6781-2023
Google Scholar ID: https://scholar.google.com/citations?user=Lka-pbUAAAAJ

Kamal Lagtati – Research Professor, HDR in Private Law, Legal Sciences and Sustainable Development Research Laboratory, Faculty of Law, Economics, and Social Sciences, Ibn Zohr University; Member of the Centre Michel de l'hospital Université de Clermont Auvergne (EA 4232).
Address: BP 32/S, Riad Salam, CP 80000, Agadir, Morocco
E-mail: k.lagtati@uiz.ac.ma
ORCID ID: https://orcid.org/0009-0004-9198-2712
Google Scholar ID: https://scholar.google.com/citations?user=W-X93ewAAAAJ

Denis Pohe-Tokpa – Research Professor, HDR in Private Law, Faculty of Law and Political Science, University of Bordeaux
Address: 16 Avenue Léon Duguit, 33608 Pessac, France
E-mail: denis.pohe-tokpa@u-bordeaux.fr
ORCID ID: https://orcid.org/0009-0007-2678-1430

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 – December 14, 2023
Date of approval – January 12, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:17:004.8
EDN: https://elibrary.ru/fhsfeo
DOI: https://doi.org/10.21202/jdtl.2024.24

От теории африканского происхождения человечества к современным социальным, правовым и технологическим новациям: краткий аналитический экскурс в антропосоциогенез

Дженеба Траоре

Университет гуманитарных и социальных наук Бамако, Бамако, Мали
Институт Западной Африки, Прая, Кабо-Верде

Ключевые слова

антропогенез,
искусственный интеллект,
общественные трансформации,
право,
промышленная революция,
социальная справедливость,
социогенез,
технологическая революция,
цифровые технологии,
эволюция человека

Аннотация

Цель: проследить эволюцию человечества и выявить роль различных социальных институтов для понимания экзистенциальной роли законов, направленных на обеспечение совместной жизни социума в контексте технологических новаций.

Методы: в процессе исследования использованы общенаучные и специальные методы познания, позволившие проследить диалектическое развитие человечества, социальные трансформации и технологические новации.

Результаты: оглядываясь на историю человечества, зародившегося на Африканском континенте (теория африканского происхождения), автор отмечает наиболее важные изменения в образе жизни человека и его окружающей среде, которые привели к необходимости построения организованных обществ и регулирования социального поведения в нем с помощью законодательных норм. Право рассматривается как часть эволюционного процесса, которое должно было возникнуть в ходе эволюции человечества. Отмечается чрезвычайная важность закона для преодоления возникающих в процессе эволюции глобальных вызовов и экзистенциальных вопросов дальнейшего сосуществования человечества. В этой связи подчеркивается историческое значение Хартии Курукан-Фуга Малийской империи как одной из древнейших конституций в мире, получившей признание на международном уровне как важного источника юридических и политических норм для современных обществ, регламентирующих устройство

государственной власти и социальное поведение, хотя и сохранившейся в основном в устной форме. Утверждается, что толчком к разработке новых законов часто служили социальные и технологические преобразования. Человечество много раз вмешивалось в собственную биологическую эволюцию при помощи технологий, теперь же наступает важный с точки зрения права и этики момент возможного вмешательства технологий в дальнейшую эволюцию человека. Наибольшее опасение в этом плане вызывает эпоха бурного развития искусственного интеллекта, предъявляющая к человеку новые требования.

Научная новизна: показана роль Африканского континента в происхождении и развитии человечества, социально-правовых институтов, находящихся в свете современных трансформаций и конструирования новой социальной реальности.

Практическая значимость: проведенное исследование создает предпосылки для дальнейшего развития теории антропосоциогенеза и углубленного концептуального историко-правового изучения роли Африканского континента в развитии человечества и его социальных институтов.

Для цитирования

Траоре, Д. (2024). От теории африканского происхождения человечества к современным социальным, правовым и технологическим новациям: краткий аналитический экскурс в антропосоциогенез. *Journal of Digital Technologies and Law*, *2*(2), 473–486. https://doi.org/10.21202/jdtl.2024.24

Содержание

Введение

С самого своего зарождения человечество управлялось устными или письменными законами. Вернемся в прошлое, чтобы понять, как глубокие социальные преобразования, первоначально вызванные новыми идеологиями, привели к изменениям в образе жизни и породили необходимость регулирования с помощью законодательных норм и правил.

На планете Земля появились растительная и животная формы жизни; человечество отделилось от животной формы благодаря развитию интеллекта, речи, прямохождения и способности изготавливать орудия труда и одомашнивать животных и растения.

В доисторических обществах человеческий вид, ставший двуногим, начал общаться. Общение позволило создать форму социальной организации, которая

дала возможность жить вместе и соблюдать определенные правила, установленные для этой цели.

Следует отметить, что правила существуют и в царстве животных, и, как ни удивительно, в царстве растений.

1. Эволюция человека в контексте технологических новаций и социально-правовых трансформаций: исторический экскурс

По мнению ученых, эволюция человека включает семь этапов[1]:

– Dryopithecus (дриопитеки);
– Ramapithecus (палеопитеки);
– Australopithecus (австралопитеки);
– Homo Habilis (человек умелый);
– Homo Erectus (человек прямоходящий);
– Homo Sapiens Neanderthalensis (неандертальцы);
– Homo Sapiens (человек разумный).

На основании археологических находок доказано, что человечество появилось на Африканском континенте: «Согласно последней теории африканского происхождения современного человека, современные люди развились в Африке, возможно, из H. heidelbergensis, H. rhodesiensis или H. antecessor и мигрировали с континента примерно 50–100 тысяч лет назад, постепенно вытесняя местные популяции H. erectus, денисовцев, H. floresiensis»[2].

Что же представляет собой процесс эволюции человечества?

«Эволюция человека – это длительный процесс изменений, в ходе которого[3] люди произошли от своих обезьяноподобных предков. Научные данные показывают, что физические и поведенческие черты, общие для всех людей, произошли от обезьяноподобных предков и развивались в течение примерно шести миллионов лет»[4].

Различные общественно-экономические формации, известные человечеству, включают в себя:

– античность, или доисторические общества;
– рабовладельческий строй;
– феодализм;
– капитализм;
– социализм;
– коммунизм.

По мнению историков, государства возникли спустя долгое время после зарождения человечества: «Ранние государства появились между шестью и пятью тысячами лет назад, прежде всего в Египте, Месопотамии и на тихоокеанском побережье Южной Америки. Несколько позже государства возникли также в долине Инда

1 Human evolution. Britannica. https://clck.ru/3BcmeF

2 Источник определения: Google, 3 декабря 2023 г.

3 National Museum of Natural History. https://clck.ru/3Bcmf8

4 Источник: Google

(около 4,5 тысяч лет назад), Китае (около 4 тысяч лет назад) и Центральной Америке (около 3,5 тысячи лет назад)»[5].

В племенах, кланах и этнических группах были разработаны правила, а затем и установлены законы, которые не только позволили людям жить вместе в относительной гармонии, но и, прежде всего, выжить как виду. Эти правила и законы определяли неприкосновенность личности и защищали ее от определенных форм насилия и жестокого обращения.

Мы видим, что роль закона чрезвычайно важна для выживания человечества, которое постоянно сталкивается с изменениями, иногда приводящими к ослаблению некоторых индивидов.

Edward W. Younkins писал: «Исторически сложилось так, что зарождающиеся в обществе идеи правовых принципов, часто соответствующие реальности, возникали до их принятия политическими властями. Добровольные формы управления с помощью обычного частного права предшествовали государственному праву и эффективно упорядочивали человеческую жизнедеятельность. Право возникло как спонтанный порядок – оно должно было быть открыто, а не введено в действие. Право – это эволюционный системный процесс, включающий в себя опыт огромного числа людей»[6].

В каждом из этих обществ действовали законы, направленные на укрепление установленного порядка.

На каждом этапе эволюции человечества некоторые законы подвергались сомнению со стороны меньшинства или большинства людей, отменялись или заменялись законами, которые считались более справедливыми.

Малийская империя, провозгласившая в 1236 г. Хартию Курукан Фуга, стала первым государством, которое законодательно закрепило права и обязанности человека и различных социально-профессиональных слоев народа Мали.

В 2009 г. Хартия была включена ЮНЕСКО в Репрезентативный список нематериального культурного наследия человечества.

На сайте ЮНЕСКО представлен обзор этой Хартии: «После крупной военной победы в начале XIII в. основатель империи Мандинго и совет мудрецов провозгласили в Курукан Фуга новую Хартию Мандена, названную так в честь территории, расположенной в верховьях реки Нигер, между современными Гвинеей и Мали. Это одна из древнейших конституций в мире, хотя и сохранившаяся в основном в устной форме. Она содержит преамбулу из семи глав, в которых говорится о многообразии общества, неприкосновенности человека, образовании, целостности родной страны, продовольственной безопасности, отмене порабощения путем набегов, а также о свободе слова и торговли. Хотя империя Мандинго исчезла, слова Хартии и ритуалы, связанные с ней, до сих пор устно передаются в местных кланах от отца к сыну. Чтобы сохранить эту традицию, в деревне Кангаба (примыкающей к обширной области Курукан Фуга, которая сейчас находится на территории Мали, недалеко от границы с Гвинеей) ежегодно проводятся памятные церемонии, посвященные принятию Хартии. Эти церемонии поддерживаются местными и национальными властями Мали и, в частности, племенными властями, которые рассматривают их

5 Источник: Google

6 Younkins, E. W. (2000, August 5). Capitalism & Commerce. The evolution of Law. https://clck.ru/3Bcmji

как источник права и как средство продвижения идей любви, мира и братства, сохранившихся в веках. Хартия Мандена по-прежнему является основой ценностей и самобытности населения страны»[7].

Когда обсуждается вопрос об искусственном интеллекте, Африку обычно исключают из числа тех, кто добился успехов в области технологий (Stiglitz, 2017, Bob-Milliar, 2021).

Однако, как утверждает Paul E. Lovejoy (2014) в своей монографии «African Contributions to Science, Technology and Development» («Вклад Африки в науку, технологию и развитие»), Африка в значительной степени способствовала развитию науки и техники и оказала реальное влияние на мир благодаря своим изобретениям и инновациям. Речь идет об изобретениях и открытиях, которые были сделаны на африканской земле в области медицины, технологии, математики, астрономии, сельского хозяйства и пищевой промышленности, и это лишь некоторые области.

«Догоны населяют район Мали под названием нагорье Бандиагара – участок песчаниковых скал длиной почти 100 миль и высотой до 1500 футов. Воспользовавшись природной защитой, племя построило свои дома на склонах скал в III в. до нашей эры и с тех пор не покидало их. Но только в 1930-х гг. французские антропологи обнаружили у них необычайно развитые астрономические знания, несмотря на то, что они вели весьма примитивный образ жизни.

Несмотря на то, что догоны живут на расстоянии более 2000 миль от Египта, их история интригующим образом связана с прославленным древним родом, имеющим отношение к звездам.

Изучая племя догонов, антрополог Марсель Гриоль узнал об их интересе к звездной системе Сириус. Сириус А виден невооруженным глазом, но его спутник, белый карлик Сириус В, был открыт только в 1950-х гг. с помощью современного телескопа. Однако догоны прекрасно знали о его существовании и периоде вращения, и их описание было подтверждено много лет спустя»[8].

В 1983 г. Ivan Van Sertima опубликовал книгу «Blacks in Science: Ancient and Modern. Journal of African Civilizations» («Чернокожие в науке: Древность и современность. Дневник африканских цивилизаций»), в которой перечисляет более тысячи изобретений, сделанных африканцами и выходцами из Африки. «Множество предметов и услуг, которыми американцы пользуются каждый день, были изобретены чернокожими – от трехцветного светофора, грузовиков-рефрижераторов, автоматических дверей лифта, цветных мониторов для настольных компьютеров до формы современной гладильной доски, приспособления для отжима белья, банков крови, лазерного лечения катаракты, систем домашней безопасности и детской игрушки-супергубки. Их создатели получили признание, однако бесчисленные другие изобретения остались безымянными, а многие были утеряны» (Sertima, 1983).

---

7 UNESCO. Manden Charter, proclaimed in Kurukan Fuga. https://clck.ru/3BcmmS

8 (2019, October 13). Was the Sirius Star System Home to the Dogon African Tribe? Gaia. https://clck.ru/3BcmnQ

Следует подчеркнуть, что именно чернокожий раб помог Америке получить вакцину против оспы. В 1706 г. он был подарен священнику-пуританину из Новой Англии Коттону Мэзеру, который дал ему новое имя – Онесимус. Онесимус познакомил Мазера с принципом и процедурой прививки против оспы для профилактики заболевания, что заложило основу для разработки вакцин.

«Операция, о которой говорил Онесимус, заключалась во втирании гноя от зараженного человека в открытую рану на руке. Это делалось особым образом под контролем врача, чтобы симптомы были более слабыми, но все же давали иммунитет. Как только инфицированный материал попадал в организм, человек получал прививку от оспы. Это не было вакцинацией, которая предполагает воздействие менее опасного вируса для выработки иммунитета, но процедура активировала иммунный ответ реципиента и в большинстве случаев защищала от болезни»[9].

Проблема с изобретениями, сделанными африканцами и представителями африканской диаспоры, заключается в том, что они затушевывались рабством и колонизацией – двумя системами угнетения и эксплуатации человека человеком, которые делали чернокожих неполноценными и не имеющими никаких прав. В те времена чернокожий не мог запатентовать свои изобретения, потому что патент – это договор между государством и гражданином, а чернокожие не были гражданами. В связи с этим возникает проблема патентов и лицензий для изобретателей, а также интеллектуальной собственности. Многим рабам приходилось ставить имя своего хозяина на патенте, чтобы зарегистрировать его.

Толчком к разработке новых законов часто служили социальные и технологические преобразования. Когда первобытное общество перешло к античности, что произошло, несомненно, благодаря открытию огня, социальное положение людей изменилось: они стали изготавливать оружие для охоты на дичь и орудия для обработки земли, а это означало, что соотношение сил менялось в пользу производителей и владельцев этих предметов.

Появление феодального общества привело к всемогуществу феодала, который обладал чрезвычайно важными полномочиями благодаря тому, что имел армию, использовал религию для укрепления своей власти и определял право своих подданных на жизнь и смерть.

Протоистория – это период истории, который начинается с появления человека и продолжается до появления письменности. С этого момента начинается другой период – Античность, который закончился с падением Римской империи в 476 г. нашей эры.

С древних времен люди начали рассказывать легенды, мифы, саги и другие виды сказаний, в которых присутствовали элементы сверхъестественного, а также люди со сверхспособностями.

С началом индустриальной эпохи в Европе стало возможным создавать машины, заменяющие человека. Именно технологические инновации, широко внедряемые начиная с XIX в., лежат в основе прекращения рабства и начала колонизации. Действительно, чтобы получить доступ к сырью, которое было необходимо Западу для работы машин, Африканский континент, обладающий этим сырьем, был

[9] Blakemore, E. (2021, April, 8). How an Enslaved African Man in Boston Helped Save Generations from Smallpox. https://clck.ru/3BcmrE

колонизирован, а его население заставляли работать силой чрезвычайно смертоносного огнестрельного оружия.

Отмечается, что «промышленная революция – это переход от создания товаров вручную к использованию машин. Начало и конец ее широко обсуждаются учеными, но в целом считается, что этот период длился примерно с 1760 по 1840 г.»[10].

Каковы же четыре этапа промышленной революции?

«Четыре промышленные революции – это угольная, газовая, электронная и ядерная, а затем Интернет и возобновляемые источники энергии. Начиная с 1765 г. и по сей день мы наблюдаем это удивительное развитие»[11].

Каждая революция приводила к появлению нового образа жизни, который необходимо было регулировать, чтобы общество функционировало в соответствии с желаниями правящего класса. Однако европейский пролетариат, находившийся под идеологическим господством и экономической эксплуатацией капитализма, организовался и потребовал более гуманных и достойных условий жизни и труда. Это ознаменовало рождение профсоюзов и становление социализма и коммунизма как политических систем.

2. Эволюция человечества и искусственный интеллект: современные перспективы

Новая технологическая революция, которую мы наблюдаем с конца XX в. и особенно в начале XXI в. с появлением искусственного интеллекта, требует принятия законов, позволяющих избежать всех форм злоупотреблений, которые может породить развитие искусственного интеллекта. В нашем понимании это означает, что искусственный интеллект сначала должен стать предметом глубоких исследований, чтобы понять все его особенности, возможности и потенциальные риски. Затем результаты этих исследований должны быть доведены до лиц, принимающих политические решения, выборных органов власти и широкой общественности.

Благодаря технологическому прогрессу, который отмечается в последние годы, использование искусственного интеллекта (ИИ) продолжает расти.

Возникнув около шестидесяти лет назад, искусственный интеллект стал главным технологическим достижением начала XXI в. (Mocanu, 2021; Mulgan, 2019; Pagallo, 2018).

ИИ присутствует во всех сферах деятельности, особенно в промышленности, транспорте, здравоохранении, торговле, экономике, сельском хозяйстве, инфраструктуре, образовании, индустрии развлечений и т. д. Прогнозируется, что он будет приносить колоссальные доходы и глубоко изменит наш образ жизни благодаря появлению новых изобретений (Avila Negri, 2021; Bertolini & Episcopo, 2022).

Один из интернет-источников дает нам определение искусственного интеллекта, как он работает и почему он важен: «Искусственный интеллект – это имитация интеллектуальных процессов человека с помощью машин, особенно компьютерных систем. Конкретные приложения искусственного интеллекта включают экспертные

[10] The Industrial Revolution. https://clck.ru/3Bcmro

[11] https://clck.ru/3BcmuT

системы, обработку естественного языка, распознавание речи и машинное зрение» (Greenstein, 2022; Hacker et al., 2020; Hárs, 2022)[12].

«При программировании ИИ основное внимание уделяется когнитивным навыкам, к которым относятся следующие:

Обучение. Этот аспект программирования ИИ сосредоточен на получении данных и создании правил для превращения этих данных в информацию, пригодную к использованию. Эти правила, называемые алгоритмами, предоставляют вычислительным устройствам пошаговые инструкции по выполнению конкретной задачи.

Обоснование. Этот аспект программирования ИИ направлен на выбор правильного алгоритма для достижения желаемого результата.

Самокоррекция. Этот аспект программирования ИИ предназначен для постоянной доработки алгоритмов и обеспечения максимально точных результатов.

Творчество. Этот аспект ИИ состоит в использовании нейронных сетей, систем, основанных на алгоритмах, статистических и других методов искусственного интеллекта для создания новых изображений, нового текста, новой музыки, новых идей»[13].

Заключение

«ИИ имеет большое значение благодаря своему потенциалу изменить то, как мы живем, работаем и развлекаемся. Он эффективно используется в бизнесе для автоматизации задач, выполняемых людьми, включая работу с клиентами, генерацию лидов, выявление мошенничества и контроль качества (Bryson et al., 2017; Calo, 2015; Chesterman, 2020). В ряде областей ИИ может выполнять задачи гораздо лучше, чем человек»[14].

Чтобы связать понятия искусственного интеллекта и права, необходимо рассмотреть эволюцию человека и различных социальных институтов, чтобы понять, как разрабатывались и внедрялись законы, направленные на обеспечение совместной жизни и выживания соответствующих групп.

Для обеспечения безопасности и предотвращения неверного понимания в этой области важно законодательно закрепить различные аспекты искусственного интеллекта (Malgieri & Comandé, 2017; McCarty, 2017; Karnouskos, 2022; Maarten Herbosch, 2024; McNally & Inayatullah, 1988).

В частности, в военной сфере необходимо предотвратить обращение с искусственным интеллектом гражданских лиц, чтобы эти изобретения, которые должны использоваться только в случае войны или других угроз безопасности, не попали в руки злонамеренных людей, не имеющих никакого отношения к армии.

При внедрении искусственного интеллекта в учебные программы важно разработать учебные программы таким образом, чтобы сделать школьную и университетскую среду здоровой и этичной (Sertima, 1983; Solaiman, 2017; Solum, 1992).

Наконец, мы должны укрепить законодательство об интеллектуальной собственности, чтобы гарантировать права изобретателей. Это чрезвычайно важно для

---

12 Gunning, D. (2017). Explainable artificial intelligence (XAI). Defense advanced research projects agency (DARPA). https://clck.ru/3BcmvV

13 Laskowski, N., & Tucci, L. Artificial intelligence (AI). TechTarget. https://clck.ru/3Bcmxj

14 Там же.

обеспечения социальной справедливости и равенства между всеми людьми, независимо от их социального, культурного и этнического происхождения. Только тогда искусственный интеллект станет инструментом социально-экономического развития и прочного мира.

Список литературы

Avila Negri, S. M. C. (2021). Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. *Frontiers in Robotics and AI*, *8*, Art. 789327. https://doi.org/10.3389/frobt.2021.789327

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

Bob-Milliar, G. M. (2021). Africa's Contributions to World Civilization. In *The Palgrave Handbook of Africa and the Changing Global Order* (pp. 25–42). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-77481-3_2

Bryson, J. J., Diamantis, M. E., & Grant, Th. D. (2017). Of, For, and By the People: The Legal Lacuna of Synthetic Persons. *Artificial Intelligence and Law*, *25*, 273–291. https://doi.org/10.1007/s10506-017-9214-9

Calo, R. (2015). Robotics and the Lessons of Cyberlaw. *California Law Review*, *103*(3), 513–563.

Chesterman, S. (2020). Artificial Intelligence and the Limits of Legal Personality. *International & Comparative Law Quarterly*, *69*, 819–844. https://doi.org/10.1017/s0020589320000366

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

Hárs, A. (2022). AI and international law – Legal personality and avenues for regulation. *Hungarian Journal of Legal Studies*, *62*(4), 320–344. https://doi.org/10.1556/2052.2022.00352

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

Lovejoy, P. E. (2014). *African contributions to science, technology and development*. Collective Volume the (Slave Route Project, UNSECO 2012).

Maarten Herbosch. (2024). Fraud by generative AI chatbots: On the thin line between deception and negligence. *Computer Law & Security Review*, *52*, 105941–105941. https://doi.org/10.1016/j.clsr.2024.105941

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

McCarty, L. T. (2017). Finding the Right Balance in Artificial Intelligence and Law. In *Research Handbook on the Law of Artificial Intelligence* (Chapter 3, pp. 55–87). Edward Elgar Publishing. https://doi.org/10.4337/9781786439055.00013

McNally, Ph., & Inayatullah, S. (1988). The Rights of Robots: Technology, Culture and Law in the 21st Century. *Futures*, *20*(2), 119–136. https://doi.org/10.1016/0016-3287(88)90019-5

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*, Art. 788179. https://doi.org/10.3389/frobt.2021.788179

Mulgan, T. (2019). Corporate Agency and Possible Futures. *Journal of Business Ethics*, *154*, 901–916. https://doi.org/10.1007/s10551-018-3887-1

Pagallo, U. (2018). Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems. *Philosophical Transactions of the Royal Society*, *376*(2133), Art. 20180168. https://doi.org/10.1098/rsta.2018.0168

Sertima, I. V. (Ed.) (1983). Blacks in Science: Ancient and Modern. *Journal of African Civilizations*, *5*(1-2).

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

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287.

Stiglitz, J. E. (2017). The coming great transformation. *Journal of Policy Modeling*, *39*(4), 625– 638. https://doi.org/10.1016/j.jpolmod.2017.05.009

Сведения об авторе

Траоре Дженеба – PhD, профессор, ректор в отставке, Университет гуманитарных и социальных наук Бамако; генеральный директор по вопросам региональной интеграции и социальных трансформаций в Западной Африке, Институт Западной Африки
Адрес: Мали, г. Бамако, E 3637; Кабо-Верде, г. Прая, 396-A
E-mail: badjenetraore@yahoo.fr
ORCID ID: https://orcid.org/0009-0006-2674-2565
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57202159729

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: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 3 декабря 2023 г.
Дата одобрения после рецензирования – 6 января 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:17:004.8
EDN: https://elibrary.ru/fhsfeo
DOI: https://doi.org/10.21202/jdtl.2024.24

From the Theory of the African Origin of Humankind to Modern Social, Legal and Technological Innovations: a Brief Analytical Excursion into Anthroposociogenesis

Djeneba Traore

University of Arts and Humanities of Bamako, Bamako, Mali
West Africa Institute, Praia, Cabo Verde

Keywords

anthropogenesis,
artificial intelligence,
social transformations,
law,
industrial revolution,
social justice,
sociogenesis,
technological revolution,
digital technologies,
evolution of a human being

Abstract

Objective: to trace the evolution of humanity and to identify the role of various social institutions in order to understand the existential role of laws aimed at ensuring the coexistence of society in the context of technological innovations.

Methods: the author used general scientific and special methods of cognition, which allowed tracing the dialectical development of humanity, social transformations and technological innovations.

Results: looking back at the history of humanity, which originated on the African continent (the theory of African descent), the author notes the most important changes in the human way of life and environment, which led to the need to build organized societies and regulate social behavior with the help of legislative norms. Law is seen as part of the evolutionary process that was to emerge in the course of human evolution. The critical importance of law in overcoming the global challenges and existential questions of humanity's continued coexistence arising in the course of evolution is emphasized. In this regard, the historical significance of the Kurukan Fuga Charter of the Malian Empire is emphasized as one of the oldest constitutions in the world, recognized internationally as an important source of legal and political norms for modern societies, regulating the structure of state power and social behaviour, although preserved largely in oral form. It is argued that social and technological change often served as the impetus for the development

of new laws. Humanity has many times intervened in its own biological evolution with the help of technology; now it is an important moment from the viewpoint of law and ethics when technology may interfere in further human evolution. The greatest concern in this regard is the era of rapid development of artificial intelligence, which makes new demands on a human being.

Scientific novelty: the article shows the role of the African continent in the origin and development of humanity and socio-legal institutions in the light of modern transformations and the construction of a new social reality.

Practical significance: the conducted research creates prerequisites for further development of the theory of anthroposociogenesis and in-depth conceptual historical and legal study of the role of the African continent in the development of humanity and its social institutions.

For citation

Traore, D. (2024). From the Theory of the African Origin of Humankind to Modern Social, Legal and Technological Innovations: a Brief Analytical Excursion into Anthroposociogenesis. *Journal of Digital Technologies and Law, 2*(2), 473–486. https://doi.org/10.21202/jdtl.2024.24

References

Avila Negri, S. M. C. (2021). Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. *Frontiers in Robotics and AI*, *8*, Art. 789327. https://doi.org/10.3389/frobt.2021.789327

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

Bob-Milliar, G. M. (2021). Africa's Contributions to World Civilization. In *The Palgrave Handbook of Africa and the Changing Global Order* (pp. 25–42). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-77481-3_2

Bryson, J. J., Diamantis, M. E., & Grant, Th. D. (2017). Of, For, and By the People: The Legal Lacuna of Synthetic Persons. *Artificial Intelligence and Law*, *25*, 273–291. https://doi.org/10.1007/s10506-017-9214-9

Calo, R. (2015). Robotics and the Lessons of Cyberlaw. *California Law Review*, *103*(3), 513–563.

Chesterman, S. (2020). Artificial Intelligence and the Limits of Legal Personality. *International & Comparative Law Quarterly*, *69*, 819–844. https://doi.org/10.1017/s0020589320000366

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

Hárs, A. (2022). AI and international law – Legal personality and avenues for regulation. *Hungarian Journal of Legal Studies*, *62*(4), 320–344. https://doi.org/10.1556/2052.2022.00352

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

Lovejoy, P. E. (2014). *African contributions to science, technology and development*. Collective Volume the (Slave Route Project, UNSECO 2012).

Maarten Herbosch. (2024). Fraud by generative AI chatbots: On the thin line between deception and negligence. *Computer Law & Security Review*, *52*, 105941–105941. https://doi.org/10.1016/j.clsr.2024.105941

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

McCarty, L. T. (2017). Finding the Right Balance in Artificial Intelligence and Law. In *Research Handbook on the Law of Artificial Intelligence* (Chapter 3, pp. 55–87). Edward Elgar Publishing. https://doi.org/10.4337/9781786439055.00013

McNally, Ph., & Inayatullah, S. (1988). The Rights of Robots: Technology, Culture and Law in the 21st Century. *Futures*, *20*(2), 119–136. https://doi.org/10.1016/0016-3287(88)90019-5

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*, Art. 788179. https://doi.org/10.3389/frobt.2021.788179

Mulgan, T. (2019). Corporate Agency and Possible Futures. *Journal of Business Ethics*, *154*, 901–916. https://doi.org/10.1007/s10551-018-3887-1

Pagallo, U. (2018). Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems. *Philosophical Transactions of the Royal Society*, *376*(2133), Art. 20180168. https://doi.org/10.1098/rsta.2018.0168

Sertima, I. V. (Ed.) (1983). Blacks in Science: Ancient and Modern. *Journal of African Civilizations*, *5*(1-2).

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

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287.

Stiglitz, J. E. (2017). The coming great transformation. *Journal of Policy Modeling*, *39*(4), 625– 638. https://doi.org/10.1016/j.jpolmod.2017.05.009

Author information

Djeneba Traore – PhD, Professor, Former Rector, University of Arts and Humanities of Bamako; Director General for Regional Integration and Social Transformations in West Africa, West Africa Institute
Address: E 3637, Bamako, Mali; 396-A, Praia, Cabo Verde
E-mail: badjenetraore@yahoo.fr
ORCID ID: https://orcid.org/0009-0006-2674-2565
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57202159729

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – December 3, 2023
Date of approval – January 6, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024